Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 2857510, 17 pages
https://doi.org/10.1155/2022/2857510

Research Article

Blockchain-Empowered High-Frequency Spectrum Management IoT: A Multilayer PBFT Consensus Perspective

Xi Chen,[1] Jian Yang,[2] and Junfei Qiu[3]

[1]School of Mechanical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China
[2]Unit. 31107 of the Chinese People's Liberation Army, Nanjing 210014, China
[3]Beijing Research Institute of Information Technology, Beijing 10094, China

Correspondence should be addressed to Jian Yang; yangjian_njust@foxmail.com

Received 27 February 2022; Revised 31 March 2022; Accepted 9 April 2022; Published 30 April 2022

Academic Editor: Mingqian Liu

High frequency (HF) is an important method for long-range communications and even the only mean when satellites are destroyed or interfered, which play an essential role in defense and economic construction. However, noncooperative frequency competition accompanied with power competition results in the continuously deterioration of HF electromagnetic environment. This article endeavors to resolve this issue through proposing blockchain-empowered HF spectrum management. Specifically, massive personal HF devices are organized around the preselected nodes to construct HF spectrum management IoT, further monitor, and share HF data through PBFT (Practical Byzantine Fault Tolerance) protocol. To address the scalability problem during the consensus, a multilayer PBFT consensus protocol is employed. Scalability evaluations show that increasing consensus layers of PBFT greatly reduces the communication complexity. Security assessments illustrate that the security performance will decline with the increase of layers. Tradeoff has been made between the communication complexity and security performance, indicating 2-4 layers PBFT is sufficient, which bring down the communication complexity and also achieve acceptable security performance.

1. Introduction

1.1. Background and Motivation. High frequency is an important method for long-range communication and even the only mean when the satellites are destroyed or interfered. Currently, wireless communication technologies, such as the 5th Generation Mobile Communication (5G) [1] and Internet of Things (IoTs) [2], are still in their booming era. Simultaneously, electromagnetic environment of high frequency (HF) band is persistently deteriorating, and HF background noise is increasing year by year, causing HF transmitters with hundreds or even thousands Watts hard to communicate well, which seriously threaten the survival and development of HF service.

So as to investigate the deteriorated degree of HF electromagnetic environment, we have monitored the evolution of HF electromagnetic environment for 5 years. The results are shown in Figures 1 and 2. From Figure 1, we can see that both the power and the number of HF signals are continuously increasing in the last 5 years. From Figure 2, we can see that in the past 5 years, the background noise of HF electromagnetic environment is increasing at a rate of 1 dB per year, which indicates that deteriorating trend of HF electromagnetic environment. How to reverse the deteriorating trend of HF electromagnetic environment? Our previous works indicate that *noncooperative frequency competition accompanied with power competition* is the key manual factor in the deterioration of HF electromagnetic environment [3]: The quality of HF communication largely depends on timely and accurately detecting of ionosphere evolution, which is hard to obtain, although hundreds of HF monitoring stations and ionosonde stations have been built. The reason is that HF transmitters neither know the ionosphere information in time nor guarantee the ionosphere of reflection point has HF monitoring stations or ionosonde stations. Then, people either blindly increase the transmission

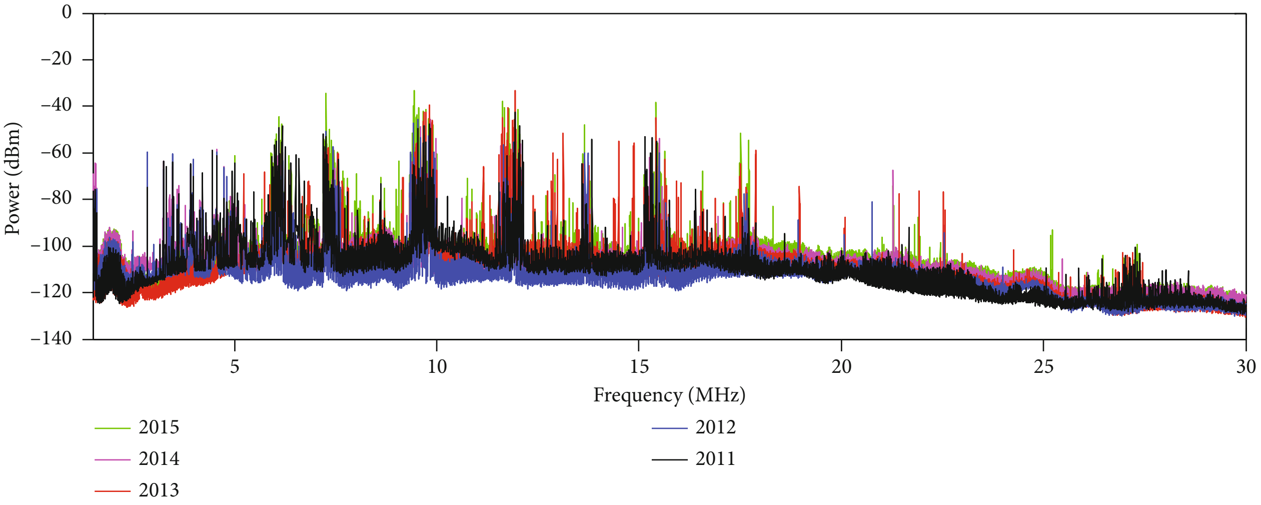

Figure 1: Five-year evolution of HF signals and HF electromagnetic environment.

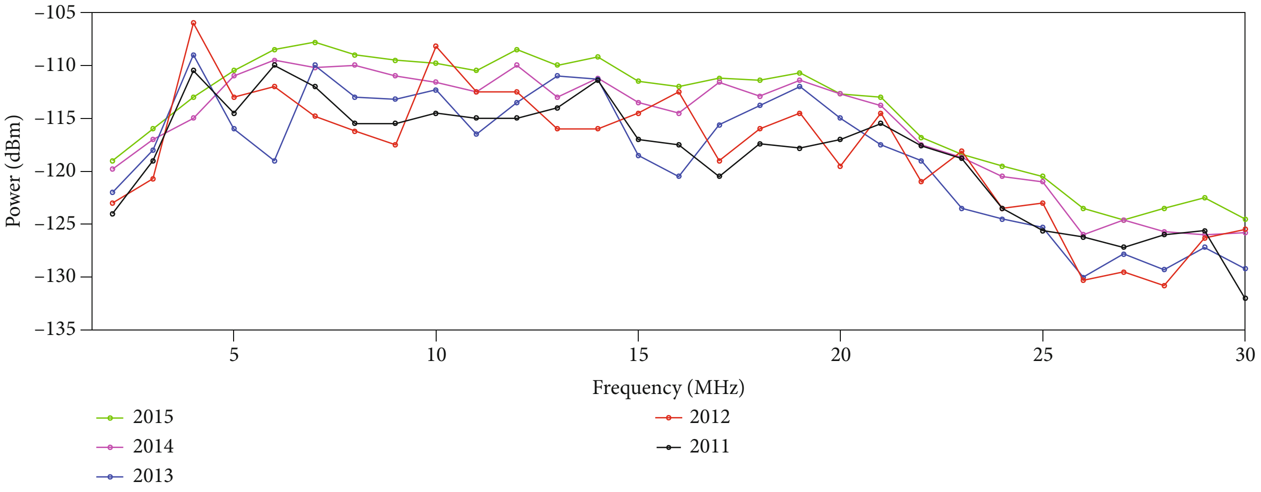

Figure 2: Five-year evolution of HF background noise.

power to improve communication quality or arbitrarily switch to idle (local) HF, i.e., the noncooperative frequency competition accompanied with power competition. It can be asserted that if we still insist utilizing HF resources in a *noncooperative* way, the earliest invented long-range communication method, HF will be probably destroyed by ourselves.

Firstly, how to change the noncooperative utilization mode of HF band? HF amateur service provides a solution. Amateur is a radiocommunication service used for self-training, intercommunication, and technical investigation [4]. HF amateurs are also called HAM and are distributed all over the world. If HF amateurs connect to each other and construct the HF spectrum management IoT, further monitor, and share the data of HF electromagnetic environment; HF transmitters no longer need to blindly increase the transmission power or arbitrarily switch to idle (local) HF; i. e. HF transmitters no longer need to adopt the noncooperative frequency utilization mode, finally promote the reduction of HF background noise, and improve the HF electromagnetic environment.

Secondly, how to motivate HF amateurs to construct the HF spectrum management IoT and monitor/share the data of HF electromagnetic environment? Emerging blockchain technology provides solution. Blockchain is a completely new distributed infrastructure and computing paradigm [5–7]. It applies a block-chain structure to store and authenticate data and distributed consensus algorithm to generate and update data, and asymmetric encryption to guarantee the security during data transmission, and smart contracts to operate and edit data. In a word, blockchain provides a safe and efficient solution for data transmission in distributed systems, which can be transplanted to HF band and construct the new framework of HF spectrum management IoT.

1.2. Related Works. Spectrum management was organized all along in a centralized manner, which was criticized for its inflexibility. The emergence of blockchain technology enables people to notice the natural connection between blockchain and spectrum management. In 2018 Mobile

World Congress, Rosenworcel, the speaker of FCC (Federal Communications Commission), said that blockchain can be recognized as lower-cost alternative of a centralized database to support shared access in specific spectrum bands [8]. Kotobi and Bilen in [9] attempted to apply blockchain to moving cognitive radio networks and proposed an Aloha medium-access protocol for dynamic spectrum access. Pei et al. in [10] combined cooperative spectrum sensing with mining in Bitcoin; each secondary user acts both a sensing node for cooperative sensing and a miner in blockchain network. After that, the applications of blockchain to spectrum management were investigated in [11, 12], including four typical scenarios, i.e., primary cooperative sharing, secondary cooperative sharing, primary noncooperative sharing, and secondary noncooperative sharing. The applications of blockchain in spectrum management are successively proceeded, some focus on UAV spectrum management [13, 14], some focus on the spectrum management in 5G/6G [15–17], and some focus on the spectrum management in Internet of Vehicles [18, 19].

In the rough, most blockchain can be divided into three categories, i.e., public blockchain, private blockchain, and consortium blockchain. Majority of early studies adopt public blockchain in the distributed spectrum management and apply proof-of-work (PoW) or proof-of-stake (PoS) as consensus protocol [9, 20, 21]. With the deepening of research, challenges gradually surfaced. Devices should be authenticated in spectrum management, no matter under a distributed or centralized manner. However, permissionless blockchain, i.e., public blockchain, is contrary to this requirement. Secondly, as time elapse, there will be increasing devices participating in the blockchain network, while private blockchain has fixed amount of nodes and cannot scale up later. A consortium blockchain is a special blockchain with multiple preselected nodes to establish the distributed shared database with moderate cost [14, 22]. For consortium blockchain, devices are allowed to join the blockchain only after authentication, which is in accordance with the concept of spectrum management IoT [23, 24].

Consensus protocol has always been seen as the core of the blockchain, which can be divided into two categories. One is represented by PoW or PoS; the other is represented by Practical Byzantine Fault Tolerance (PBFT) [20]. The following advantages indicate PBFT is more appropriate than PoW or PoS for spectrum management IoT. Firstly, compared with the throughput of PoW (7 Transactions Per Second (TPS)), the throughput of PBFT can achieve thousands of TPS [25, 26], which is essential for processing massive spectrum data. Secondly, the energy efficiency of PBFT is far superior to PoW. Considering that a large number of personal HF devices, i.e. HAMs, participate in the consensus, the simple consensus process of PBFT (consensus only performed among preselected nodes) represents higher energy efficiency compared with PoW or PoS (consensus is performed by all nodes). Thirdly, the confirmation delay of PoW sometimes can be up to hours, while that of PBFT is only milliseconds [27]. Last but not the least, the poor scalability of PBFT has always been criticized. In this article, multilayer PBFT is proposed to achieve a tradeoff between scalability and security for HF spectrum management IoT.

1.3. Contributions. Motivated by the aforementioned observations, in this article, we exploit the consortium blockchain to develop a HF spectrum management IoT and apply PBFT protocol to achieve consensus among edge computing nodes. A multilayer PBFT is proposed to solve the problem of scalability [28]. A tradeoff has been made between communication complexity and security, so as to derive the optimal structure of the blockchain-empowered HF spectrum management IoT. Specifically, the contributions of this article are summarized as follows:

(1) A blockchain-empowered HF spectrum management IoT is presented to motivate the personal HF devices to monitor and share the HF data for the first time. Massive personal HF devices are organized around the preselected nodes, i.e., 4G/5G base stations, to monitor and share the HF data, which bridges the gap between the collection of HF data and the inference of spectrum strategy

(2) A multilayer PBFT consensus protocol is employed to achieve the tradeoff between the scalability and security. The detailed operations of consensus process are illustrated to show how spectrum management agencies, 4G/5G base stations, and personal HF devices overcome the disadvantages of scalability while preserving the advantages of its throughput and energy efficiency

(3) Under the multilayer PBFT consensus, a tradeoff is formulated to obtain the optimal structure of HF spectrum management IoT, which jointly minimize the communication complexity and maintain an acceptable security performance

The rest of this article is organized as follows. Blockchain-empowered HF spectrum management framework and detailed operations are introduced in Section 2. In Section 3, a multilayer PBFT consensus is presented and the scalability of which is analyzed. In Section 4, the security of multilayer PBFT consensus is assessed to show the tradeoff between scalability and security. Scalability evaluation and security assessment are performed in Section 5, and conclusion has been made in Section 6.

2. Blockchain-Empowered Hf Spectrum Management

Blockchain is a decentralized database, a distributed infrastructure and computing paradigm, that uses block-chain structures to verify and store data and distributed consensus algorithms to generate and update data, asymmetric cryptography to ensure the security during the transmission and access, and smart contracts composed of automated script codes to program and manipulate data. In this section, a blockchain-empowered HF spectrum management IoT is proposed to timely and accurately obtain the changes of HF electromagnetic environment.

2.1. Overview of the Blockchain-Empowered HF Spectrum Management. Consensus in blockchain can be divided into two categories. The first category is represented by PoW, which is a computational processing called "mining"; i.e., a set of participants called miners need to solve a complex computation problem, i.e., proof-of-work puzzle, to confirm and secure the integrity and validity of transactions before adding the records into the blockchain. The security and privacy of the blockchain depend on the distributed consensus mechanism managed by these miners. However, in traditional public/permissionless blockchain (such as Bitcoin or Ethereum), the consensus is performed by all nodes (miners), which results in high cost and low throughput. To relieve the computation-intensive challenge of constructing HF blockchain, unlike existing works, in this article, a consortium blockchain is explored to empower the operation of HF spectrum management. Consortium blockchain is permissioned blockchain in which the consensus process is executed by preselected nodes. The consensus process of consortium blockchain is Practical Byzantine Fault Tolerance (PBFT), i.e., the second consensus protocol, with the throughput up to thousands TPS, which is essential to the blockchain empowered HF spectrum management, considering the HF spectrum data can be seen as a kind of big data [29]. Furthermore, the framework of private blockchain is also inappropriate for HF spectrum management, as the user of HF spectrum management is still increasing, while the number of user in private blockchain is fixed. Consequently, consortium blockchain is more suitable for HF spectrum management IoT.

In the proposed HF spectrum management IoT, the limited computing resource and energy supply become one of major problems, especially for the communication and computing load in the consensus-reaching process. Instead, edge computing provides necessary computing and communication resources for the blockchain-empowered IoT [30]. For example, base stations equipped with small data center can accept offloaded computation-intensive jobs from adjacent IoT devices [31]. Then, we leverage edge computing as an enabler to offload the computation-intensive puzzles to proximate edge computing nodes. Compared with traditional cloud computing [32, 33], edge computing brings network resources (e.g., computation power and storage space) closer to the users, which can effectively shorten the transmission delay and reduce the energy consumption [34]. The consortium blockchain-empowered HF spectrum management IoT is illustrated in Figure 3, which consists of the following major entities.

(i) ITU HF Agency: ITU HF agency is a trusted authority and operated by International Telecommunication Union (ITU). In this framework, ITU HF agency is responsible for initializing the entire HF spectrum management IoT, including the preselected edge computing nodes. ITU HF agency authenticate personal HF devices, and generates the public/private keys for them. Note that the ITU HF agency is offline for most of the time. It does not serve as a central controller and is not conflict with the distributed characteristics.

(ii) Computing nodes: computing nodes include an ITU HF server (cloud computing node) and edge computing nodes. The ITU HF server is operated by ITU and deployed at the same location of ITU HF agency. ITU HF server provides huge storage space and powerful computing power for inferring HF spectrum strategy in a centralized manner. Unlike ITU HF agency, the ITU HF server is online most of the time. 4G/5G base stations serve as edge computing nodes and provide relatively high computing power and large storage space for inferring HF spectrum strategy in a distributed manner. The storage space of edge computing nodes is mainly used to store HF spectrum data.

(iii) Personal HF devices: personal HF devices, i.e., HF amateurs, also called HAM, are distrusted widely over the world. Generally, personal HF devices are responsible for monitoring HF electromagnetic environment and uploading HF data to the proximate edge computing nodes. In addition, HF spectrum data and transaction data are asymmetric encrypted before uploading or transmission.

Additionally, in the proposed framework, the HF blockchain composes of HF blocks, including HF spectrum data and transaction data. For each edge computing node, it packs the HF spectrum data and transaction data every period of time to generate a preadded HF block and broadcasts this preadded HF block to the surrounding edge computing nodes. The object is to reach consensus on the preadded HF block through PBFT protocol.

In the proposed framework, ITU HF agency is designed for authenticating personal HF devices and allocating public/private keys. The ITU HF server is deployed at the same place of ITU HF agency and provides large space and powerful computing power for storing HF spectrum data and inferring HF spectrum strategies. 4G/5G base stations are deployed in the edge, with the aim of providing relative large space and powerful computing power. Personal HF devices are located at the end of the network. Then, ITU HF agency, base stations, and personal HF equipment constitute an end-edge-cloud structure and apply edge computing to operate the blockchain-empowered HF spectrum management IoT.

2.2. Detailed Operations of the Blockchain-Empowered HF Spectrum Management IoT. In the operation of HF spectrum management IoT, the process can be divided into 3 steps, i. e., the collection of HF spectrum data, the generation of HF blocks, and the trading of HF spectrum data. We elaborate the details as follows.

(1) Collection of HF spectrum data: in the 5G era, base stations can be regarded as the nodes with powerful computing power and massive storage space, which

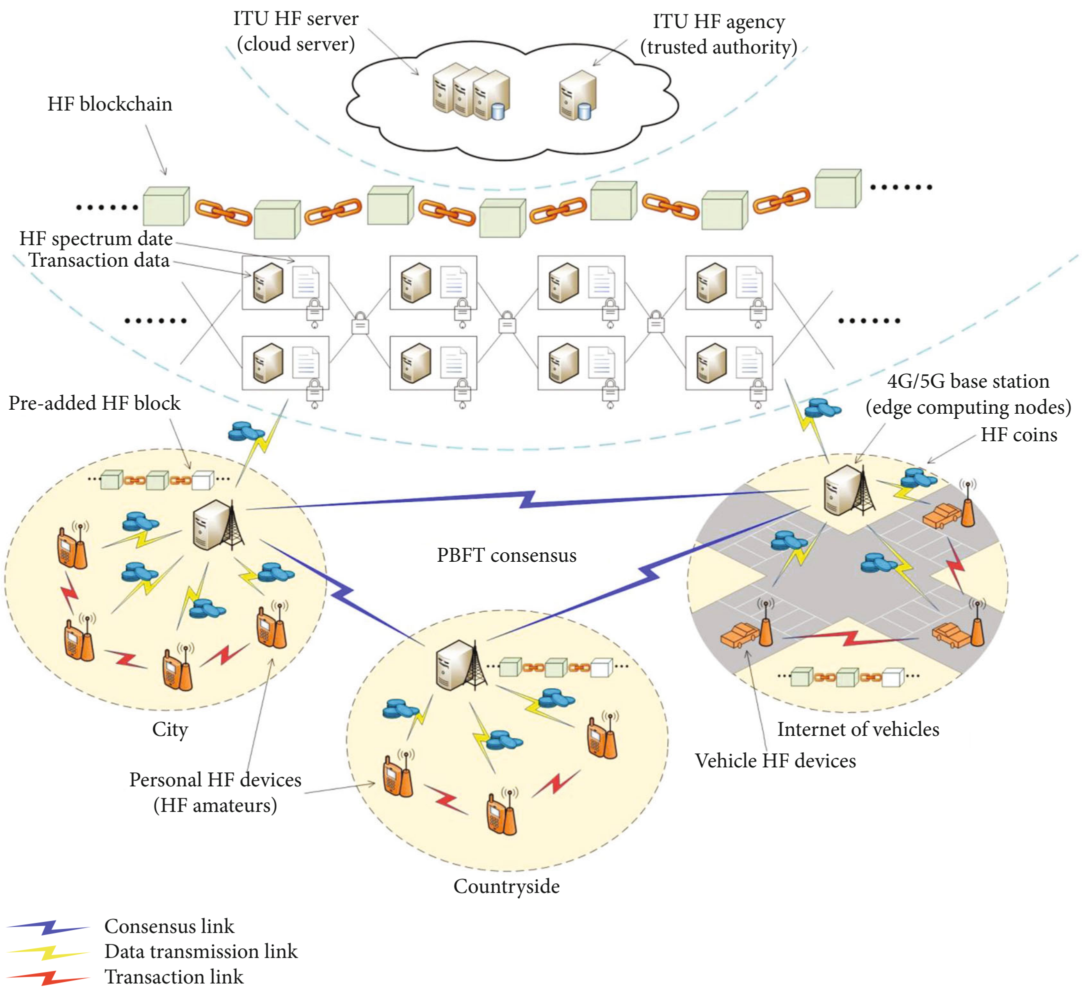

Figure 3: Consortium blockchain-empowered HF spectrum management IoT.

are deployed in a distributed manner. Here, each base station is assumed to manage surrounding HF electromagnetic environment. In ITU Spectrum Monitoring Handbook [35], 7 × 24-hour continuous spectrum monitoring is recognized sufficient to characterize the electromagnetic environment of a region. An HF electromagnetic environment is generally stable and partially dynamic. HF spectrum strategies of a certain region can be further inferred based on the collected HF spectrum data [36].

Personal HF devices can run an App that can be seen as smart contract, to automatically collect HF spectrum data. Personal HF devices upload the collected HF spectrum data to the proximate edge computing node for a period of time.

In the proposed framework, the automatically collected HF spectrum data has identical data structure that can be directly used by most personal HF devices. Intuitively, HF spectrum data is a kind of big data. If we use 1 byte to represent the HF spectrum data in a geospatial grid of 1000 m × 1000 m, and the frequency and time resolutions are assumed to 1 kHz and 100 ms, respectively. After one month, the total HF spectrum data size in the frequency band ranging from 2 to 30 MHz and a geospatial region of 100 km × 100 km can be as large as

$$\begin{aligned}&\frac{30\text{ days}}{\text{month}}\times\frac{24\text{ hours}}{\text{day}}\times\frac{3600\text{ seconds}}{\text{hour}}\times\frac{1\text{ hour}}{100\text{ ms}}\\&\quad\times\frac{28\text{ MHz}}{1\text{ kHz}}\times\frac{100\text{ km}\times100\text{ km}}{1\text{ km}\times1\text{ km}}\times1\text{ byte}\\&=7.257\times10^{15}\text{byte/month}\\&=7.257\times10^{3}\text{terabyte (TB)/month.}\end{aligned}\tag{1}$$

By comparison, Facebook, one of well-known big data examples, generates approximately 1.4×10^{4} TB per month. The size of HF spectrum data described above is approximately half of Facebook in the same duration. Moreover, the size of HF spectrum data will grow with the time duration and spatial scale, as well as the corresponding resolution in each dimension. It will cause heavy pressure to the ITU HF Server, needless to say under a centralized network framework.

Edge computing could efficiently processing HF spectrum data. Once the base station receives the HF spectrum

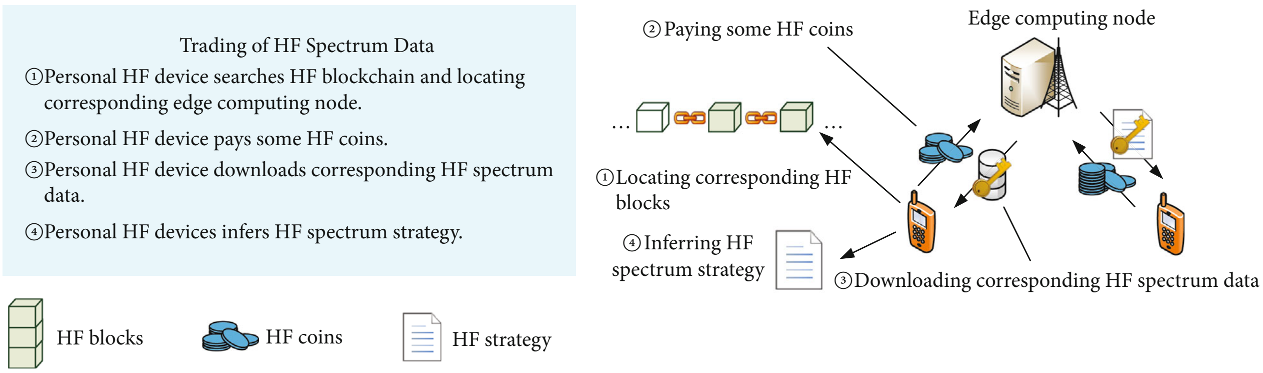
Trading of HF Spectrum Data
①Personal HF device searches HF blockchain and locating corresponding edge computing node.
②Personal HF device pays some HF coins.
③Personal HF device downloads corresponding HF spectrum data.
④Personal HF devices infers HF spectrum strategy.
②Paying some HF coins
Edge computing node
①Locating corresponding HF blocks
④Inferring HF spectrum strategy
③Downloading corresponding HF spectrum data
HF blocks
HF coins
HF strategy

Figure 4: Trading of HF spectrum data.

data and transaction data that uploaded by personal HF devices, it extracts the key information from the HF spectrum data and generates a digest. The main body of HF spectrum data is locally stored in edge computing nodes.

(2) Trading of HF spectrum data: the uploaded HF spectrum data is divided into the digest and main body of HF spectrum data. Edge computing nodes cooperate through PBFT protocol to reach consensus on uploaded HF spectrum data to form the preadded HF blockchain. HF blockchain is stored online and saved as a copy in each edge computing node. It should not take a large space to store the HF blockchain and not take long to download the HF blockchain, since the HF blockchain only saves the digest of HF spectrum data, which indicates the main body of HF spectrum data is stored in which edge computing node. When personal HF devices need to download the main body of HF spectrum data for inferring HF spectrum strategy, it locates the exactly base station, i.e., the edge computing node, that the main body of HF spectrum data is stored and connects the base station to download through high speed 4G/5G channels.

If massive personal HF devices, i.e., HF amateurs, share HF spectrum data, HF strategy is expected to change from noncooperative frequency competition accompanied with power competition to cooperative competition and sharing. It will gradually reduce the HF background noise and improves HF electromagnetic environment. Consequently, personal HF devices need to make use of HF spectrum data to infer HF spectrum strategy. The above process can be concluded into four steps, as shown in Figure 4.

(i) Personal HF device searches HF blockchain and locates corresponding edge computing node through the digest that stored in HF block

(ii) Personal HF device pays some HF coins

(iii) Personal HF device downloads corresponding HF spectrum data

(iv) Personal HF device infers HF spectrum strategy according to the downloaded HF spectrum data

In the third step, when personal HF device needs to download corresponding HF spectrum data, there are two options:

(1) *Option 1: the main body of HF spectrum data is stored in* ***local*** *edge computing node.* Personal HF device pays some HF coins to local edge computing node and downloads corresponding HF spectrum data. Edge computing node receives minority HF coin and transfers majority HF coin to personal HF devices that provide HF spectrum data.

(2) *Option 2: the main body of HF spectrum data is stored in* ***foreign*** *edge computing node.* Personal HF device sends request to foreign edge computing node through local edge computing node and pay some HF coins beforehand. Foreign edge computing node transmits corresponding HF spectrum data through high-speed network, e.g., 4G/5G network, to the local edge computing node. Then, HF coins are transferred to personal HF devices that provide HF spectrum data.

In the fourth step, when personal HF device infers HF spectrum strategy according to the downloaded HF spectrum data, there are also two options.

(1) *Option 1: personal HF device infers HF spectrum strategy locally.* If personal HF device has enough computing power and storage space, it could infer HF spectrum strategy locally.

(2) *Option 2: local edge computing node assist personal HF device inferring HF spectrum strategy.* If personal HF devices do not have enough computing power, it could send the requirements to local edge computing node and pay some HF coins. With relative sufficient computing power and large storage space, local edge computing node could quickly infer the HF spectrum strategy and then transmit the results back to personal HF device.

Moreover, the security during the transmission is guaranteed by asymmetric encryption [37]. For instance, when personal HF device A transmits HF spectrum data Data_A to edge computing node B, device A downloads the public key of node B and encrypts Data_A:

$$\mathrm{Record}_{\mathrm{Data}} = \mathrm{RSA}\left(\mathrm{Data}_A, \mathrm{key}_B^P\right). \tag{2}$$

$\mathrm{Record}_{\mathrm{Data}_A}$ is the encrypted HF spectrum data, RSA is the asymmetric encryption algorithm [38], and key_B^P is the public key of edge computing node B. When edge computing node B receives $\mathrm{Record}_{\mathrm{Data}_A}$, it decrypts with his private key key_B^P and obtains the HF spectrum data:

$$\mathrm{Data}_\mathrm{A} = \mathrm{RSA}\left(\mathrm{Record}_{\mathrm{Data}_A}, \mathrm{key}_B^S\right). \tag{3}$$

Secondly, personal HF devices can check whether HF spectrum data has been tampered. When personal HF device C uploads HF spectrum data Data_C to edge computing node, device C first generates the digest of Data_C through Hash algorithm [39]:

$$\mathrm{Digest}_{\mathrm{Data}_C} = \mathrm{Hash}\left(\mathrm{Data}_C, \mathrm{key}_C^P\right). \tag{4}$$

Device C encrypts the digest $\mathrm{Digest}_{\mathrm{Data}_C}$ and generates digital signature:

$$\mathrm{Sign}_{\mathrm{Digest}} = \mathrm{RSA}\left(\mathrm{Digest}_{\mathrm{Data}}, \mathrm{key}_C^S\right). \tag{5}$$

Device C appends $\mathrm{Sign}_{\mathrm{Digest}}$ to the end of Data_C and uploads Data_C to edge computing node. Then, other personal HF devices can decrypt $\mathrm{Sign}_{\mathrm{Digest}}$ with the public key of device $C\mathrm{key}_B^P$ and obtain $\mathrm{Digest}_{\mathrm{Data}_C}$:

$$\mathrm{Digest}_{\mathrm{Data}_C} = \mathrm{RSA}\left(\mathrm{Sign}_{\mathrm{Digest}}, \mathrm{key}_C^P\right). \tag{6}$$

Other personal HF devices apply Hash Algorithm to Data_C and obtain the digest $\mathrm{Digest}'_{\mathrm{Data}_C}$. Then, other personal HF devices compare $\mathrm{Digest}'_{\mathrm{Data}_C}$ with $\mathrm{Digest}_{\mathrm{Data}_C}$; if $\mathrm{Digest}'_{\mathrm{Data}_C} = \mathrm{Digest}_{\mathrm{Data}_C}$, it indicates that the HF spectrum data has not been tampered.

(3) Generation of HF Block: when the accumulated HF spectrum data of a certain region exceeds 7 × 24 hours, the base station iteratively discards redundant HF spectrum data to make it light-weighting. Once the accumulated HF spectrum data reach a certain amount, e.g., 24 hours, the edge computing node extracts the key information and generates a digest and packs with the transaction data to form the preadded HF block; then, broadcasts it to surrounding edge computing nodes and seeks for consensus. The preadded HF block contains a unique serial number, duration/spectrum range/monitoring location, time/frequency/spatial resolution, data size, and storage location (i.e., the location in the base station). The size of the preadded HF block is relatively small. Note that the preadded HF blocks are asymmetric encrypted (e.g., SHA-256 algorithm) by the private key of the edge computing node. When these edge computing nodes reach consensus about the preadded HF block, it will be appended at the end of the HF blockchain and becomes an official block. Note that other personal HF devices could decrypt HF block with the public key of edge computing node that uploaded online and easily obtain the location of demanding HF spectrum data through the digest of HF spectrum data. When the preadded HF block becomes an official one, the personal HF devices that provide the HF spectrum data will get some HF coins automatically as rewards. As stated above, the strategy that the HF spectrum data been divided into digest and main body and been stored in HF blockchain and edge computing node, respectively, not only greatly reduces the traffic load but also saves the computing power and energy consumed in the consensus process.

The structure of HF block is illustrated in Figure 5, including the digest of HF spectrum data, transaction data, timestamp, and the hash value of the previous block. HF blocks are linked end by end according to the timestamp, which record the time of consensus-reached. The subblocks are organized in the structure of Merkel Tree. Note that HF blocks only contain the digest of HF spectrum data, and the main body is stored at corresponding edge computing node. Similar to Bitcoin, the ITU HF server regularly releases HF coins for their contributions of collecting HF spectrum data. When surrounding edge computing nodes reach consensus on the preadded HF block, the HF block will be appended to the end of HF blockchain, personal HF devices that provide HF spectrum data and edge computing nodes participating in consensus both will be rewarded some HF coins. HF coins can be used to purchase additional HF bandwidth and additional HF spectrum usage rights.

3. Scalability of Multilayer PBFT Consensus

3.1. Multilayer PBFT Consensus. Before introducing the multilayer PBFT, we first review the single-layer PBFT protocol. Practical Byzantine Fault Tolerance was first presented to solve the malicious attacks in Byzantine General Problem [25, 26]. Figure 6 shows the flow chart of the single-layer PBFT; one primary node (replica 0) and three replicas work together to carry consensus process forward. The whole consensus process generally includes 5 steps, i.e., *request*, *pre-prepare*, *prepare*, *commit*, and *reply*. PBFT consensus is triggered by a client sending a *request* message to the primary node. Then, primary node broadcasts a *preprepare* message to other replicas. All replicas, including primary node, send messages to each other for checking the validity of the received

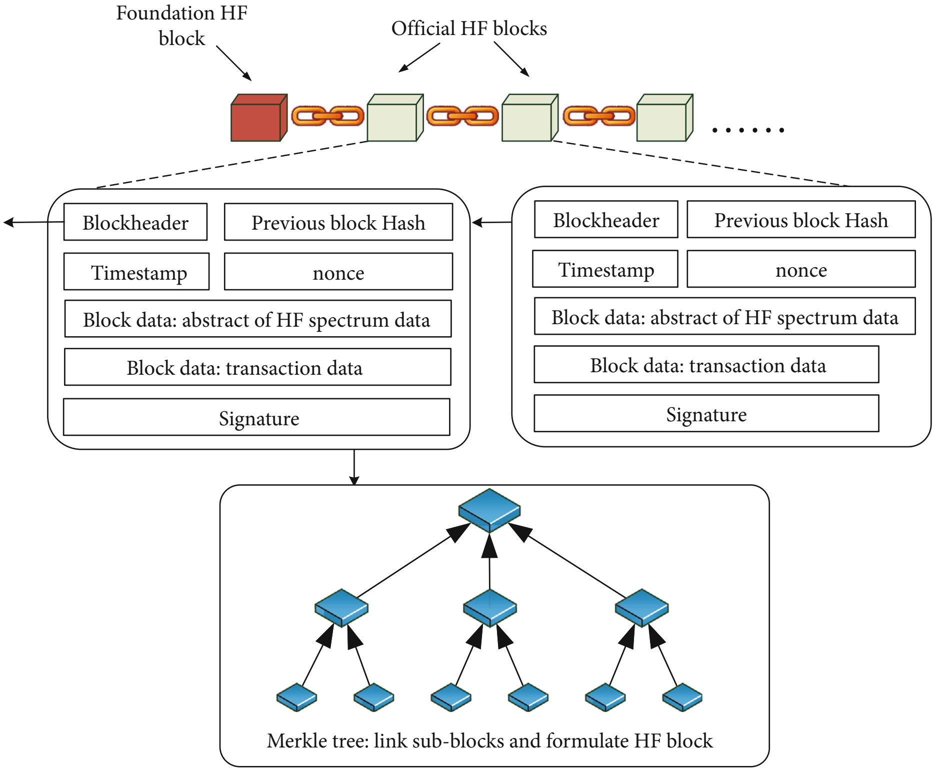
Foundation HF block
Official HF blocks
......
Blockheader
Previous block Hash
Timestamp
nonce
Block data: abstract of HF spectrum data
Block data: transaction data
Signature
Blockheader
Previous block Hash
Timestamp
nonce
Block data: abstract of HF spectrum data
Block data: transaction data
Signature
Merkle tree: link sub-blocks and formulate HF block

Figure 5: Structure of HF blocks.

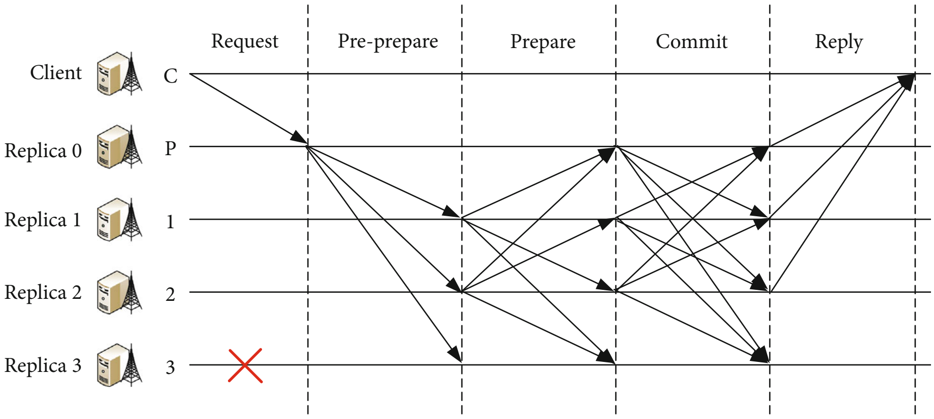

Figure 6: Single-layer PBFT consensus.

messages in *prepare* and *commit* steps. Finally, if an agreement is achieved in *reply* step, the preadded HF block will be added to end of HF blockchain.

PBFT consensus is designed to tolerate f faulty nodes with a total number of $3f + 1$ replicas [25, 26]. Therefore, the security threshold of the single-layer PBFT can be seen as f, given a total number of $3f + 1$ replicas participating the consensus process. From Figure 6, we can see that PBFT is a communication-intensive consensus process. Given the total number N, the single-layer PBFT requires $O(N^2)$ times internode communications to reach consensus. Obviously, the communication complexity will become increasingly unaffordable with the increasing of nodes. It is also the reason for the poor scalability of the PBFT consensus.

Next, a multilayer PFBT is applied to bring down the communication complexity to an acceptable level when the number of nodes sharply increases. Generally speaking, the core idea of the multilayer PBFT consensus is successively inserting a PBFT consensus between *commit* and *reply* steps to reduce the whole communication complexity [28]. The consensus process of the second layer is inserted after the *commit* step; after that, each node has generated his own judgment about whether the preadded HF block is valid. At this time, whether the PBFT consensus of the second layer is reached only affects the *reply* message of one replica in the first layer and will not affect the *reply* message of other replicas. As an example, Figure 7 illustrates the process of two-layer PBFT, Replica 3 is assumed to be a malicious

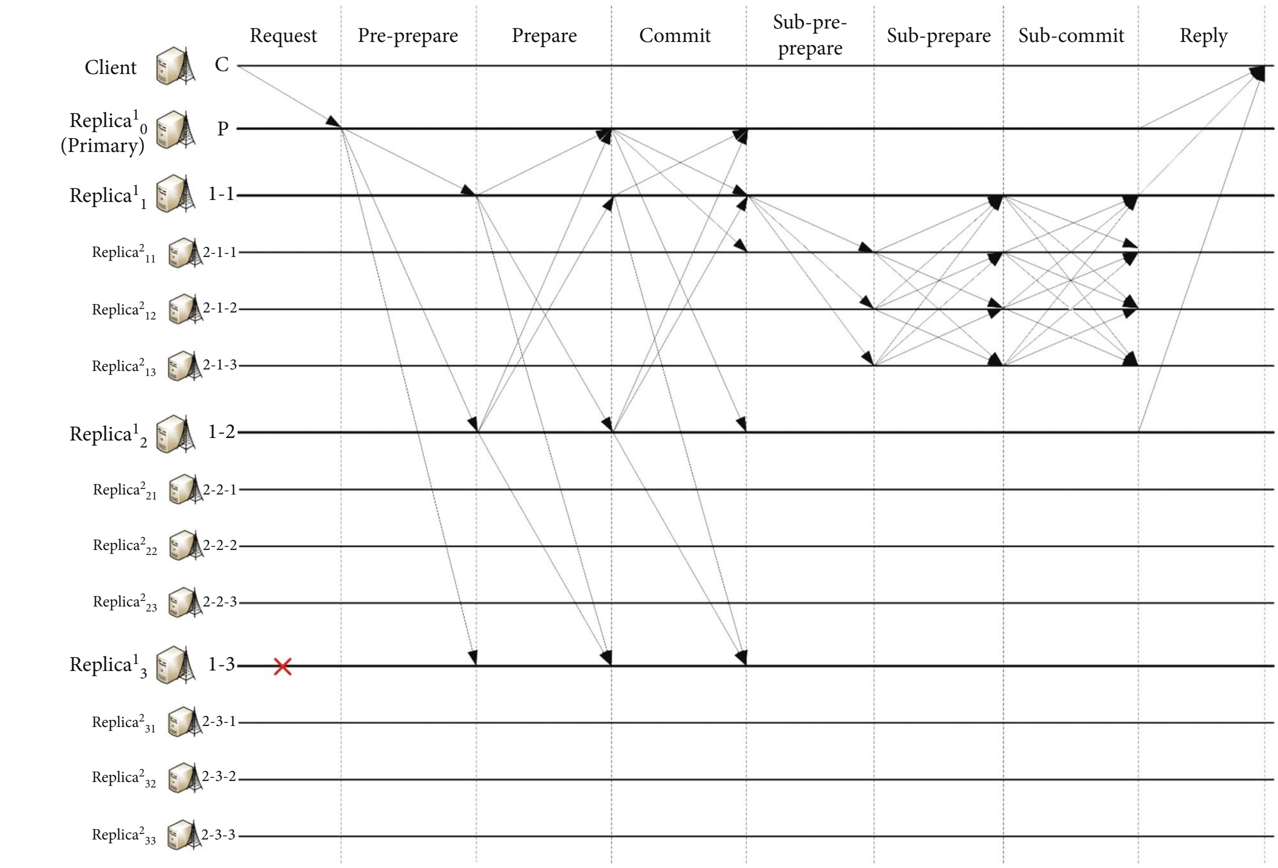

Figure 7: Multilayer PBFT consensus.

node, which is down during the whole consensus process, where the first layer contains $m_1 = 3$ replicas, and each serves as a primary node (Replica$^1_0$) with $m_2 = 3$ sublayer replicas in the second layer. Then, the total number of nodes in the double-layer PBFT consensus is $N = 1 + m_1 + m_1 m_2 = 13$. The pseudocodes of Primary, Replica^1_i, and Replica^2_i for two-layer PBFT consensus are described in Algorithms 1, 2, and 3, respectively. Note that we assume each group in the second layer contain the same number of nodes. A previous study has derived the communication complexity of a double-layer PBFT system [27].

3.2. Scalability of Multilayer PBFT Consensus. **Therem 1.** For a double-layer PBFT consensus process with m_1 replicas in the first layer and m_2 sublayer replicas in

$$C_2 = (m_1 + 1)^2 + m_1 (m_2 + 1)^2. \tag{7}$$

Then, what is the optimal network structure that achieve the lowest communication complexity for the double-layer PBFT? The optimization problem can be formulated as

$$\begin{aligned} \text{Problem 1}: \quad & \min C = \min_{m,n} (m_1 + 1)^2 + m_1 (m_2 + 1)^2 \\ & \text{s.t.} \quad m_1 \geq 4, m_2 \geq 3 \\ & m_1, m_2 \in Z. \end{aligned} \tag{8}$$

As $N = 1 + m_1 + m_1 m_2$ is total number of nodes and the constrains are $m_1 \geq 4$, $m_2 \geq 3$, Problem 1 is a quadratic integer programming problem and is nonconvex. Substituting $m = N - 1/n + 1$ into Equation (8), we have

$$\begin{aligned} \text{Problem 2}: \quad & \min C = \min_{m,n} (m_1 + 1)^2 + m_1 (m_2 + 1)^2 \\ & \text{s.t.} \quad m_1 \geq 4, m_2 \geq 3 \\ & m_1, m_2 \in Z \\ & N = 1 + m_1 + m_1 m_2. \end{aligned} \tag{9}$$

It is an integer programming problem and NP-hard problem. Considering that the feasible solution domain is not very large under the constraint $N = 1 + m_1 + m_1 m_2$, the optimal network structure can be solved by exhaustive searching.

Consider the case of multilayer PBFT, the communication complexity can be derived accordingly.

Therem 2. For a double-layer PBFT consensus process with m_1 replicas in the first layer and m_2 sublayer replicas in each subgroup, the communication complexity C_2 to reach consensus is

$$C_n = \sum_{i=1}^{n} m_{i-2} m_{i-1} (m_i + 1)^2. \tag{10}$$

```
while valid $request^1$ received=True do
    if client identity authenticated=True then
        $m \leftarrow n$
        multicasts $pre\text{–}prepare^1$ to $Primary$
    end if
end while
while valid $prepare^1$ received=True do
    if number of valid $prepare^1 \geq 2f$ then
        $prepare^1$=valid
        multicast $commit^1$ to $\mathrm{Replica}_i^1$
    end if
end while
while valid $commit^1$ received=True do
    if number of valid $commit^1 \geq 2f$ then
        $commit^1$=valid
    end if
end while
while valid $reply^1$ received=True do
    if number of valid $reply^1 \geq 2f$ then
        reply client with $reply^1$
    end if
end while
```

Algorithm 1: Two-layer PBFT consensus: primary.

```
while valid $pre\text{-}prepare^1$ received=True do
    multicasts $prepare^1$ to $\mathrm{Replica}_i^1$
end while
while valid $prepare^1$ received=True do
    if number of valid $prepare^1 \geq 2f$ then
        $prepare^1$=valid
        multicasts $commit^1$ to $\mathrm{Replica}_i^1$
    end if
end while
while valid $commit^1$ received=True do
    if number of valid $commit^1 \geq 2f$ then
        $commit^1$=valid
        multicasts $sub\text{-}pre\text{-}prepare^2$ to $\mathrm{Replica}_i^2$
    end if
end while
while valid $sub\text{-}prepare^2$ received=True do
    if number of valid $sub\text{-}prepare^2 \geq 2f$ then
        $sub\text{-}prepare^2$=valid
        reply primary with $reply^1$
    end if
end while
while valid $sub\text{-}commit^2$ received=True do
    if number of valid $sub\text{-}commit^2 \geq$ 2f then
        reply client with $reply^1$
    end if
end while
```

Algorithm 2: Two-layer PBFT consensus: $\mathrm{Replica}_i^1$.

```
while valid $sub\text{-}pre\text{-}prepare^2$ received=True do
    multicasts $sub\text{-}prepare^2$ to $\mathrm{Replica}_i^2$ in the same
    consensus group
end while
while valid $sub\text{-}prepare^2$ received=True do
    if number of valid $sub\text{-}prepare^2 \geq 2f$ then
        $sub\text{-}prepare^2$=valid
        multicasts $sub\text{-}commit^2$ to $\mathrm{Replica}_i^2$ in the same
        consensus group
    end if
end while
while valid $sub\text{-}commit^2$ received=True do
    if number of valid $sub\text{-}commit^2 \geq 2f$ then
        $sub\text{-}commit^2$=valid
        send $sub\text{-}reply^2$ to group leader
    end if
end while
```

Algorithm 3: Two-layer PBFT consensus: $\mathrm{Replica}_i^2$.

Based on the above analysis, we infer that, given the total number of edge computing nodes N, the minimum communication complexity can be achieved when PBFT consensus has the most layers. The PBFT consensus contains the most layers, meaning that each group only contains the least nodes, i.e., 3 nodes. At this time, PBFT consensus has the most layers $X_{\max}$:

$$X_{\max} = \lfloor \log_3(2N+1) \rfloor - 1. \tag{11}$$

Then, the total number of nodes in PBFT system N can be written as

$$N = 1 + 3 + 3^2 + \cdots + 3^{X_{\max}}. \tag{12}$$

Thus, the lowest communication complexity can be expressed as

$$C_{X_{\max}} = \sum_{i=1}^{X_{\max}} 3^{i-1}(3+1)^2 = 16 \times \frac{3^{X_{\max}} - 1}{3 - 1} = \frac{16N - 16}{3}. \tag{13}$$

It can be seen that the communication complexity C has a linear relationship with the number of edge computing nodes N. Intuitively, it is impossible to reduce the communication complexity without any cost. We can see in the following that the cost is the system security. Consequently, when we increase the layers of PBFT consensus to reduce the communication complexity, the security of PBFT consensus will be degraded at the same time. In order to maintain a basic security performance when we reduce the communication complexity, it is necessary to make a tradeoff between communication complexity and system security. We discuss it in the following subsection.

4. Security Analysis of Multilayer PBFT Consensus

4.1. Security of Double-Layer PBFT Consensus. Security of double-layer PBFT is discussed firstly. Assume that the 1st layer contain m_1 edge computing nodes, and each group in the 2nd layer contains m_2 nodes. The double-layer PBFT can reach consensus under following conditions: the summation of the number of malicious edge computing node i_1 (name as malicious nodes hereinafter) in the 1st layer and the number of groups j_2 of the 2nd layer that does not reach consensus (the head node is normal) should be less than or equal to $\lfloor m_1/3 \rfloor$, i.e., $0 \leq i_1 + j_2 \leq \lfloor m_1/3 \rfloor$. The 1st layer contains i_1 malicious nodes indicating that there are i groups that cannot reach consensus and there are j_2 groups failing to reach consensus in the 2nd layer meaning the head nodes of these groups are treated as malicious nodes.

If there are i_1 malicious nodes in the 1st layer, it means the number of groups that fails to reach consensus is no more than bm1 $\lfloor m_1/3 \rfloor - i_1$, i.e., $0 \leq j_2 \leq \lfloor m_1/3 \rfloor - i_1$. That is to say, two necessary conditions constitute the sufficient condition of consensus-reached. In the premise of the 1st layer contains no more of $\lfloor m_1/3 \rfloor$ malicious nodes, the 2nd layer contains no more than $\lfloor m_1/3 \rfloor - i_1$ groups that fail to reach consensus; then the system can reach consensus. We have the following definitions.

(i) Event A1: the 1st layer contains no more than $\lfloor m_1/3 \rfloor$ malicious nodes.

(ii) Event B2: the 2nd layer contains no more than $\lfloor m_1/3 \rfloor - i_1$ group that fails to reach consensus.

$P_{C_2} = P(A_1) \times P(B_2)$, P_{C_2} is the probability of consensus-reached for the double-layer PBFT. We have

$$
\begin{aligned}
P(A_1) &= \sum_{i_1=0}^{\lfloor m_1/3 \rfloor} C_{m_1}^{i_1} P_f^{i_1} \left(1 - P_f\right)^{(m_1 - i_1)}, \\
P(B_2) &= \sum_{j_2=0}^{\lfloor m_1/3 \rfloor - i_1} C_{m_1 - i_1}^{j_2} P_{g_2}^{j_2} \left(1 - P_{g_2}\right)^{(m_1 - i_1 - j_2)},
\end{aligned}
\tag{14}
$$

where P_f is the probability that the nodes of the 1st layer are malicious and P_{g_2} is the probability that the group of the 2nd layer fails to reach consensus, which is derived as follows.

If $\lfloor m_2/3 \rfloor + 1 \leq i_2 \leq m_2$ (the head node of the group in the 2nd layer is normal), the group fails to reach consensus. P_{g_2} can be written as

$$
P_{g_2} = \sum_{i_2=\lfloor m_2/3 \rfloor + 1}^{m_2} C_{m_2}^{i_2} P_f^{i_2} \left(1 - P_f\right)^{(m_2 - i_2)}. \tag{15}
$$

The probability of consensus-reached for the double-layer PBFT is derived as

$$
\begin{aligned}
P_{C_2} = P(A_1) \times P(B_2) = &\sum_{i_1=0}^{\lfloor m_1/3 \rfloor} C_{m_1}^{i_1} P_f^{i_1} \left(1 - P_f\right)^{(m_1 - i_1)} \\
&\cdot \sum_{j_2=0}^{\lfloor m_1/3 \rfloor - i_1} C_{m_1 - i_1}^{j_2} P_{g_2}^{j_2} \left(1 - P_{g_2}\right)^{(m_1 - i_1 - j_2)}.
\end{aligned}
\tag{16}
$$

4.2. Security of Multilayer PBFT Consensus. Next, we analyze the security performance of the three-layer PBFT and further derive the security performance of X-layer PBFT. Please note that the derivation of security performance of the three-layer PBFT has some differences with that of the double-layer PBFT. The number of nodes in the 1st layer is assumed to be m_1, and the numbers of nodes in the group of 2nd and 3rd layer are denoted as m_2 and m_3, respectively. The number of malicious nodes in the 1st layer is assumed to be i_1, and the numbers of malicious nodes in the group of 2nd and 3rd layer are denoted as i_2 and i_3, respectively.

The numbers of groups that do not reach consensus in the 2nd/3rd layer are assumed to be j_2 and j_3 (the head node is normal). We can infer that the consensus is reached or not is determined by the number of malicious node in the 1st layer i_1 and the number of groups that does not reach consensus in the 2nd layer j_2, i.e., $0 \leq i_1 + j_2 \leq \lfloor m_1/3 \rfloor$. Let $P(A_1)$ denote the probability that the number of malicious nodes in the 1st layer i_1 less than $\lfloor m_1/3 \rfloor$ and $P(B_2)$ represent the probability that the number of groups have not reached consensus in the 2nd layer j_2 less than $0 \leq i_1 + j_2 \leq \lfloor m_1/3 \rfloor - i_1$. Then, we have $P_{C_3} = P(A_1) \times P(B_2)$, where P_{C_3} is the probability of three-layer PBFT reaching consensus. We can derive

$$
\begin{aligned}
P(A_1) &= \sum_{i_1=0}^{\lfloor m_1/3 \rfloor} C_{m_1}^{i_1} P_f^{i_1} \left(1 - P_f\right)^{(m_1 - i_1)}, \\
P(B_2) &= \sum_{j_2=0}^{\lfloor m_1/3 \rfloor - i_1} C_{m_1 - i_1}^{j_2} P_{g_2}^{j_2} \left(1 - P_{g_2}\right)^{(m_1 - i_1 - j_2)},
\end{aligned}
\tag{17}
$$

where P_{g_2} is the probability that the group in the 2nd layer fails to reach consensus. Given the head node is normal, how does the group fail to reach consensus? Considering that there are m_2 nodes and i_2 malicious nodes in the 2nd layer and there are j_3 groups in the 3rd layer failing to reach consensus, when $\lfloor m_2/3 \rfloor + 1 \leq i_2 + j_3 \leq m_2$, the 2nd layer cannot reach consensus. We have

$$
P_{g_2} = P(A_2) \times P\left(\overline{B_3}\right) + P\left(\overline{A_2}\right) = 1 - P(A_2)P(B_3). \tag{18}
$$

Let $P(\overline{A_2})$ denote the probability that $i_2 \geq \lfloor m_2/3 \rfloor + 1$ and $\overline{P(B_3)}$ denote the probability that $j_3 \geq \lfloor m_2/3 \rfloor + 1 - i_2$. Equation (18) indicates that, except for $i_2 \leq \lfloor m_2/3 \rfloor$ and $j_3 \leq \lfloor m_2/3 \rfloor - i_2$, the groups in the 2nd layer always cannot reach consensus. We have

$$
\begin{aligned}
P(A_2) &= \sum_{i_2=0}^{\lfloor m_2/3 \rfloor} C_{m_2}^{i_2} P_f^{i_2} \left(1 - P_f\right)^{(m_2 - i_2)}, \\
P(B_3) &= \sum_{j_3=0}^{\lfloor m_2/3 \rfloor - i_2} C_{m_2 - i_2}^{j_3} P_{g_3}^{j_3} \left(1 - P_{g_3}\right)^{(m_2 - i_2 - j_3)},
\end{aligned}
\tag{19}
$$

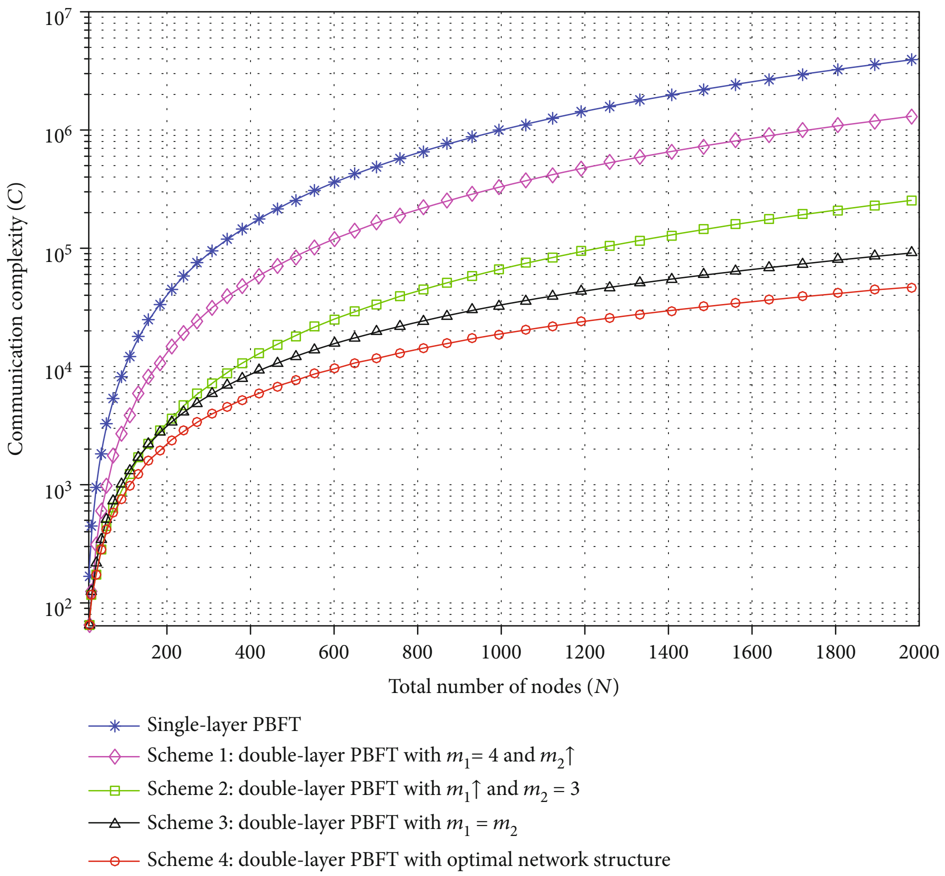

Figure 8: Communication complexity of single-layer and double-layer PBFT.

where P_{g_3} is the probability that the group in the 3rd layer fails to reach consensus. Similarly, we have

$$P_{g_3} = \sum_{i_3=\lfloor m_3/3\rfloor+1}^{m_3} C_{m_3}^{i_3} P_f^{i_3}\left(1-P_f\right)^{(m_3-i_3)}, \tag{20}$$

indicating that the group in the 3rd layer cannot reach consensus when $\lfloor m_3/3\rfloor + 1 \le i_3 \le m_3$.

Substituting (17)–(20) into $P_{C_3} = P(A_1)\times P(B_2)$, we can derive the probability of consensus-reached of three-layer PBFT. Then, the probability of consensus-reached of the X -layer PBFT can be derived as follows.

The numbers of nodes in the 1~X-th layer are assumed to be $m_1, \cdots, m_k, \cdots, m_X$. The numbers of malicious nodes in the 1~X-th layer are assumed to be $i_1, \cdots, i_k, \cdots, i_X$. The numbers of groups that do not reach consensus in the 2~X layer are denoted as $j_2, \cdots, j_k, \cdots, j_X$ (the head node is normal). The security of X-layer PBFT is

$$P_{C_X} = P(A_1)\times P(B_2) = \sum_{i_1=0}^{\lfloor m_1/3\rfloor} C_{m_1}^{i_1} P_f^{i_1}\left(1-P_f\right)^{(m_1-i_1)} \times \sum_{j_2=0}^{\lfloor m_1/3\rfloor-i_1} C_{m_1-i_1}^{j_2} P_{g_k}^{j_2}\left(1-P_{g_k}\right)^{(m_1-i_1-j_2)},, \tag{21}$$

where P_{g_k} is given by

$$P_{g_k} = \begin{cases} \displaystyle\sum_{i_2=\lfloor m_2/3\rfloor+1}^{m_2} C_{m_2}^{i_2} P_f^{i_2}\left(1-P_f\right)^{(m_2-i_2)}, & X=2, k=2, \\ \displaystyle\sum_{i_k=0}^{\lfloor m_k/3\rfloor} C_{m_k}^{i_k} P_f^{i_k}\left(1-P_f\right)^{(m_k-i_k)} \times \sum_{j_{k+1}=\lfloor m_k/3\rfloor+1-i_k}^{m_k} C_{m_k-i_k}^{j_{k+1}} P_{g_{k+1}}^{j_{k+1}}\left(1-P_{g_{k+1}}\right)^{(m_k-i_k-j_{k+1})} + \left(1-\sum_{i_k=0}^{\lfloor m_k/3\rfloor} C_{m_k}^{i_k} P_f^{i_k}\left(1-P_f\right)^{(m_k-i_k)}\right), & X\ge 3, 2\le k\le X-1, \\ \displaystyle\sum_{i_X=\lfloor m_X/3\rfloor+1}^{m_X} C_{m_X}^{i_X} P_f^{i_X}\left(1-P_f\right)^{(m_X-i_X)}, & X\ge 3, k=X. \end{cases} \tag{22}$$

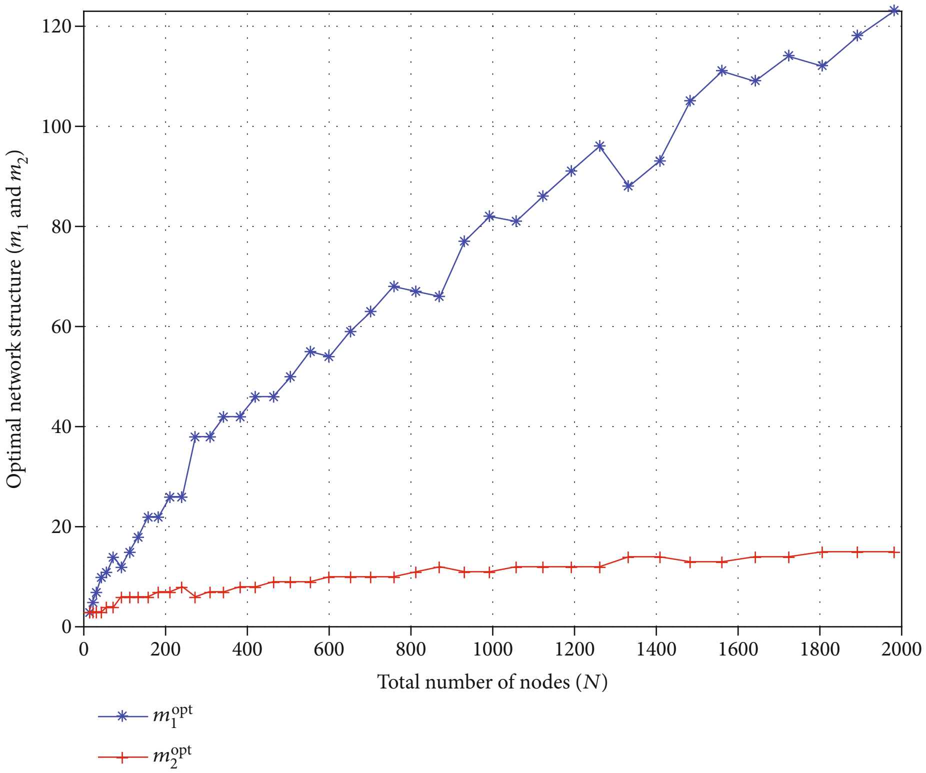

Figure 9: Optimal network structure of double-layer PBFT.

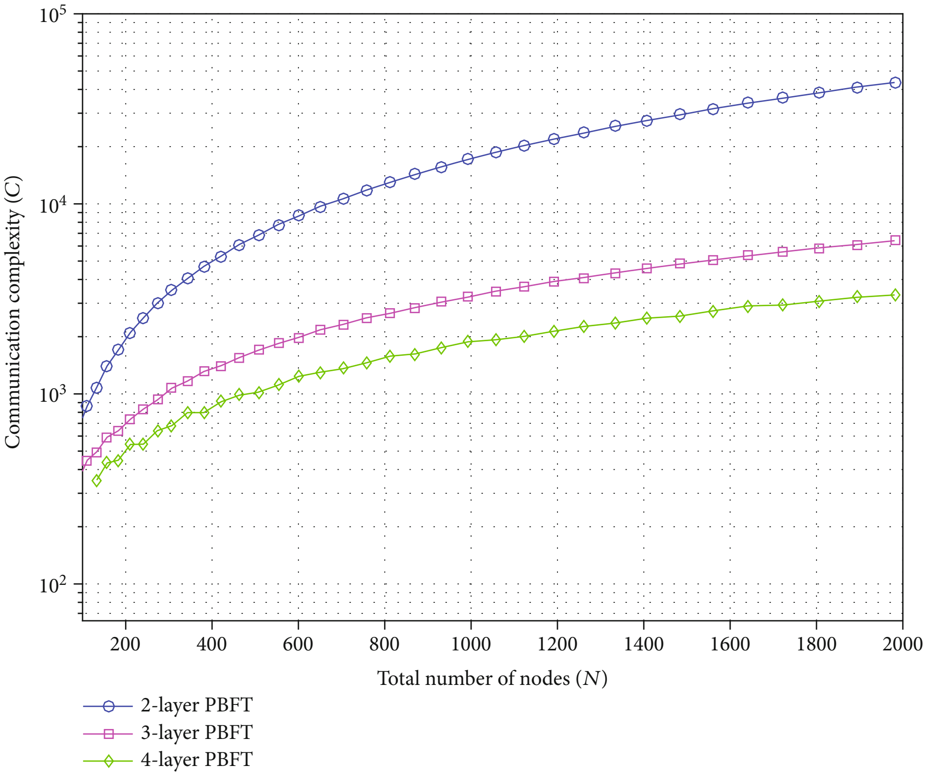

Figure 10: Communication complexity comparison of multi-layer PBFT under optimal network structure.

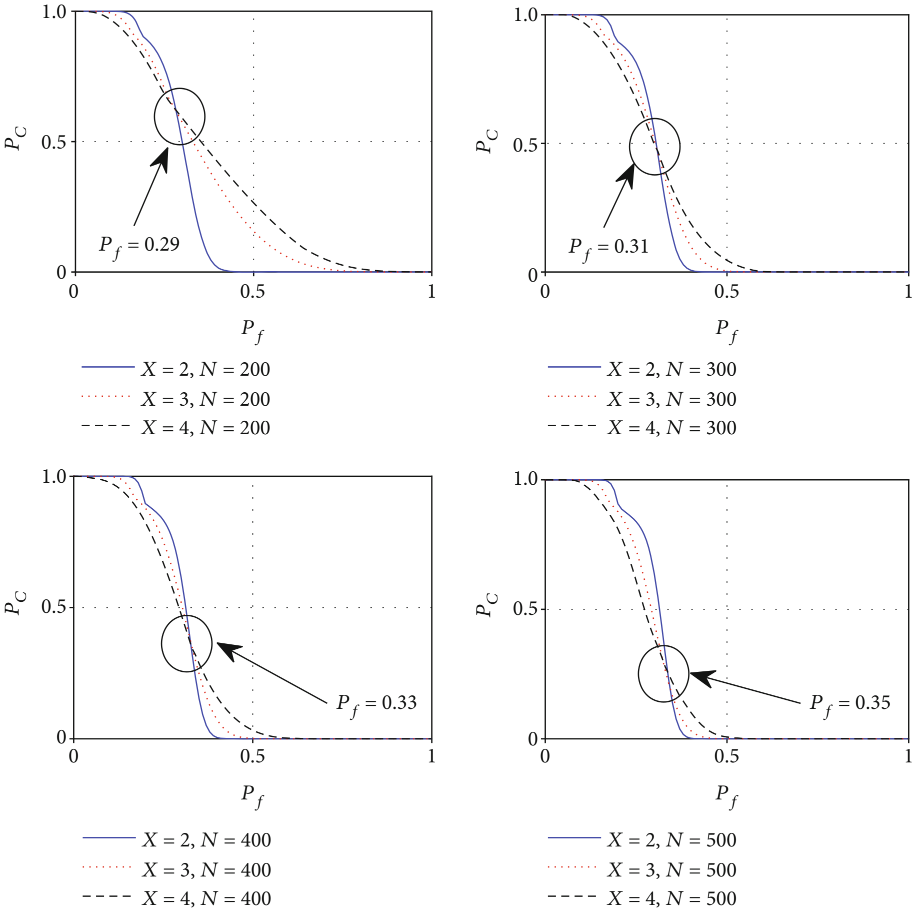

Figure 11: Security performance of multi-layer PBFT under given number of nodes.

5. Scalability Evaluations and Security Assessments

In this section, a scalability evaluation of the proposed multilayer PBFT consensus is firstly given. After that, some security assessments are provided to show that we should reasonably design the structure of multilayer PBFT consensus for the blockchain-empowered HF spectrum management, in order to tradeoff between scalability and security.

5.1. Scalability Evaluations of Multilayer PBFT Consensus. In this subsection, the scalability performance of multilayer PBFT consensus is demonstrated. Intuitively, the poor scalability of the PBFT consensus mainly comes from the sharply increasing of communication complexity as the number of nodes increases. Consequently, the scalability of the PBFT consensus will be greatly improved with the reduction of communication complexity.

In *Evaluation 1*, four schemes are demonstrated in Figure 8 to show the improvement in communication complexity of double-layer PBFT. In *Scheme 1*, double-layer PBFT, m_1 keeps the minimum ($m_1 = 4$, include one head node) and m_2 increases linearly. In *Scheme 2*, double-layer PBFT, m_1 increases linearly and m_2 keeps the minimum ($m_2 = 3$). In *Scheme 3*, double-layer PBFT with $m_1 = m_2$. In *Scheme 4*, double-layer PBFT with an optimal network structure achieves the lowest communication complexity. Evaluations are performed under the constraint of $N = 1 + m_1 + m_1 m_2$. Obviously, the communication complexity of double-layer PBFT is significantly reduced compared with that of single-layer PBFT. Secondly, the communication complexity of *Scheme 2* further reduced compared with that of *Scheme 1*, indicating that we should first increase the nodes in the 1st layer, i.e., m_1, rather than the nodes in each group of the 2nd layer, i.e., m_2. Thirdly, compared with the communication complexity of single-layer PBFT, the communication complexities of *Scheme 3* and *Scheme 4* reduce by at least 1 order of magnitude. Fourthly, the communication complexity of *Scheme 3* is relatively close to that of *Scheme 4*, indicating that $m_1 = m_2$ is a suboptimal solution when the optimal network structure cannot be obtained.

The optimal network structure of double-layer PBFT when the lowest communication complexity achieved is shown in Figure 9. It can be seen that as the total number of nodes increases, the number of nodes in the 1st layer, i.e., m_1^{opt}, increases almost linearly, while the number of nodes in each group of the 2nd layer, i.e., m_2^{opt}, hardly increases. From (6), we can see that the communication complexity of double-layer PBFT, i.e., C_2, has a linear relationship with m_1^2 and $m_1 m_2^2$. Therefore, for the double-layer PBFT, when

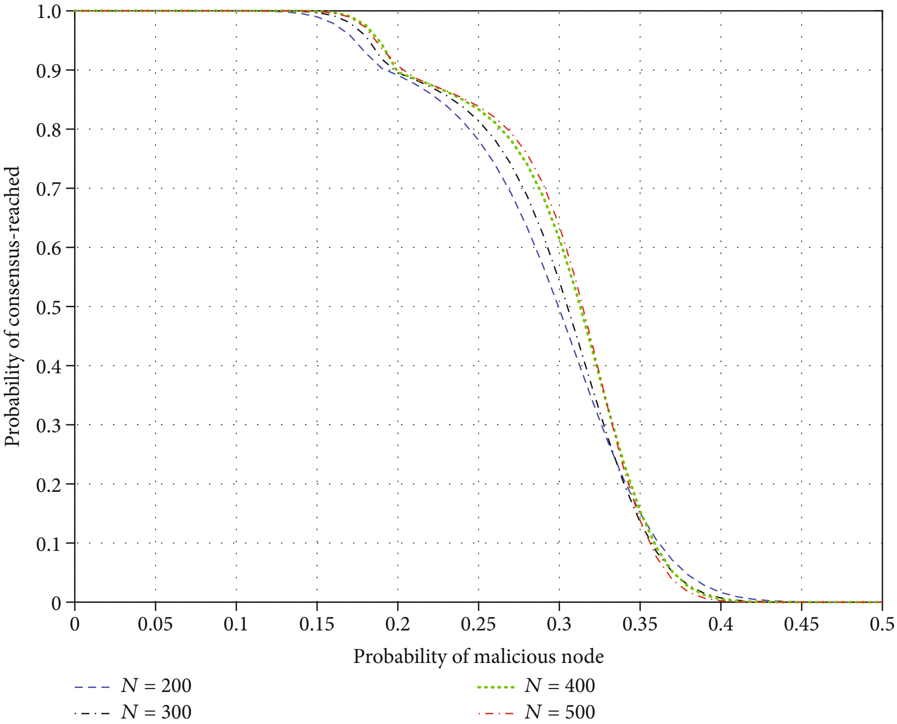

Figure 12: Security performance of double-layer PBFT under different N.

the total number of nodes increases, we should firstly increase the nodes in the 1st layer, i.e., m_1, rather than increase the nodes in the 2nd layer, i.e., m_2.

Figure 10 shows the lowest communication complexity under different layers PBFT with the variation of the number of nodes, which further confirms the conclusion that the more layers in PBFT are, the lower of communication complexity is.

5.2. Security Assessment of Multilayer PBFT Consensus. Given the total number of nodes $N = 100$, the security performance of X-layer PBFT ($X = 2$, $X = 3$, and $X = 4$) is illustrated in Figure 11. It can be seen that when P_f is relatively low, the probabilities of consensus-reached decrease with P_f. When P_f is relatively high, the probabilities of consensus-reached increase with P_f instead, which indicates that increasing PBFT layers does not always bring down the security performance. When P_f is relatively high, we have $P_{C_4} > P_{C_3} > P_{C_2}$. However, the security performance decreases sharply and becomes very poor at that time, and it is almost impossible to reach consensus for the multilayer PBFT. Secondly, with the increasing of N, the critical point, i.e., the intersection point of P_{C_2}, P_{C_3}, and P_{C_4}, gradually moves forward and indicates that the increasing of N will reduce the security performance.

The security performances of the double-layer PBFT under different number of nodes N are illustrated in Figure 12, given $N = 200/300/400/500$. It can be seen that when $P_f \leq 0.34$, increasing the number of nodes will improve the security performance (probability of consensus-reached). On the contrary, when $P_f > 0.34$, increasing the number of nodes will reduce the security performance (probability of consensus-reached).

Consequently, in order to greatly reduce the communication complexity and obtain an acceptable security performance, too many layers are unpractical. A 2- to 4-layer PBFT is sufficient to bring communication complexity down and also achieve an acceptable security performance.

6. Conclusion

In this article, a consortium blockchain-empowered HF spectrum management is exploited to improve the deteriorating HF electromagnetic environment; massive personal HF devices are organized around the preselected nodes to monitor and share HF data through PBFT protocol. To address the scalability problem, a multilayer PBFT consensus protocol is presented. Scalability evaluations shows that increasing the layers of PBFT greatly reduce the communication complexity. Security assessments illustrate that the security performance does not always decrease with the increasing of the layers of PBFT, but fewer layers indeed guarantee a better security performance. Tradeoff has been made between the communication complexity and security performance, a 2- to 4-layer PBFT is considered sufficient to bring the communication complexity down and also achieve an acceptable security performance. In a future work, it is interesting to extend the utilization of blockchain-empowered HF spectrum management for better improving HF electromagnetic environment, such as deployment optimization of edge computing nodes and spectrum strategy inference under energy constraint.

Data Availability

The supporting data are not yet open to public access.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. Shafi, A. F. Molisch, P. J. Smith et al., "5G: a tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, pp. 1201–1221, 2017.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): a vision, architectural elements, and future directions," *Future Generation Computer System*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] ITU-R, "Technical and operational principles for HF sky-wave communication stations to improve the man-made noise HF environment," Question ITU-R 258/5, 2019.

[4] ITU-R, "Radio regulations," *Radio Regulations-Articles*, vol. 1, 2016.

[5] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: a technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[6] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: a distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[7] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: a state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 858–880, 2018.

[8] J. Rosenworcel, *Remarks of Commissioner Jessica Rosenworcel Mobile World Congress Americas*, Mobile World Congress Americas, Los Angeles, California, 2018.

[9] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Vehicular Technology Magazine*, vol. 13, no. 1, pp. 32–39, 2018.

[10] Y. Pei, S. Hu, F. Zhong, D. Niyato, and Y. C. Liang, "Blockchain-enabled dynamic spectrum access: cooperative spectrum sensing, access and mining," in *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Waikoloa, HI, USA, 2019.

[11] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 2, pp. 193–205, 2019.

[12] M. Cao, L. Zhang, and B. Cao, "Toward on-device federated learning: a direct acyclic graph-based blockchain approach," *IEEE Transactions on Neural Networks and Learning Systems*, 2021.

[13] B. Shang, V. Marojevic, Y. Yi, A. S. Abdalla, and L. Liu, "Spectrum sharing for UAV communications: spatial spectrum sensing and open issues," *IEEE Vehicular Technology Magazine*, vol. 15, no. 2, pp. 104–112, 2020.

[14] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: an operator's perspective," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 451–466, 2020.

[15] T. Maksymyuk, J. Gazda, M. Volosin et al., "Blockchain-empowered framework for decentralized network management in 6G," *IEEE Communications Magazine*, vol. 58, no. 9, pp. 86–92, 2020.

[16] Z. Zhou, X. Chen, Y. Zhang, and S. Mumtaz, "Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks," *IEEE Network*, vol. 34, no. 1, pp. 24–31, 2020.

[17] P. Gorla, V. Chamola, V. Hassija, and N. Ansari, "Blockchain based framework for modeling and evaluating 5G spectrum sharing," *IEEE Network*, vol. 35, no. 2, pp. 229–235, 2021.

[18] G. Rathee, F. Ahmad, F. Kurugollu, M. A. Azad, R. Iqbal, and M. Imran, "CRT-BIoV: a cognitive radio technique for blockchain-enabled internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4005–4015, 2021.

[19] R. Zhu, H. Liu, X. Liu, S. Wan, and W. Hu, "Contract-theory-based secure spectrum sharing framework in internet of vehicles," *IEEE Consumer Electronics Magazine*, 2021.

[20] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2019.

[21] B. Cao, Z. Zhang, D. Feng et al., "Performance analysis and comparison of PoW, PoS and DAG based blockchains," *Digital Communications and Networks*, vol. 6, no. 4, pp. 480–485, 2020.

[22] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6–14, 2018.

[23] Y. Li, B. Cao, M. Peng, L. Zhang, D. Feng, and J. Yu, "Direct acyclic graph-based ledger for Internet of Things: performance and security analysis," *IEEE/ACM Transactions on Networking*, vol. 28, no. 4, pp. 1643–1656, 2020.

[24] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690–3700, 2018.

[25] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proc. of the 3rd Symp. Oper. Sys. Design Imple*, New Orleans, USA, 1999.

[26] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems (TOCS)*, vol. 20, no. 4, pp. 398–461, 2002.

[27] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable multi-layer PBFT consensus for blockchain," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 5, pp. 1146–1160, 2021.

[28] W. Lv, X. Zhou, and Z. Yuan, "Design of tree topology based byzantine fault tolerance system," *The Journal of Communication*, vol. 38, no. Z2, pp. 143–150, 2017.

[29] Q. Wu, G. Ding, Z. Du, Y. Sun, M. Jo, and A. V. Vasilakos, "A cloud-based architecture for the internet of spectrum devices over future wireless networks," *IEEE Access*, vol. 4, pp. 2854–2862, 2016.

[30] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[31] Y. Wu, J. Zheng, K. Guo, L. P. Qian, X. Shen, and Y. Cai, "Joint traffic scheduling and resource allocations for traffic offloading with secrecy-provisioning," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 9, pp. 8315–8332, 2017.

[32] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: the communication perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[33] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: a survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450–465, 2018.

[34] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: a survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[35] ITU-R SG01, *Handbook: Spectrum Monitoring*, ITU Publisher, Geneva, 2011.

[36] G. Ding, Y. Jiao, J. Wang et al., "Spectrum inference in cognitive radio networks: algorithms and applications," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 150–182, 2017.

[37] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.

[38] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," in *2017 International Conference on Engineering and Technology (ICET)*, pp. 1–7, Antalya, Turkey, 2017.

[39] H. Gilbert and H. Handschuh, "Security analysis of SHA-256 and sisters," in *Selected Areas in Cryptography, SAC*, vol. 3006 of Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2003.