Design of Routing Incentive Protocol for Space Network Based on Blockchain Technology

Ning Ma[1](✉), Xi Wang[2], Zhen Li[3], Panpan Zhan[1], Xiongwen He[1], Xiaofeng Zhang[1], and Zhigang Liu[1]

[1] Beijing Institute of Spacecraft System Engineering, Beijing 100094, China
mnuestc@163.com

[2] Beijing Aerospace Linkage and Innovation Technology Co. Ltd., Beijing, China

[3] Institute of Electronics, Chinese Academy of Science, Beijing 100190, China

Abstract. The global commercialization of satellites has intensified, and the types and numbers of new spacecrafts have increased year by year. However, the repeated functional construction and “islandization” characteristics of spacecraft severely restrict the use efficiency of space resources. How to realize the open interconnection and self-adaptation optimization cooperation of satellite resources and encourage more and more on-orbit spacecrafts to share spatial data services and routing resources is a severe challenge for the new generation space network communication protocol. This paper builds the Incentive Protocol of Routing based on the TCP/IP protocol family under the CCSDS spatial communication protocol standard framework. Using blockchain distributed database technology and consensus mechanism, combined with routing flow identification technology, design, and implement a network route incentive protocol and game model based on spacecraft route contribution proof consensus mechanism, intended to provide a feasible technical framework and feasible solution for the construction of the integrated digital intelligent economic ecology of the world.

Keywords: Space networking · Incentive protocol of routing · Blockchain · Space and ground network integration

1 Introduction

With the intensification of the global commercialization of satellites, the types and numbers of new research spacecraft have increased year by year. Under the existing spacecraft development and launch system, the repeated construction of the load function and the isolation feature of “islandization” are widespread, and there is undoubtedly serious restriction and waste on the use of near-Earth space resources. Therefore, in order to realize the open interconnection and adaptive optimization of satellite resources, and encourage more on-orbit spacecraft to share spatial data services and routing resources, higher requirements are put forward for the new generation satellite network communication protocol [1–3].

L. Wang et al. (eds.), *Proceedings of the 5th China High Resolution Earth Observation Conference (CHREOC 2018)*, Lecture Notes in Electrical Engineering 552,
https://doi.org/10.1007/978-981-13-6553-9_14

(1) Openness: Any on-orbit spacecraft which belong to different organizations and types can be freely joined or withdrawn from the network without the permission of a third party, subject to the corresponding technical specifications and conditions.
(2) Standardization: A common protocol family architecture should be adopted to maximize the integration of compatible satellite standards and ground Internet communication protocols to achieve integration of space and ground network.
(3) Self-driven: The networking protocol should have a built-in economic model, which can independently optimize the scheduling space routing resources, and encourage spacecraft to share data services: quantify the value of data services and routing resources contributed by in-orbit spacecraft, and Real-time clearing of data services and routing resources provided by the orbiting spacecraft.
(4) Security: Using mature digital signature and encryption algorithm, under the open information transmission system, data encryption transmission and confirmation are realized, and a peer-to-peer security information transmission network is constructed to serve the settlement system.
(5) Neutrality: The space network will serve as a public infrastructure that is not owned and controlled by any single or a small number of institutions and individuals. It will treat the information content of the space network fairly and provide relay and transmission services without review and distinction.

2 Protocol Technology Architecture

In addition to the basic communication functions, the spatial networking protocol quantifies the contribution value of the routing resources (connectivity, transmission data volume, and propagation delay) provided by the spacecraft in the spatial data communication service by the incentive protocol. The identification of the routing information of the space information flow through the spacecraft node is effectively identified and counted, and broadcasted to the entire network in real time. The ground verification node is then responsible for collecting and verifying the broadcast routing information, recording it in the blockchain data book in a distributed competitive accounting manner, and completing the real-time clearing and reward distribution of the spatial network data service and routing resources. The network incentive protocol encourages spacecraft individuals to share data services and routing resources by constructing an economic game model, thereby optimizing the use efficiency of spatial network routing resources.

The incentive protocol architecture is mainly divided into three subsystems: (1) Information Routing Flow Identification Subsystem: completes the routing information identification and statistics of the TCP/IP format exchange distribution information flow between space network spacecraft nodes, and broadcasts to the whole network. (2) Distributed Verification Subsystem: The local verification node checks the broadcast data of the information flow by competing accounting, and stores it in the Distributed File Storage System of IPFS (InterPlanetary File System), and the corresponding IPFS index. The hash value is used for blockchain accounting processing [4].

(3) Self-adaptive optimization scheduling subsystem: The space data service request will divide the real-time priority according to the amount of the additional certificate bonus when it is initiated, and the spatial routing node will give priority to the service of the higher data service request for the certificate. In this subsystem, an economic benefit coordination and game model with positive feedback mechanism is constructed. When each routing node participant adopts the strategic behavior of maximizing its own interests, the utilization efficiency of the entire space network will be optimal (Fig. 1).

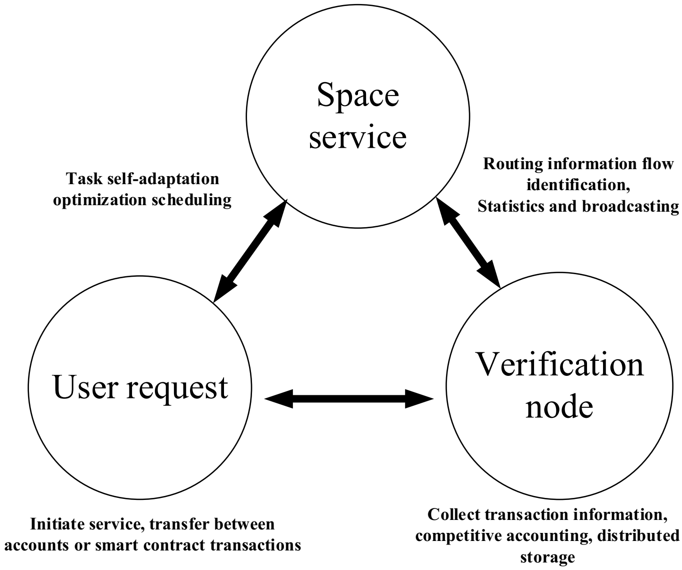

Fig. 1. protocol architecture model diagram

2.1 Information Flow Route Identification

A set of information flows is a set of single-item packets between a given source node and a destination node. Both source and destination nodes are defined by the address of the network layer and the port of the transport layer. The incentive protocol records and analyzes the network traffic information based on the flow network packet exchange technology, distributes the information according to the service request priority, and collects and broadcasts the routing information of each node in real time. This process is divided into two steps

(1) Data exchange and distribution according to the optimal use efficiency of the routing performance of the own node and the priority order of the transfer target data. The prioritization can be expressed as the amount of the token attached that the user is willing to pay when requesting the service.
(2) After the data transmission is completed, the distribution data stream is collected and broadcast to the entire network. The broadcast statistics include: the incentive layer protocol version number, the source port IP address, the source port ID (public key address), the target port IP, Target port ID (public key address), data transfer amount, transfer start and end time stamp, and stream ID.

2.2 Distributed Consensus Synchronization

The distributed consensus subsystem is mainly responsible for verifying and storing the information flow identification data of the broadcast, and forming the consensus of the whole network and recording it in the blockchain ledger. Considering the operating costs, the verification node body is generally composed of a ground network computer. After the verification node verifies the routing information broadcast by the space routing incentive protocol, the route contribution value of each spacecraft routing node in the data service is converted, packaged, and stored in the IPFS (InterPlanetary File System, IPFS) distribution. In the data sharing system, the index hash address of the packet in the IPFS is stored in the blockchain data book as the workload of the routing node to obtain the certificate revenue.

The information packed by the verification node includes not limited to the following contents: (1) digital signature of the source node, the destination node and the relay node in the transmission service; (2) transmission time stamp of each node; (3) data transmission amount; (4) The data packet hash value of each node; (5) The verification result of the data service correctness of the destination node at the time of service termination. The process of verifying the routing of the routing information by the node is as follows (Fig. 2).

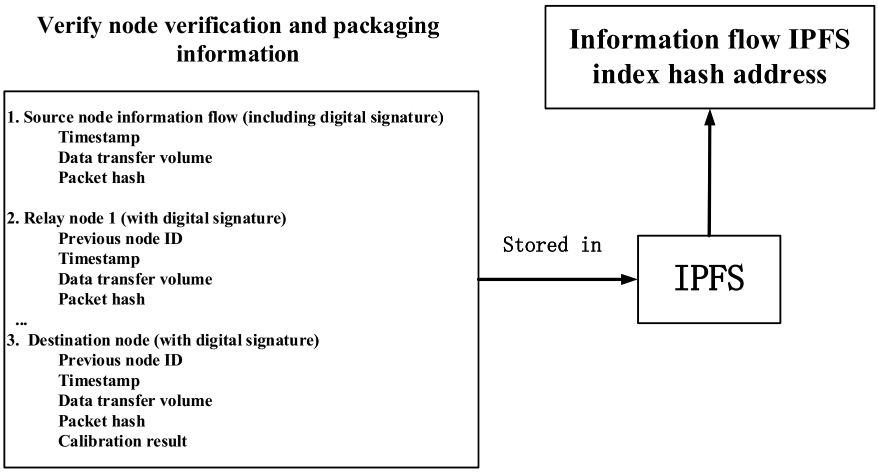

Fig. 2. Information flow IPFS index hash generation diagram

Considering that it is expensive to store data for blockchain, only the IPFS index hash address corresponding to the key data is stored in the blockchain ledger, and the complete data content is stored in the IPFS system. The IPFS system is based on a globally distributed peer-to-peer encryption storage protocol. Any node can only store one fragmented content of a complete file, and each fragment is backed up in multiple IPFS storage nodes, and only the complete index hash address is obtained [5, 6]. In order to collect all the file fragments and extract the complete file. Therefore, the scheme design of adopting such index address winding can not only ensure the security of data storage, but also save construction cost and improve the running efficiency of the entire system.

The generation of a block will package the following information: (1) The hash address of the collected and verified information flow during the period; (2) The transaction information between the collected and verified accounts during the period; (3) Block Generate timestamp information; (4) Incentive protocol version number; (5) Block height; (6) Previous block hash value. Therefore, the ground verification node is a non-tamperable high-performance chained distributed storage database [7, 8] (Fig. 3).

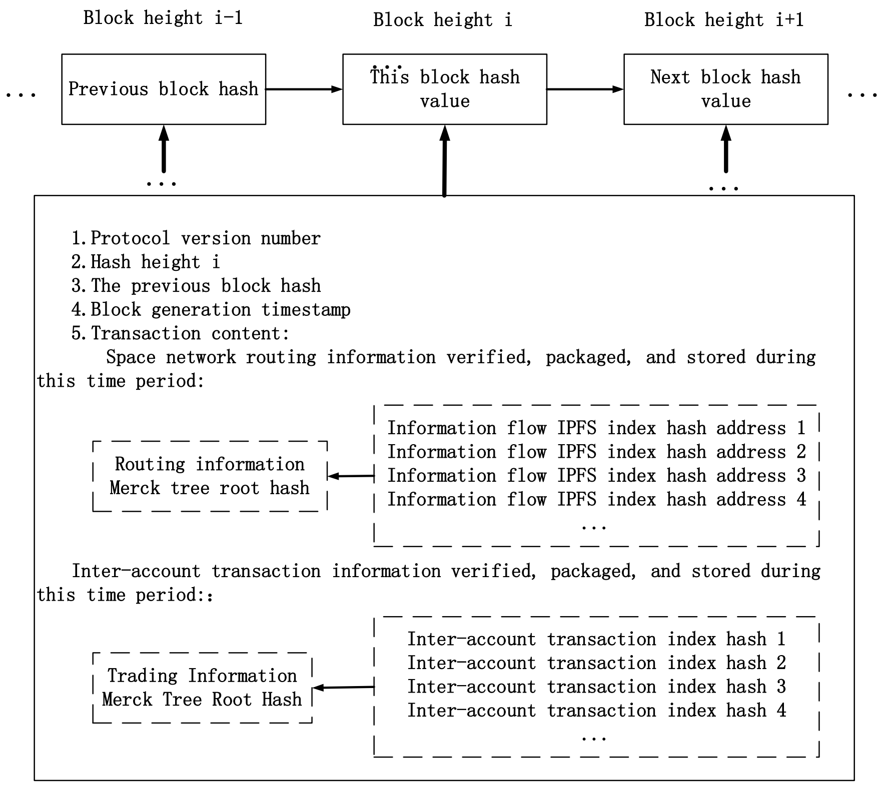

Fig. 3. block structure diagram

2.3 Self-adaptive Optimization Scheduling

The implementation of the self-adaptive optimization scheduling subsystem relies on constructing a credible economic model that can coordinate the interests of all parties and has a positive feedback incentive effect. The incentive agreement involves three parties: the space routing node, the ground verification node, and the user. The constructor of the spatial network service is mainly composed of the spatial routing node and the verification node: the spatial routing node forms a spatial network to provide spatial routing resources and data services for users; the ground verification node collects and verifies the routing contribution of routing nodes in the spatial data service. Value and inter-account transaction information, store key information and generate a blockchain transaction book that cannot be tampered with. The user holds a certain amount of pass and enjoys a certain share of the space network, and can use the pass to purchase data services or increase the priority of service requests.

The implementation of the self-adaptive optimization scheduling subsystem relies on constructing a credible economic model that can coordinate the interests of all parties and has a positive feedback incentive effect. The incentive agreement involves three parties: the space routing node, the ground verification node, and the user. The constructor of the spatial network service is mainly composed of the spatial routing node and the verification node: the spatial routing node forms a spatial network to provide spatial routing resources and data services for users; the ground verification node collects and verifies the routing contribution of routing nodes in the spatial data service. Value and inter-account transaction information, store key information and generate a blockchain transaction book that cannot be tampered with. The user holds a certain amount of pass and enjoys a certain share of the space network, and can use the pass to purchase data services or increase the priority of service requests (Fig. 4).

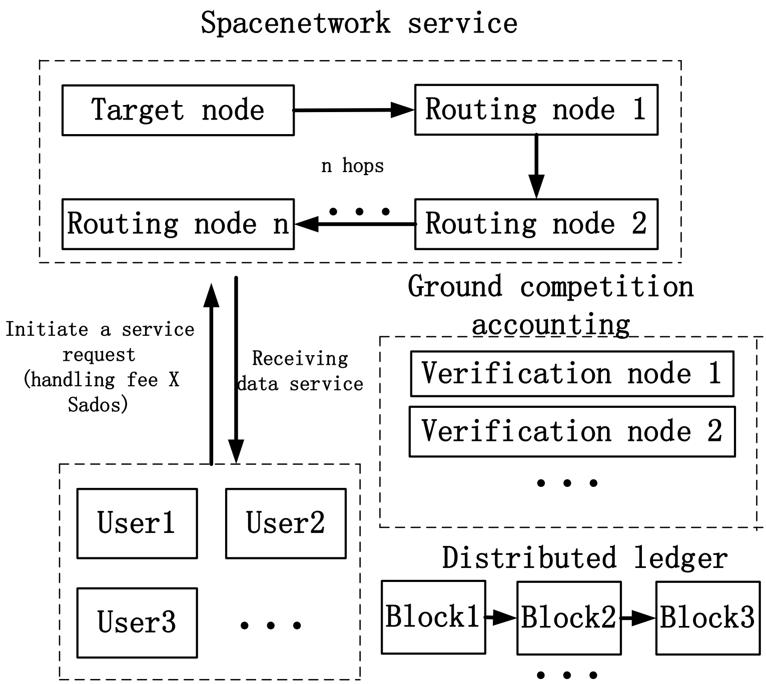

Fig. 4. Schematic diagram of self-adaptive optimization scheduling

The economic incentive model is designed as follows: The pass name used to measure the space data service of the whole network is the Satdomain, shorthand: Sado, which characterizes the holder of the Sado to enjoy the use of the routing resources of the space network. The initial circulation of Sado is 20,000,000, the final circulation is 200,000,000, the full issuance period is 45–106 years, and the annual issuance limit is 2–5%. The annual Sado issuance rate is based on the growth rate of the total service value of the previous year. The full issuance period is 45–106 years. The additional issuance amount is used to reward the contribution of the space routing node and the verification node as the infrastructure.

The following economic indicators are defined for the entire network:

(1) $GSSP_j$: Gross Spacenetwork Service Product AD j.

$$GSSP_j = \sum_{i=1}^{mj} Hop_{ij} * MB_{ij} \tag{1}$$

m_j	The total number of information flow routing services provided by the whole network in AD j.
Hop_{ij}	the number of hops of the i-th space routing data service in AD j.
MB_{ij}	The data transmission volume of the i-th space routing data service in AD j.

(2) Pj: The growth rate of GSSP in the previous year compared to the previous year in AD j.
(3) Sj: The total amount of Sado basic certificate issued in AD j.
(4) ΔSj: New circulation of Sado in AD j.

The following design for the entire network Sado distribution and rewards.

The Sado characterizes the use of space network data services. In order to maintain the stability of the Sado currency, the increase in the total amount of Sado's issuance should always be consistent with the growth of GSSP (Gross spacenetwork service production). The total value of the default space network service will reach saturation in 106 years, that is, the Sado circulation will reach no increase after the number of 200 million issuance. During this issuance, the annual new circulation of Sado is always issued according to ΔSj (when ΔSj meets the conditions: $2\% < \Delta\ Sj < 5\%$), the current year $GSSP_{j-1}$ growth rate $\Delta\ P_{j-1}$ is also in the range of 2–5%, then in the current year Sado new circulation

$$\Delta S_j = \Delta P_{j-1} * S_{j-1} \tag{2}$$

The increase in the total value of the space network service is due to the expansion of the scale of the service provider's space routing node and the verification node and the improvement of the efficiency. Therefore, the issued Sado is used for proportional rewards and routing nodes and verification nodes. 95% of the new circulation is awarded to the routing node. 5% of the new circulation is awarded to the verification node. In addition to this, the routing node and the verification node will also obtain a transaction reward for the user's additional payment.

Annual total revenue distribution of space routing nodes in AD j:

$$E_{R\mathrm{j}} = \mathrm{X}\frac{n}{n+1} + 95\% * \triangle S_{\mathrm{j}-1} \tag{3}$$

X Annual user additional payment fee;
n average hop count of the annual information flow space route;

Annual total revenue distribution of the ground verification node in AD J

$$E_{Vi} = \mathrm{X}\frac{1}{n+1} + X_{\mathrm{j}-1} + 5\% * \triangle S_{\mathrm{j}-1} \tag{4}$$

For a single space routing node A and a verification node B, the respective proportion of the total annual route contribution and the verification contribution is k_{ar} and k_{bv} then

Annual total revenue of space routing node a in AD J

$$E_R = \sum_{\mathrm{i}=1}^{a_j} \frac{\mathrm{Xa}_i}{n_{ai}+1} + 95\% * k_{ar} * \triangle S_{\mathrm{j}-1} \tag{5}$$

a_j the total number of routing data services in the space routing node A in AD j;
X_{ai} the additional payment fee for routing node A's i-th routing data service;
n_{ai} the average hop count of routing node A's i-th routing data service space;

The total annual revenue of the ground verification node b in AD J:

$$E_V = \sum_{\mathrm{i}=1}^{b_j} \frac{\mathrm{X}_{bi}}{n_{bi}+1} + 5\% * k_{bv} * \triangle S_{\mathrm{j}-1} + \mathrm{X}_{\mathrm{bj}} \tag{6}$$

b_j the total number of data services verified by ground verification node B in AD j.
X_{bi} the additional payment for ground verification node B's i-th verifing data service;
n_{bi} the average hop count of ground verification node B's i-th verifing data service space;
X_{bj} The fee charged by the ground verification node B in the transaction service in AD j.

3 Application Prospects and Value—Space and Ground Integration Intelligent Digital Ecological Economy

This paper designs the technical framework of spatial networking route incentive protocol based on blockchain technology, and demonstrates that the economic significance of its certificate-exciting model plays an important role in promoting the construction of the worldwide integrated network. At the same time, the technical framework of the incentive agreement has a high degree of expansion and broad application space. Through the incentive agreement, the economic model is conducive to building a worldwide intelligent network economy based on spatial data services, creating a fair, mutually beneficial and diversified intelligent contract platform and network intelligent economic ecology.

References

1. Satellite Industry Association. State of the satellite industry report[EB/OL]. [2016-03-02]. http://www.sia.org/wpcontent/uploads/2013/06/2013_SSIR_Final.pdf.
2. Iridium. Iridium NEXT: The bold future of satellite communications [EB/OL]. [2016-03-02]. https://www.iridium.com/network/iridiumnext.
3. Wang Jiasheng. China data relay satellite system and its application prospect[J]. Spacecraft Engineering, 2013(1): 1–6.
4. IPFS - Content Addressed,Versioned, P2P File System[EB/ OL]. https://blog.acolyer.org.
5. I.BitTorrent. Bittorrent and ˆA¸ttorrent software surpass 150 million user milestone, Jan. 2012 [Z].
6. L. Wang and J. Kangasharju.Measuring large-scale distributed systems : case of bittorrent mainline dht[C]. In Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on, IEEE, 2013:1–10.
7. Mukhopadhyay U, Skjellum A, Hambolu O, Oakley J, Yu L, Brooks R. A brief survey of Cryptocurrency systems. In: Privacy, Security and Trust. 2017. 745–752.
8. Antonopoulos AM. Mastering Bitcoin: Unlocking Digital Crypto-Currencies. O'Reilly Media, Inc., 2014.