Blockchain-Based Integrated Sensing and Communication Services in 6G Networks

Haihan Duan, Abdulmotaleb El Saddik, and Xiping Hu

Abstract

Growth in the metaverse has been significant in recent years, aided by the robust communication capacities of the 5G network. Moving into the 6G era, integrated sensing and communication (ISAC) services are regarded as a potential solution for controlling avatars in the metaverse, because ISAC can enable users to have all-pervasive sensing capabilities at all times without needing additional equipment. However, current research primarily delves into the technological aspects of ISAC under the presumption of these sensing services being handled by centralized entities, such as corporations or organizations, while considerably less attention has been given to the potential issues inherent in such centralized control, including problems of privacy and the risks from monopolies. In light of these gaps, our paper introduces a novel framework for implementing blockchain-based ISAC services in 6G networks. Recognizing the associated challenges and possible risks with our proposed framework, we provide an interactive process featuring appropriate solutions. Moreover, this paper further evaluates the capacity and performance of our theoretical framework through a case simulation based on the real-world distribution of base stations. Furthermore, we conclude the limitations inherent within our proposed blockchain-based ISAC services and provide a list of relevant and consequential future research topics.

Introduction

0ver the past few years, driven by the advances in 5G technology, the metaverse, a visionary concept, has rapidly come to the forefront of technological discourse and development. Metaverse denotes the next-generation Internet, where the users can act as avatars and interact with each other and software applications in a three-dimensional (3D) virtual world [1]. This rich virtual experience is amplified by the profound communication capabilities inherent in the 5G network. Through the 5G network, real-time interactions and controls become possible and more accurate. While wearables, such as motion-capturing suits, offer an effective medium to translate physical actions to the virtual domain, they also present limitations. Primarily, the metaverse hinges on unrestricted accessibility [1], an omnipresent user connection irrespective of geographical or temporal constraints. Thus, despite the precision and immersive experience wearables provide, their bulkiness and complexity pose challenges, especially when considering mobile users. An alternate method is explored in computer vision (CV) regarding action recognition and reconstruction [2], but CV approaches grapple with their own complications, ranging from environmental factors like poor lighting to physical obstructions. Moreover, the lingering specter of privacy concerns, especially the leakage of captured images and videos, remains a significant barrier to its widespread adoption.

As we pivot towards the impending era of 6G communication [3], the concept of integrated sensing and communication (ISAC) emerges as a potential game-changer [4]. ISAC aims to create a world where sensing technologies are seamlessly integrated into the communication network, making them available everywhere. For illustrative purposes, Fig. 1 depicts a prototypical workflow commencing with the sensing phase and culminating in metaverse avatar control. In the proposed framework, transmitters disseminate signals within an environment containing a user. These signals are captured by the receiver, processed to extract channel state information (CSI), and transformed into tensors after denoising. These tensors will be fed into a deep neural network model designed for skeleton estimation (also named pose estimation [2]). The results will enable the accurate reconstruction of the user's skeletal structure, which is then utilized for avatar control within the metaverse. Compared to traditional wearable or CV-based methodologies, the ubiquitous sensing approach showcases its advantages in broad accessibility, user convenience, and privacy protection. Existing research further supports the viability of this method, spanning various standards such as radio frequency [5], Wireless Fidelity (WiFi) [6], Long-term Evolution (LTE) [7], and Millimeter Wave (mmWave)

Haihan Duan is with the Artificial Intelligence Research Institute, Shenzhen MSU-BIT University, Shenzhen 518172, China, also with the Guangdong-Hong Kong-Macao Joint Laboratory for Emotion Intelligence and Pervasive Computing, Shenzhen 518172, China, also with the Computer Vision Department, Mohamed bin Zayed University of Artificial Intelligence, Abu Dhabi, United Arab Emirates, and also with the Multimedia Communication Research Laboratory (MCRLab), University of Ottawa, ON K1H 8M5, Canada; Abdulmotaleb El Saddik is with the Human Computer Interaction Department, Mohamed bin Zayed University of Artificial Intelligence, Abu Dhabi, United Arab Emirates, and also with the Multimedia Communication Research Laboratory (MCRLab), University of Ottawa, ON K1H 8M5, Canada; Xiping Hu (corresponding author) is with the Artificial Intelligence Research Institute, Shenzhen MSU-BIT University, Shenzhen 518172, China, also with the Guangdong-Hong Kong-Macao Joint Laboratory for Emotion Intelligence and Pervasive Computing, Shenzhen 518172, China, and also with the School of Medical Technology, Beijing Institute of Technology, Beijing 100090, China.

Digital Object Identifier: 10.1109/MNET.2024.3516140
Date of Current Version: 18 March 2025
Date of Publication: 12 December 2024

[8]. In the forthcoming 6G era, the envisioned global expanse of the ISAC network holds the theoretical potential to enable universal access to sensing services, irrespective of location, without the necessity for auxiliary equipment. Consequently, ISAC services emerge as an indispensable and propitious cornerstone of the 6G network.

In recent scholarly endeavors, extensive analyses of ISAC have predominantly concentrated on the technological dimensions, especially pointing toward sensing technologies [4]. However, detailed examinations of the service mechanisms are absent from these discussions. A prevailing assumption in the existing literature [5], [6], [7], [8] is the adoption of centralized telecommunications entities or organizations for ISAC services, which shows a consolidated process that spans from initial transmission to sensing and data relay. While this approach offers streamlined efficiency for ISAC service provision, it is not devoid of significant challenges: (1) the centralized service necessitates a robust Know Your Customer (KYC) protocol, thus singular entities can access comprehensive user data (ranging from identifications to locations and activities), posing substantial privacy risks; (2) with centralized control, there's an inherent potential for monopolistic dominance, which can adversely impact service pricing transparency and overall efficacy; (3) the requirement for additional data-sharing methodologies to ensure unoccupied signal channels introduces supplementary operational expenses. In light of these challenges, turning to a blockchain-based decentralized framework emerges as a potential solution for ISAC services. At its core, blockchain operates as a distributed ledger, and contemporary blockchain systems support smart contracts to enable the automated execution of programs [9]. This decentralized approach promises enhanced privacy safeguards. Users are abstracted behind anonymous identifiers, and financial transactions are completed via cryptocurrencies, obviating traditional KYC protocols. Furthermore, it's imperative to highlight that emerging metaverse architectures are increasingly underpinned by blockchain ecosystems [1]. Thus, a blockchain-based ISAC service infrastructure exhibits a natural compatibility with future metaverse applications.

With this backdrop, our study embarks on an exploratory journey into integrating blockchain and ISAC service in the 6G landscape. The contributions of this paper are as follows:

- This paper conceptualizes a framework for integrating blockchain with ISAC services in 6 G network. To the best of our knowledge, this is the first study that focuses on ISAC services from a decentralized perspective.
- By delving deep into the inherent challenges and potential risks of such integration, this paper not only illuminates these issues but also proposes a comprehensive ISAC service workflow complemented by targeted solutions.
- Grounding our theories in practice, this paper conducts a case simulation rooted in real-world base station distributions around our affiliated university and offers insights into the operational viability of our proposed framework.

ISAC aims to create a world where sensing technologies are seamlessly integrated into the communication network, making them available everywhere.

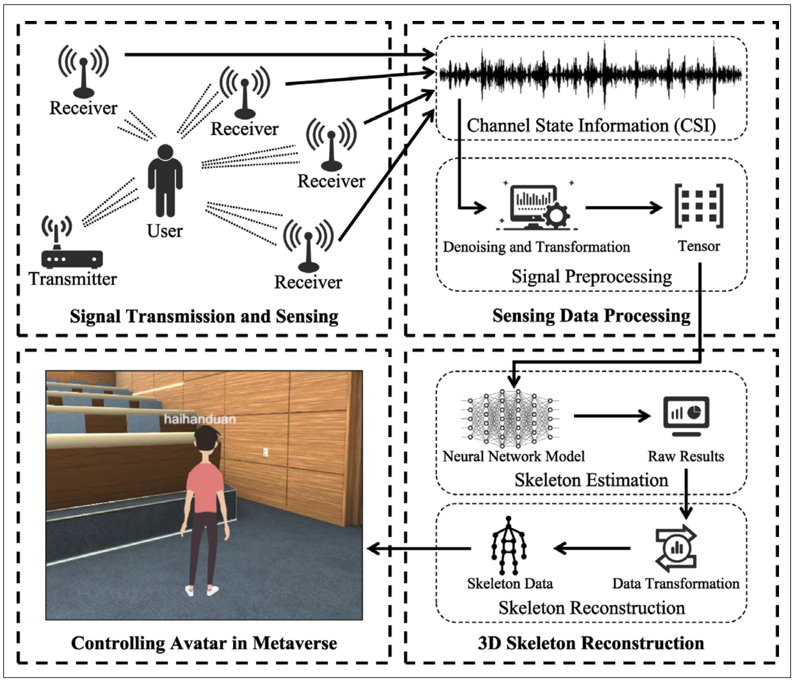

FIGURE 1. Workflow from Sensing to Metaverse Avatar Control.

- In conclusion, this paper critically examines the limitations of our proposal while also charting out potential research topics.

Blockchain-Based Integrated Sensing and Communications Services in 6G Network

In this section, we first overview the proposed framework for the blockchain-based ISAC services in 6G network, then we investigate the challenges and risks. At last, we present a workflow for the services, offering solutions to the identified challenges.

Framework Overview

Fig. 2 illustrates the proposed framework for blockchain-based ISAC services in 6G network, with three primary layers: the physical layer, the network layer, and the application layer. Additionally, the user experience and the details regarding mobile devices are elucidated on the right side of Fig. 2. To provide a comprehensive understanding, this subsection begins by explaining a typical example of user interaction with ISAC services in a practical application scenario, following with the data flow indicated by the solid arrow in Fig. 2.

Consider a scenario where a user intends to utilize the ISAC service for a metaverse connection. Equipped solely with a mobile phone and a portable virtual reality (VR) headset with a lightweight design (which integrates the mobile phone as its display), the user first uses the mobile phone to explore nearby service providers supported by smart contracts. After identifying appropriate transmitters and receivers, the user wears the

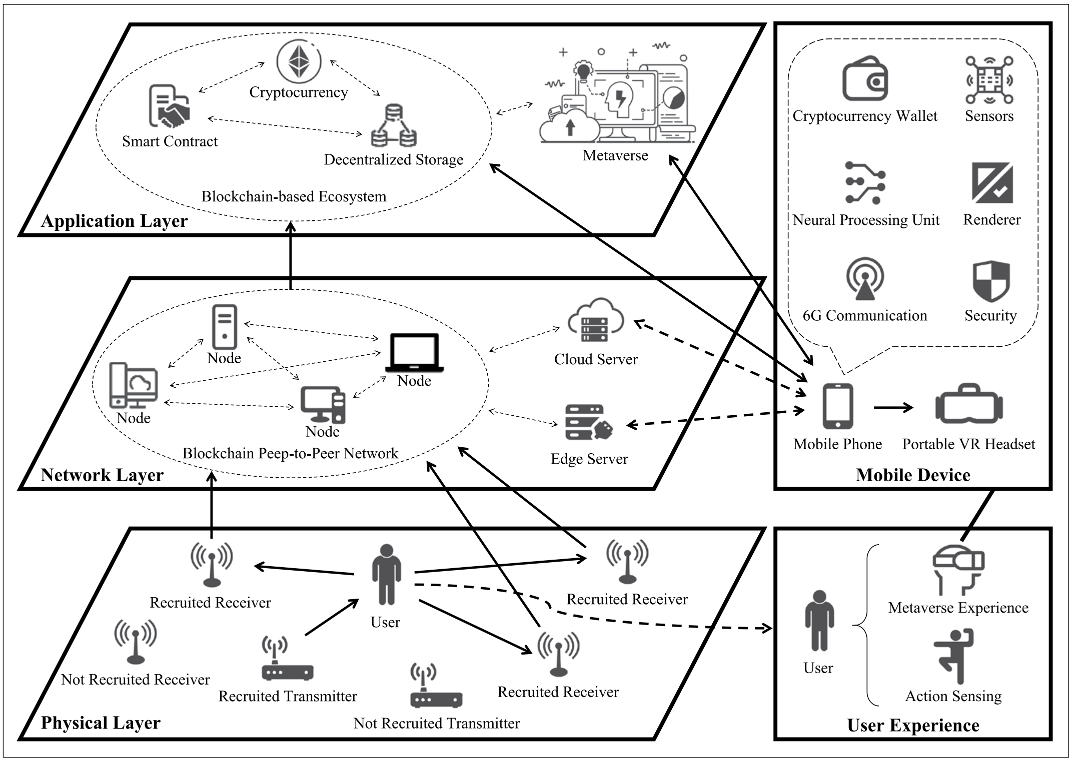

FIGURE 2. Framework of Blockchain-based Integrated Sensing and Communications Services in 6G Network.

VR headset to engage with the service. Before delving into the metaverse, there is a brief phase of neural network model training tailored to the new sensing context, given the prevalence of deep learning in current effective sensing techniques [5], [6], [7], [8]. For instance, following an app's guidance, the user performs specific actions, allowing data collection to fine-tune a pre-trained model on the mobile phone. After that, the user can continuously engage with the ISAC service and count expenses by usage duration.

The components essential to realizing this application scenario across different parts are detailed as follows:

Physical Layer. The ubiquitous sensing technology fundamentally hinges on physical signals. As demonstrated in Fig. 2, transmitters emit signals ubiquitously, and a set of receivers capture user-reflected signals, processing and transmitting this data to users' mobile phones. Specifically, the transmitters and receivers are collectively termed "service providers."

Network Layer. The proposed ISAC services are built on a blockchain peer-to-peer (P2P) network as the infrastructure of the services. Additionally, the network layer incorporates both cloud and edge servers, potentially accelerating neural network model training and skeleton reconstruction.

Application Layer. For a simplified illustration, the application layer mainly consists of two core components: (1) blockchain-based ecosystem, encapsulating cryptocurrency, smart contracts, and decentralized storage, pivotal for the complete ISAC service cycle; (2) metaverse, representing various applications facilitated by ubiquitous sensing technologies.

Mobile Device. The framework relies on a mobile phone and a portable VR headset. The mobile phone is a central terminal to orchestrate the ISAC service using integrated components. Features such as a cryptocurrency wallet and security unit can ensure anonymity during interactions and transactions, and sensors, neural processing units, and a renderer can enhance user immersion when collaborating with the VR headset. The cornerstone of the entire framework is the 6 G communication, which is essential for delivering the overall ISAC service.

Challenges and Risks

Regarding the detailed service process, several challenges and risks inherent to the system necessitate discussion and solutions, where five salient challenges and risks are elucidated in this subsection. Specifically, it is crucial to acknowledge two foundational assumptions for this initial version of the ISAC service framework: (1) service participants operate rationally, suggesting they lean towards decisions offering positive utility; (2) service providers do not collude, ensuring the retention of a decentralized system's anonymity.

CR1. *Obtaining Available Service Providers:* In the ISAC service ecosystem, users' positions are not fixed, while the service providers can also dynamically enter or exit the ecosystem. Thus, users require an efficient approach for obtaining information about nearby service providers to assess their availability and recruit suitable ones.

CR2. *Occupied Signal Channel Identification:* As evidenced by WiPose [6] and RF-Pose3D [5], ubiquitous sensing technologies necessitate fixed signal channels or frequency bands, so users in the same region should employ unoccupied channels to minimize signal interference. Hence, signal transmitters must be aware of occupied channels to avoid overlaps.

CR3. *Anonymous Sensing Data Transmission:* A notable benefit of the proposed framework is user privacy, facilitated by the inherent anonymity of the public blockchain. Therefore, it is also imperative to ensure that the data transmission remains inviolable, shielding users' IP/MAC addresses from potential exposure.

CR4. *Service Payment in an Untrusted Decentralized Network:* Due to the anonymity, inherent distrust exists within the public blockchain. As such, anonymous service providers might cease operations after receiving payments, emulating "lazy workers" in crowdsourcing [10]. Considering the assumption that service providers act rationally, such behavior might be lucrative without transmission or reception costs.

CR5. *Privacy Concerns of Action Reconstruction Model Training:* As discussed in the section "Framework Overview," the current effective ubiquitous sensing technologies require fine-tuning pre-trained models to better facilitate skeleton reconstruction. Concurrently, since signals permeate public physical spaces, malicious attackers might also capture these signals and reconstruct users' activities.

Workflow

In this subsection, we propose a comprehensive interactive process for blockchain-based ISAC services in 6G network, as depicted in Fig. 3. This process primarily encompasses four phases: service participants registration, service request and preparation, signal transmission and sensing, and service completion. More importantly, we will also delve into solutions for the challenges and risks enumerated in the section "Challenges and Risks," aligning with each step of the interactive process illustrated in Fig. 3.

> In light of these challenges, turning to a blockchain-based decentralized framework emerges as a potential solution for ISAC services.

Phase 1: Service Participants Registration. Initially, all service participants are required to register in the blockchain. In step (1), common users simply generate a public key (user address) and private key pair from the blockchain, subsequently storing them within their cryptocurrency wallet. As for service providers, they are asked to register in the blockchain smart contract, in which they provide the necessary physical parameters of their devices (e.g., location, signal coverage range, antennas, sampling rate, subcarrier amount) and information about their services (e.g., price, available duration), referring to step (2). This registration does not differentiate between transmitters and receivers. Service providers lacking signal transmission capabilities (who can only be recruited as receivers) can be identified by a signal coverage range equal to zero, which incentivizes the general public to contribute to the service using surplus 6G devices with only signal reception capabilities, enhancing service capability and promotes societal benefit. Concurrently, decentralized storage services may

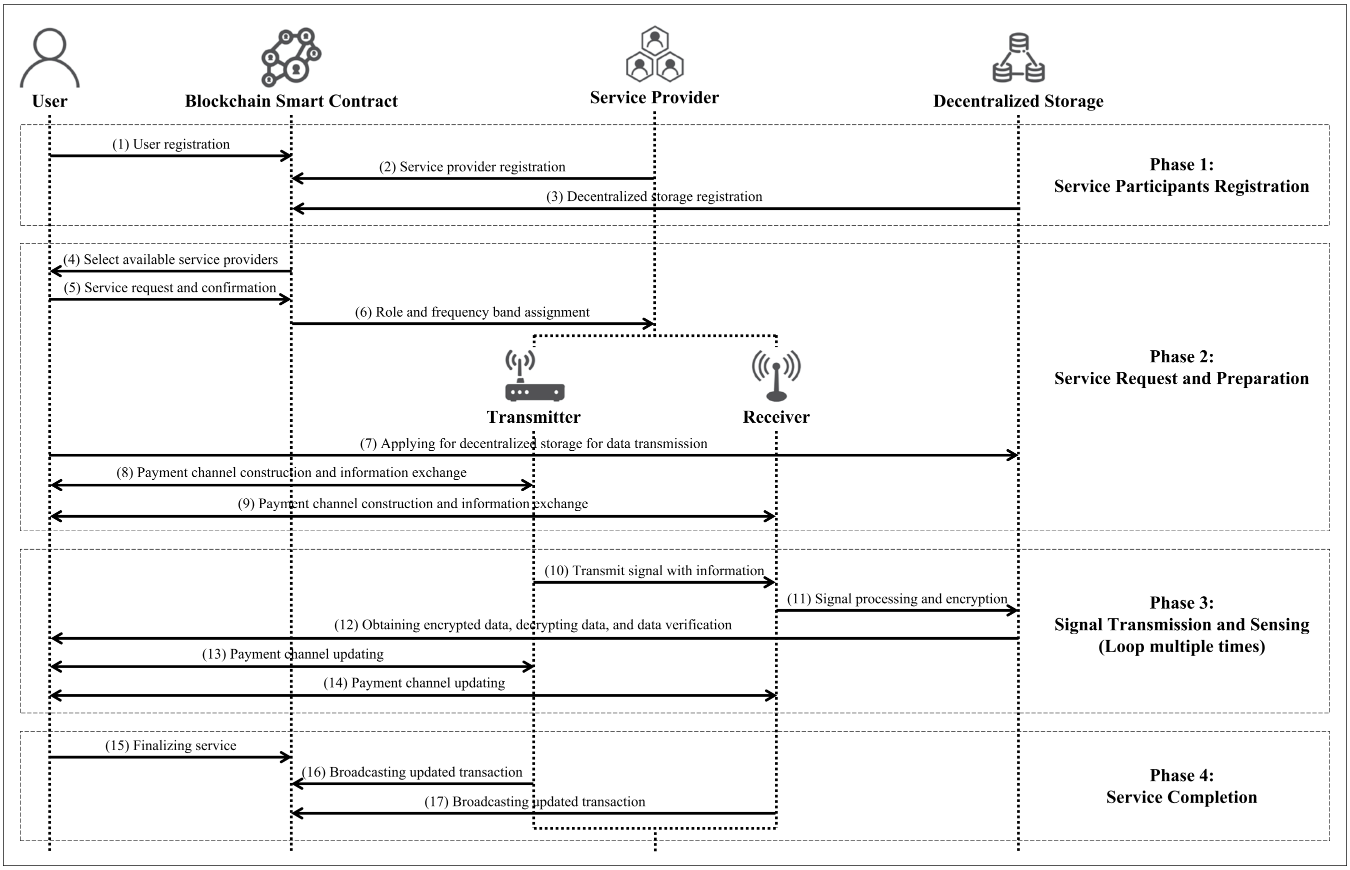

FIGURE 3. Interactive Process of the Blockchain-based Integrated Sensing and Communications Services in 6G Network.

also register in the smart contract, as illustrated in step (3), and their functions will be further discussed in Phase 2.

Phase 2: Service Request and Preparation. To engage with the ISAC service, users utilize an application on their mobile devices to discover and select available service providers in step (4). In this scenario, the public blockchain act as a transparent database, and the users can filter nearby service providers based on the their private location. In step (5), following the service provider selection, the service request procedure requires signature confirmation using the user's private key. Subsequently, the recruited service providers' status is updated to "unavailable" for other users, effectively addressing **CR1**.

After that, step (6) delineates the assignment of roles and frequency bands. According to the users' appointments, the smart contract assigns roles to the recruited service providers. Then, the service providers are categorized into transmitters and receivers (aligning with WiPose's experimental setup [6], we assume there are one single transmitter and multiple receivers). With states of all service providers accessible to the smart contract, it can determine and allocate an unoccupied frequency band within the service region, solving **CR2**.

Step (7) is to apply for decentralized storage for sensing data transmission, which refers to the challenge of **CR3**. Specifically, this decentralized storage system must support queues or streaming services to facilitate real-time data read/write capabilities. Acting as an intermediary between users and service providers negates the need for direct communication using IP/MAC address, addressing **CR3**. Besides, during this step, users can also grant access solely to the addresses of their recruited service providers, preventing unauthorized or malicious interference writing by potential attackers.

During the service preparation, necessary information needs to be exchanged between the user and service providers, referring steps (8) and (9). This encompasses parameters such as sampling rate and the address/interface of the decentralized storage secured in step (7). Simultaneously, these steps include the establishment of a payment channel [11] between users and service providers, laying the groundwork for a secure ISAC service, where the details are explicitly discussed in Phase 3.

Phase 3: Signal Transmission and Sensing. One of the most pressing concerns revolves around the inherently decentralized and anonymous nature of the blockchain, as identified in **CR4**. The system is susceptible to untrustworthy participants, termed "lazy workers". However, this challenge can be effectively alleviated by the innovative incorporation of blockchain payment channel technology [11]. Originally conceived as a strategic off-chain scalability solution, payment channels were designed to enhance both the frequency and volume of transactions of the large-scale public blockchain. The operation is relatively straightforward: two participating entities deposit a predetermined amount of cryptocurrency on the blockchain, then they engage in transactions off the blockchain by continually updating their balances authenticated through dual-sided signatures, ensuring the integrity of each transaction. Eventually, the final balance, reflecting all off-chain transactions, is reconciled and updated on the main blockchain (more details can refer to Papadis and Tassiulas [11]).

In the context of our proposed framework, users make an upfront deposit during the payment channel establishment, representing the service fee. With the ISAC service actively running, transmitters emit predetermined signals ubiquitously.

Once captured by receivers, these signals undergo a transformation into tensors after denoising, denoted as sensing data. Specifically, the sensing data transmissions are organized into brief and concise frames by controlling the sampling rate, as indicated in step (10). For instance, WiPose [6] applies a sampling rate of 10 frames per second (FPS) to form an input tensor. After this transformation, the sensing data is sent to the user-provided decentralized storage, as depicted in step (11). Note that a crucial security measure here is the encryption of this sensing data using the user's public key. In step (12), the user retrieves the encrypted data, undertakes the decryption process, and verifies the integrity and authenticity of the received data. Subsequently, both the user and service providers update the payment channel with signature verification, adjusting the balance in favor of the service providers based on the average price of the short data frame (steps (13) and (14)). Such a fine-grained approach to service provision acts as a deterrent against misconduct, particularly for lazy workers in **CR4.**

However, even with the payment channel ensuring service post-payment, there remains the risk of lazy workers without physical capabilities of data reception to transmit deceptive data to users. Therefore, it becomes imperative to detect and rectify such behavior to address **CR4.** Thanks to ISAC's capabilities, the transmitted signal can also convey specific information from the transmitter to receivers. This realization paves the way for our proposed mechanism, centered around the verification of pseudo-random numbers. During step (8) of Phase 2, the user offers the transmitter a generator of pseudo-random numbers, denoted as $G(s, t)$. Here, s stands for the seed, while t represents the timestamp assigned to each data frame, which is unexposed to the receivers. This design ensures that each signal frame captured by the receivers is embedded with a unique pseudo-random number that evolves with the timestamp. Such a mechanism makes the prediction of the pseudo-random numbers virtually impossible for the receivers, while the user can easily verify these numbers. Thus, this strategy provides an effective mechanism to detect and identify lazy workers without genuine service capabilities.

Moreover, the broad dissemination of signals introduces another challenge identified in **CR5**. As previously discussed in the section "Framework Overview," a brief model training phase necessitates users to perform guided actions. A potential countermeasure to the risks is introducing a degree of randomness during the training, e.g., actions could be assigned at random intervals, ensuring unpredictability. Consequently, attackers face challenges in obtaining ground truth for their model training, thereby safeguarding the system and addressing **CR5.**

Phase 4: Service Completion. At the end of the service, the user finalizes the process in step (15). Then, service providers broadcast their latest transactions to the public blockchain to claim their earnings (refer to steps (16) and (17)), which marks the conclusion of the blockchain-based ISAC service loop.

Case Simulation

To evaluate the potential capacity and performance of the proposed service framework, we conduct a case simulation based on data of actual base stations. This section initiates with the experimental settings, and then we study the impact of varying user amounts and service provider selection methods.

Experimental Settings

To conduct a realistic simulation of the service framework, we sourced data of base stations situated in proximity to the Mohamed bin Zayed University of Artificial Intelligence in Abu Dhabi, United Arab Emirates, from OpenCelliD (www.opencellid.org). The geographical coordinates span from 24.4119°N to 24.4398°N in latitude and from 54.5844°E to 54.6342°E in longitude, containing 838 base stations. This data encompasses details like each base station's precise coordinates, radio types, signal coverage range, etc. Fig. 4 provides a visualization of the base stations' distribution. This map is rendered using OpenStreetMap [12], which applies a color gradient to indicate signal coverage, with deeper shades of blue signifying areas of stronger signal coverage. It's crucial to highlight our assumption that, in this case simulation, these base stations operate on a 6 G communication network.

In this simulation, to avoid complex mathematical formulations, several assumptions are posited as follows: (1) there exists a positive relationship between the service price of each base station and its signal coverage range; (2) the quality of service is inversely correlated with the distance between the user and recruited service providers. For the generation of users' coordinates, a uniform distribution is employed. Subsequently, a Gaussian distribution is utilized to generate the volume of users per hour, spanning from 0 to 23 , as well as the anticipated service duration for each user, denominated in hours. These distributions intend to emulate the service demand over a typical day. According to the experimental settings of WiPose [6], we assume that every user requires the engagement of one transmitter and nine receivers within the signal coverage range, culminating in 10 service providers per user. Note that, in this simulation, factors such as signal degradation after reflection are not taken into account.

The Impact of Service User Amounts

In this analysis, we aim to investigate the potential capacity of the established settings by incrementally increasing the daily service user amount from 100 to 2000. For the service provider selection, we adopt a nearest first selection approach. As illustrated in Fig. 5, the figure showcases the service rate in terms of hours. We can find that the capacity well meets the demand when the service user amount stands at 100. However, there is a noticeable decline in the service rate as the user amount augments, with a pronounced drop during peak usage hours. For instance, when the user count reaches 2000, only approximately 20% of users can access the service during these peak periods. However, this capacity is insufficient for developed cities, highlighting the importance of integrating more public service providers through crowdsourcing [10], potentially enhancing both the service capacity and effectiveness. Therefore, the proposed public blockchain-based ISAC service framework well fits the identified service demands, since it allows the general public to contribute to the service using their surplus 6 G devices, enhancing social welfare.

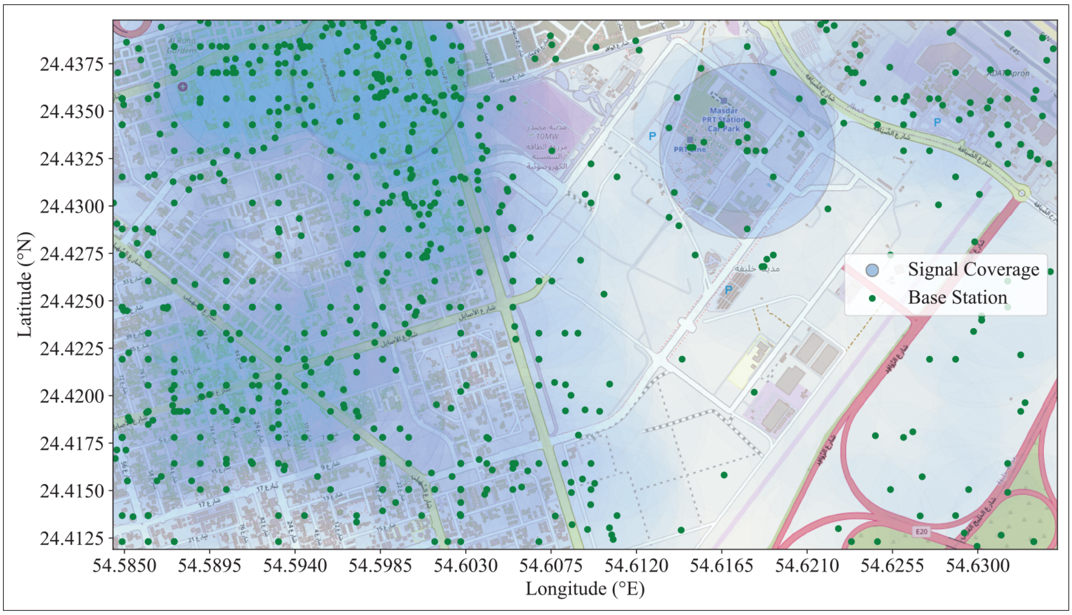

FIGURE 4. Distribution Map of the Base Stations and Their Signal Coverage Nearby the Mohamed bin Zayed University of Artificial Intelligence in Abu Dhabi, United Arab Emirates.

The nascent field of blockchain-based ISAC services in the 6G network is a burgeoning research area that presents various challenges and offers ample opportunities for improvement.

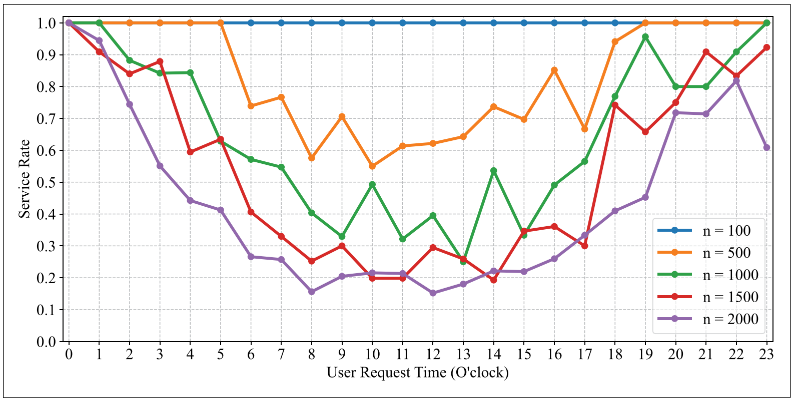

FIGURE 5. Service Rate in Different Service User Amounts Changing with Time.

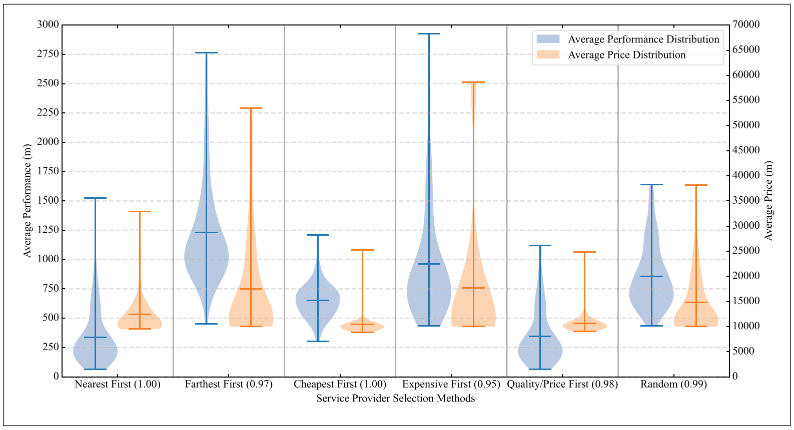

FIGURE 6. Average Performance and Total Price Distribution of Different Service Provider Selection Methods.

The Impact of Service Provider Selection Methods

This subsection delves into the impacts of different service provider selection methodologies. Specifically, we simulate six strategies: nearest first, farthest first, cheapest first, expensive first, quality/price first, and random selection. For the setup of this analysis, we set the number of users remaining constant at n = 100. The experimental results of these methodologies are graphically represented in Fig. 6, which employs violin plots for the 100 users to illustrate the distribution of average performance and total price, and the service rate is indicated within brackets of each strategy. The presented data shows that each selection strategy has unique characteristics in terms of performance, expenditure, and service rate. For instance, the nearest first approach optimizes performance, the cheapest first method is most cost-effective, and the quality/price first strategy seems to be relatively optimal with a good trade-off between the performance and cost. In fact, seemingly counter-intuitive strategies like farthest first and expensive first also have their advantages, which can offer enhanced privacy by obfuscating the user's location due to the broader signal coverage range of service providers. Thus, an effective ISAC service must be versatile to accommodate different users' diverse strategies and preferences.

Limitations and Future Research Topics

The nascent field of blockchain-based ISAC services in the 6G network is a burgeoning research area that presents various challenges and offers ample opportunities for improvement. While ISAC technology itself has vast potential for further study, such as enhancements in sensing accuracy, multi-person adaptation (more research directions can refer to Cui et al. [4]), this paper focuses on service-related limitations. Herein, we list several pressing research topics as the tip of the iceberg:

RT1. *Addressing Malicious Service Participant Behavior:* In the section "Challenges and Risks," we have assumed that service participants exhibit rational behavior without collusion. Nevertheless, in practice, untrustworthy service providers on the public blockchain could deliberately disrupt the service devoid of rationality. This vulnerability becomes particularly evident when considering the pseudo-random number verification of the section "Workflow," where malicious service providers could deploy a device to capture the pseudo-random number and share it among other colluding service providers. While a reputation system [13] might offer a solution, it remains susceptible to manipulations by colluding malicious entities. Another potential method could be the permissioned blockchain, but it may compromise the decentralization and create barriers for prospective participants.

RT2. *Determining Optimal Pricing Strategies:* Establishing an appropriate pricing model for the blockchain-based ISAC service holds significant implications for social welfare. Service providers must integrate considerations of physical attributes into their pricing models, encompassing the geographic location, device-specific parameters, etc. Concurrently, they must follow the shifts in the broader market landscape, particularly fluctuations in user demand and competitor presence, potentially leading to dynamic pricing strategies [14].

RT3. *Optimizing Service Provider Selection and Scheduling:* This study operates under the presumption that users select service providers based on their individual strategies. However, constrained by limited information, the decision-making capacity of a single user may influence the service's efficiency. Integrating smart contracts to govern service scheduling emerges as a preferable alternative, but it also presents various challenges. One pressing concern is the acquisition of user locations without breaching privacy, which might be addressed through zero-knowledge technologies [15]. Additionally, our simulation follows with the settings of WiPose [6], engaging 10 service providers. However, this paper [6] also studies the varying numbers of receiving antennas, revealing a concave function characterized by diminishing marginal utility, which motivates further research regarding the optimal number of service providers. In essence, multiple research questions surrounding optimizing selection and scheduling within the ISAC service framework necessitate thorough exploration.

RT4. *Navigating the Balance Between Signal Strength and Privacy:* Proximity to transmitters and receivers typically enhances signal strength, thereby augmenting sensing accuracy. However, this proximity also restricts the user's physical radius, amplifying potential privacy vulnerabilities, especially given the inherent transparency of public blockchains. Thus, navigating the balance between signal strength and privacy becomes a critical consideration in practical applications.

RT5. *Mitigating the Influence of Service Provider Dropout:* As highlighted in the section "Framework Overview," state-of-the-art ubiquitous sensing technologies predominantly rely on learning-based methodologies [5], [6], [7], [8]. Nonetheless, in real-world scenarios, unforeseen events may prompt service providers to exit. Such attrition might perturb the input tensor distribution, necessitating model recalibration or retraining. While measures such as financial penalties or reputation loss can discourage providers from leaving without valid reasons, unexpected events like power outages remain inevitable. Thus, strategies or technologies to lessen the influence of such dropouts are imperative.

RT6. *Investigating the Balance Between Sensing Latency and Privacy:* As discussed in Phase 3 of Fig. 3, decentralized storage is utilized as a communication intermediary between users and service providers to protect the users' privacy. However, the latency in authentication and data transmission through decentralized storage will influence the real-time sensing and controlling performance. To this end, the balance between sensing latency and privacy risk needs to be investigated, e.g., by introducing other communication intermediaries or protocols for users and service providers.

Conclusion

In this study, we have introduced a novel blockchain-based ISAC service framework in 6G network. We investigate five salient challenges and risks inherent within the framework, presenting solutions grounded in the service's interactive process. Moreover, a case simulation was conducted to evaluate the potential service capacity and assess its performance. Subsequently, we conclude the limitations intrinsic to the proposed blockchain-based ISAC service and propose five future research topics. While the fusion of ISAC with the 6G landscape remains nascent, the integration of ISAC technologies and blockchain will promise significant breakthroughs for both the academic and industrial realms, particularly in the enhancement of the metaverse in the forthcoming 6 G epoch.

Acknowledgment

This work was supported in part by the Guangdong-Hong Kong-Macao Joint Laboratory for Emotional Intelligence and Pervasive Computing, Artificial Intelligence Research Institute, Shenzhen MSU-BIT University.

References

[1] H. Duan et al., "Metaverse for social good: A university campus prototype," in *Proc. 29th ACM Int. Conf. Multimedia*, Oct. 2021, pp. 153–161.

[2] W. Liu et al., "Recent advances of monocular 2D and 3D human pose estimation: A deep learning perspective," *ACM Comput. Surv.*, vol. 55, no. 4, pp. 1–41, 2022.

[3] C.-X. Wang et al., "On the road to 6G: Visions, requirements, key technologies and testbeds," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 905–974, 2nd Quart., 2023.

[4] Y. Cui et al., "Integrating sensing and communications for ubiquitous IoT: Applications, trends, and challenges," *IEEE Netw.*, vol. 35, no. 5, pp. 158–167, Sep. 2021.

[5] M. Zhao et al., "RF-based 3D skeletons," in *Proc. Conf. ACM Special Interest Group Data Commun. (SIGCOMM)*, Aug. 2018, pp. 267–281.

[6] W. Jiang et al., "Towards 3D human pose construction using WiFi," in *Proc. Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Apr. 2020, pp. 1–14.

[7] W. Chen et al., "Robust dynamic hand gesture interaction using LTE terminals," in *Proc. 19th ACM/IEEE Int. Conf. Inf. Process. Sensor Netw. (IPSN)*, Apr. 2020, pp. 109–120.

[8] S.-P. Lee et al., "HuPR: A benchmark for human pose estimation using millimeter wave radar," in *Proc. IEEE/CVF Winter Conf. Appl. Comput. Vis. (WACV)*, Jan. 2023, pp. 5715–5724.

[9] A. Kumari, R. Gupta, and S. Tanwar, "Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review," *Comput. Commun.*, vol. 172, pp. 102–118, Apr. 2021.

[10] J. Kang et al., "Reliable federated learning for mobile networks," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 72–80, Apr. 2020.

[11] N. Papadis and L. Tassiulas, "Blockchain-based payment channel networks: Challenges and recent advances," *IEEE Access*, vol. 8, pp. 227596–227609, 2020.

[12] M. Haklay and P. Weber, "OpenStreetMap: User-generated street maps," *IEEE Pervasive Comput.*, vol. 7, no. 4, pp. 12–18, Oct. 2008.

[13] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Toward blockchain-based trust and reputation management for trustworthy 6G networks," *IEEE Netw.*, vol. 36, no. 4, pp. 112–119, Jul. 2022.

[14] A. Kumari, R. Gupta, and S. Tanwar, "PRS-P2P: A prosumer recommender system for secure P2P energy trading using Q-learning towards 6G," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2021, pp. 1–6.

[15] X. Sun et al., "A survey on zero-knowledge proof in blockchain," *IEEE Netw.*, vol. 35, no. 4, pp. 198–205, Jul. 2021.

Biographies

Haihan Duan (Member, IEEE) (duanhaihan@smbu.edu.cn) received the Ph.D. degree in computer and information engineering from The Chinese University of Hong Kong, Shenzhen, China. He is currently an Associate Professor with the Artificial Intelligence Research Institute, Shenzhen MSU-BIT University (SMBU). He is also with the Guangdong-Hong Kong-Macao Joint Laboratory for Emotion Intelligence and Pervasive Computing, Shenzhen. His research interests include multimedia, blockchain and Web3, human-centered computing, and metaverse.

Abdulmotaleb El Saddik (Fellow, IEEE) (elsaddik@uottawa.ca) is currently a Distinguished University Professor with the University of Ottawa, Ottawa, ON, Canada, and the Mohamed bin Zayed University of Artificial Intelligence, Abu Dhabi, United Arab Emirates. His research interests include metaverse, digital twins, multimedia communication, connected health, and quality of experience. He is a fellow of the Royal Society of Canada (FRSC), the Engineering Institute of Canada (FEIC), and the Canadian Academy of Engineers (FCAE).

Xiping Hu (Member, IEEE) (huxp@smbu.edu.cn) received the Ph.D. degree from The University of British Columbia, Vancouver, BC, Canada. He is currently a Professor with the School of Medical Technology, Beijing Institute of Technology, China, the Artificial Intelligence Research Institute, Shenzhen MSU-BIT University (SMBU), and the Guangdong-Hong Kong-Macao Joint Laboratory for Emotion Intelligence and Pervasive Computing, Shenzhen, China. His research interests include mobile cyber-physical systems, crowd sensing, and affective computing.