electronics

MDPI

Article

A Blockchain-Based Authentication Protocol Using Cryptocurrency Technology in LEO Satellite Networks

Xia Deng [1], Junbin Shao [1,*], Le Chang [2,*] and Junbin Liang [3]

[1] School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou 510006, China; gzhu_dx@gzhu.edu.cn
[2] School of Automation, Guangdong University of Technology, Guangzhou 510006, China
[3] School of Computer and Electronics Information, Guangxi University, Nanning 530004, China; liangjb@gxu.edu.cn
* Correspondence: 2112006187@e.gzhu.edu.cn (J.S.); lechang@gdut.edu.cn (L.C.)

Abstract: With the rapid development of satellite technology and the high transmission efficiency of LEO satellites, LEO satellite communication has received increasing attention. However, the frequent switching of satellite-earth links imposes a great challenge in LEO communication authentication. To tackle this challenge, this paper proposes a Blockchain-based Authentication Protocol Using Cryptocurrency Technology (BAPC), which solves the problem of a long pause time of satellite services caused by user access authentication in a scenario of frequent switching between satellites and ground users. First, we design three stages of the authentication process and introduce the cryptocurrency technology. Using currency transactions as the certificate of authentication improves not only the security of authentication, but also the efficiency of switching authentication. Next, in the network topology, the satellite cluster is divided into multiple regions to improve the efficiency of block consensus. Finally, the protocol is tested through extensive NS2-based simulations, and the results verify that BAPC can greatly shorten the response time of switching authentication and significantly reduce the time of block generation and the network throughput. As the number of users increases, the block generation time and network throughput can be further reduced.

Keywords: LEO satellite networks; blockchain; cryptocurrency; switching authentication

Citation: Deng, X.; Shao, J.; Chang, L.; Liang, J. A Blockchain-Based Authentication Protocol Using Cryptocurrency Technology in LEO Satellite Networks. *Electronics* **2021**, *10*, 3151. https://doi.org/10.3390/electronics10243151

Academic Editors: Mauro Tropea and Manuel Arrebola

Received: 30 September 2021
Accepted: 14 December 2021
Published: 17 December 2021

1. Introduction

Low-Earth-Orbit (LEO) satellite networks have attracted considerable attention in recent years. LEO satellite networks are useful in a variety of scenarios. In some remote areas with small populations and the ocean, it is difficult to provide internet services from the ground due to the high construction cost of the network. In addition, when traveling in fast-moving vehicles, such as airplanes, communication frequently switches between different ground base stations, resulting in high packet loss rates and poor service quality [1–3]. At this point, LEO satellite networks can provide broadband communication where there is no ground equipment, and provide high-quality services to anyone, anytime and anywhere [4–6].

The LEO satellite networks have a low delay, high bandwidth, high transmission rate, and low link loss, and bring global coverage and efficient frequency reuse [7–10]. As 5G communication standards mature, satellite communications play an important role in expanding and completing ground networks [11,12]. With the increasing demand for seamless broadband communication, the global LEO satellite communication system has become an important part of connecting space and ground. The goal is to provide high-quality access for all users at any time and in any space [13–15].

In LEO satellite networks, traditional access authentication needs satellites to send authentication information back to the ground control center to confirm user identity. There are so many hops of transmission that the overhead of the certificate management using a

public key infrastructure is not negligible. In addition, due to the high-speed movement of LEO satellites in space, users on the ground can only be served by one satellite within approximately ten minutes in the Iridium system. Communication requires frequent switching of authentication, and traditional authentication protocols are greatly affected by onboard routing protocols. Because the authentication process is greatly affected by the centralized certificate authority. In the authentication process, satellites need to obtain the certificate revocation list which is used to notify the satellite that the certificate has been cancelled by the certificate authority. Such communication is implemented by transmitting control data through the inter-satellite links. The inter-satellite links may be congested or disconnected, so it is particularly important to choose a proper routing protocol. Improper routing will not only increase the delay, but also lead to data loss. Researchers have proposed using an identity-based encryption algorithm to replace certificate authority institutions [16]. However, the system stores a large number of user parameters, making the efficiency low. Concerning switching authentication, researchers transmitted data through broadcast according to the distributed characteristics of blockchain, which reduced the dependence on routing protocols [17]. However, these studies limit the prerequisite conditions of authentication. Not all types of switched authentication can achieve high efficiency.

To tackle these challenges, this paper proposes a blockchain-based authentication protocol using cryptocurrency technology (BAPC) that not only solves the problem of difficult certificate management by using blockchain and cryptocurrency technology, but also enables the satellite to independently access authentication without being affected by routing protocols. It is suitable for various types of switching authentication.

The main contribution of this paper is summarized as follows.

1. The registration stage, initial authentication stage and switching authentication stage of access authentication are designed, and the cryptocurrency technology is introduced. It not only improves the security of authentication, but also improves the efficiency of switching authentication. Therefore, cryptocurrency plays an important role in these three stages. Currency transactions, as certificates that cannot be tampered with, ensure the reliability of authentication information.
2. According to the network topology, multiple areas are divided, and nodes in the area collaborate to generate blocks. After a node receives a transaction, the transaction is temporarily stored in the local cache pool, and the node independently verifies the local transactions. This scheme not only reduces the network load of intersatellite transmission but also reduces the computational overhead of a single node in verifying transactions.
3. Computational overhead of BAPC is compared with other protocols, and the security of BAPC is analyzed. The asymmetric encryption operation, signature operation and verification operation adopted in BAPC are at the average computation level, and there are fewer communication times. In addition, in terms of security, it not only ensures the security of the key but also effectively resists replay attacks, denial of service attacks and impersonation attacks.
4. BAPC is simulated on the NS2 network simulation platform. Simulation results show that BAPC greatly reduces switching authentication time compared with other protocols. In addition, compared with no regional partitioning, regional partitioning significantly reduces the block generation time and the network throughput. Moreover, the computation time of the signature and validation operations are tested on Python.

The remainder of this paper is organized as follows. Section 2 reviews the relevant work in satellite access authentication. Section 3 introduces the blockchain and cryptocurrency technology and describes the system model. In Section 4, the three stages of the proposed authentication protocol are introduced. Section 5 describes the method and analysis of area division. Section 6 compares the computational overhead with other protocols

and analyzes the security. In Section 7, the simulation results on the NS2 platform are presented. Section 8 concludes this paper.

2. Related Work

In LEO satellite networks, the service area of the satellite is constantly moving; therefore, the connection between the user and satellites needs frequent switching. How to efficiently implement switching authentication is an important research problem.

Regarding identity authentication protocols in terrestrial networks, Ao et al. proposed a new secure identity authentication scheme based on blockchain and identity-based cryptography. The scheme implemented a decentralized private key generator in the Ethereum blockchain, and used the identity-based encryption signature algorithm and challenge-response protocol during the authentication process. This scheme used blockchain to solve the single point of failure and identity-based encryption to avoid the complex certificate management [16], but bilinear pairs have high computational cost and system overhead. Zhang et al. proposed a certification public key cryptography. The key generation center gave part of the user's private key. The user selected a secret value and combined part of the private key to generate a complete private key. This method avoided the problem of private key escrow in identity based public key cryptography [18]. In the terrestrial network, the existing work uses identity-based encryption algorithm or blockchain technology to avoid complex certificate management.

For the satellite networks using key authentication protocols, Cruickshank et al. proposed mutual authentication between users and satellites using a public key encryption system, which uses a key algorithm to encrypt data, and a public key encryption system can ensure the security of data transmission [19]. However, its operation is too complicated, and the reliability of authentication information is not involved. Wu et al. proposed a Beidou2 navigation information authentication scheme, which uses an elliptic curve digital signature algorithm to generate digital signatures to verify the integrity and authenticity of navigation data and avoid entity disguise and data tampering [20]. However, information authentication during satellite switching is not involved. Altaf et al. proposed a robust key negotiation authentication scheme suitable for mobile satellite environments, providing mutual authentication, session key negotiation and correct user anonymity concepts [21], but there are problems of protocol storage, high communication cost and complex calculation. In satellite networks, most work considered optimizing the calculation method of authentication, which involved the management of certificate authority and thus suffered from the single-point-of-failure problem. In addition, the distance between the satellite and the certificate authority is varying, and the data transmission between them may need to be forwarded through multiple satellite nodes. The data volume and transmission time of trusted certificate cannot be simply ignored, which increases the communication delay in the switch authentication process.

Regarding signature algorithms in the satellite networks, Meng et al. designed an authentication scheme based on a proxy signature, and the authentication interaction process was only realized between mobile users and satellite nodes, thus reducing the long delay of authentication implementation [22]. Although proxy signature can avoid the problem of certificate management, each authentication needs to pass through the gateway to obtain permission, which causes a problem with too many transmission hops. In resource-constrained LEO satellite networks, the response latency of the above authentication protocols needs to be improved, and the distributed characteristics of LEO satellite networks needs attention. According to the distributed characteristics of LEO satellite networks, we adopt the blockchain technology. In the network, satellites can calculate independently, become peer nodes, and thus no longer rely on a control center. This effectively solves the problem of single point of failure of the public key infrastructure and provides support for users' fast access authentication. According to latest research results in the field, compared with traditional authentication protocols, the additional overhead

brought by blockchain is in an acceptable range, which makes the blockchain technology feasible for LEO satellite networks [23–26].

Regarding the satellite networks using blockchain technology, Pokhrel et al. proposed a federated learning framework based on blockchain. They quantified the forking probability of the blockchain and exploit double deep Q-network algorithm for efficacious resource allocation [23]. In our protocol, the blockchain we use is consortium blockchain which is one type of the blockchains. Satellite nodes do not compete for bookkeeping rights, so we do not need to consider the bifurcation of blockchain. Ibrahim et al. reviewed some scenarios in which blockchain technology is applied to satellite communication, and discussed the contributions and challenges of deploying blockchain in satellite clusters and the solutions to the challenges [24]. The contribution and challenge of applying blockchain technology to satellite communication have been discussed and its efficacy in satellite communication has been verified.

Wei et al. proposed abstracting the characteristics of LEO satellite dynamic topology by using regional division and establishing a consensus among satellites on user authentication by using the consensus mechanism in blockchain. The protocol also combines a distributed hash table and hash lock to reduce storage and computing overhead and to realize user switching authentication in LEO satellite networks [25]. However, it transmits a large amount of data and has a longer communication time. Wei et al. proposed an access authentication protocol combining identity-based encryption and blockchain technology. The protocol can be quickly reconnected to satellites in the same orbit, and two different key management schemes of identity-based encryption and blockchain were studied [26]. However, when users access authenticated satellites in different orbits, complete reauthentication is required. The above work mainly focused on using blockchain to ensure the security of handover authentication by combining the distributed characteristics of satellite networks, but in the initial authentication stage, the correctness of the information added to the blockchain cannot be ensured. Nodes in the same region trust other nodes excessively. Once a malicious node appears in the region, the normal nodes in the same region will not be able to recognize the wrong authentication information. In our protocol, based on the openness and transparency of cryptocurrency, all nodes in the network can verify the correctness of authentication information.

As discussed above, centralized secret-key based approaches suffer from single-point-of-failure problem, while blockchain is a distributed method that solves the problem. During the switching authentication process, the satellite can independently authenticate the user identity without communicating with the authentication center, while the traditional protocol cannot. In addition, the blockchain operation has been completed before user switch authentication, which will not affect the performance during the switch authentication process. Moreover, although cryptocurrency is a technology based on blockchain, there is still limited work on cryptocurrencies in LEO satellite networks. Therefore, in this paper, we apply cryptocurrencies to satellite access authentication. The authentication center verifies the user identity and stores a transaction in the blockchain. When a user switches from one satellite to another, the satellite finds the user address included in the transaction within the blockchain. At this time, the transaction becomes a trusted credential in the authentication process, and the user address in the transaction is generated by the user's public key through the hash algorithm, which plays a key role in data authentication. We design a blockchain-based authentication protocol using cryptocurrency technology (BAPC), which not only improves the efficiency of switching authentication, but also improves the security of authentication. In addition, a regional division method is used to reduce the time of block generation and network throughput.

3. System Model

In satellite communication, the communication between ground users and satellites is an important part. With the continuous movement of satellites, the connections between users and different satellites need to be switched frequently. Before the satellite serves the

users, the user identity must be authenticated. The speed and correctness of user identity authentication will affect the user experience and satellite security. In this paper, we aim at finding how to efficiently and accurately authenticate the user identity by satellites. In this section, we introduce the background and the system model of our blockchain-based authentication scheme in LEO satellite networks.

3.1. Blockchain

A blockchain is a distributed database system with multiple peer nodes. It is also a distributed ledger maintained by all peers in the network, with each node keeping a complete copy of the chain. Its core advantages are establishing trust between nodes, preventing data from being tampered with or forged, and ensuring data reliability. In the operation of the system, all transactions are open, transparent and traceable [27,28]. In a blockchain, data are encapsulated in blocks. Each block has a block header containing a hash of the previous block and a block body containing transaction information, and all blocks are connected in a chain structure. Blockchain technology has many advantages. For example, when adding data, the block needs to pass the consensus of the node before it can be connected. All participants in the network can verify that the data are correct through specific calculations. Each peer's ledger is consistent across the network. Any node can record data on the chain through agreed-upon rules [29,30]. User information can be stored under a non-real name. Suciu et al. compared blockchain with IOTA which is a distributed database. Blockchain allows a procedure to be created as a chain of records which cannot be altered. In tangle, every new transaction needs to allow other two [31]. In our protocol, satellite nodes take turns to account and the blockchain will not be forked. So it is more appropriate to store data in a single chain structure. These features are more suitable for the transaction storage requirements of cryptocurrencies. We use blockchain technology to support BAPC [32]. The blockchain type we use is consortium blockchain. The consortium blockchain specifies multiple preselected nodes as bookkeepers. Compared with the public blockchain, the consortium blockchain has lower complexity, simpler consensus algorithm and less resource consumption. Moreover, in a satellite network shared by multiple different authorities, the blockchain technology facilitates secure cooperation among multiple authorities.

3.2. Cryptocurrency

Cryptocurrency is a medium of exchange that uses cryptography to secure transactions. Cryptocurrencies are a type of digital currency. In addition, cryptocurrency relies on blockchain technology, which is an application of blockchain [33]. Cryptocurrencies can be a borderless way to provide people with financial products, as well as physical spending power. In other words, cryptocurrency is finance designed for the Internet, a programmable currency that anyone can send and receive easily on the network. Bitcoin, the best-known cryptocurrency in history, became the first decentralized cryptocurrency in 2009. Cryptocurrencies are based on decentralized consensus mechanisms, as opposed to banking and financial systems that rely on centralized regulatory systems. At the same time, cryptocurrency has become a new digital economy based on blockchain [34,35].

3.3. System Model

We use the blockchain network, which is jointly maintained and mined by each node in the satellite network system and each satellite node holds an identical ledger. The blockchain type we use is consortium blockchain and we introduce cryptocurrency to the network. We assume that there is no interest competition among all satellites and satellites provide services to users equally. As shown in Figure 1, adjacent satellite nodes in the same orbit are divided into the same region in the network topology. When receiving a user transaction, a satellite node stores it temporarily in the local cache pool instead of broadcasting it immediately. When a mining pool obtains the right of bookkeeping, the nodes in the pool jointly create a block. In the process of block generation, each node

verifies the transaction in the local cache pool, and then the nodes at both ends of the region send the information to the master node in the middle of the region, which contains the successfully verified transaction and the calculated root hash. Finally, the master node integrates all transactions and broadcasts the block. In the consensus process, accounting in turn is adopted. All mining pools generate blocks and broadcast them in turn. This is similar to the process that the leaders in the RAFT consensus algorithm take turns to keep accounts. The RAFT consensus algorithm has three statuses: leader, candidate and follower. The followers nominate the leader via an election process. The leader is responsible for sending all messages to the participating followers in the network [36]. The order of block production in each round is random. We do not use incentive mechanism and nodes do not need to consume extra computing power to compete for the right of accounting. Each new block will be generated in sequence and thus the ledger can be synchronized.

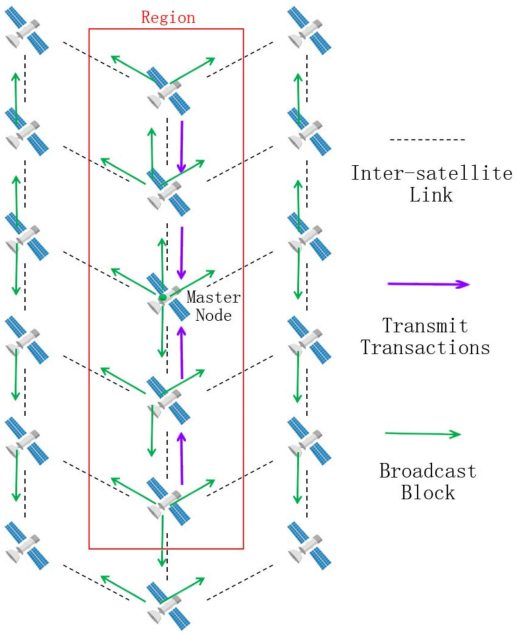

Figure 1. Block generation and broadcast.

We design an authentication method based on cryptocurrency to improve authentication speed and security. As shown in Figure 2, authentication process is divided into three stages. In registration stage, the user applies to the authentication center for purchasing cryptocurrency. After verifying the user identity information and waiting for the user to pay successfully, the authentication center transfers the corresponding amount of cryptocurrency from the authentication center address to the user address. Then the authentication center sends the transaction to a satellite node, and the satellite node stores the transaction in the blockchain. In initial authentication stage, the user applies to a satellite node to purchase services. The satellite finds the user address on the blockchain according to the user's request information. If there is enough balance in the user address, the transaction submitted by the user is stored in the blockchain, and then the service can be provided. In the switching authentication stage, the user needs to switch to another satellite and apply for identity authentication from the satellite. The satellite checks the transaction submitted by the user when purchasing the service on the blockchain. If the transaction is valid, the satellite continues to provide services. Through the above three-stage authentication process using cryptocurrency technology, we can achieve fast switch authentication.

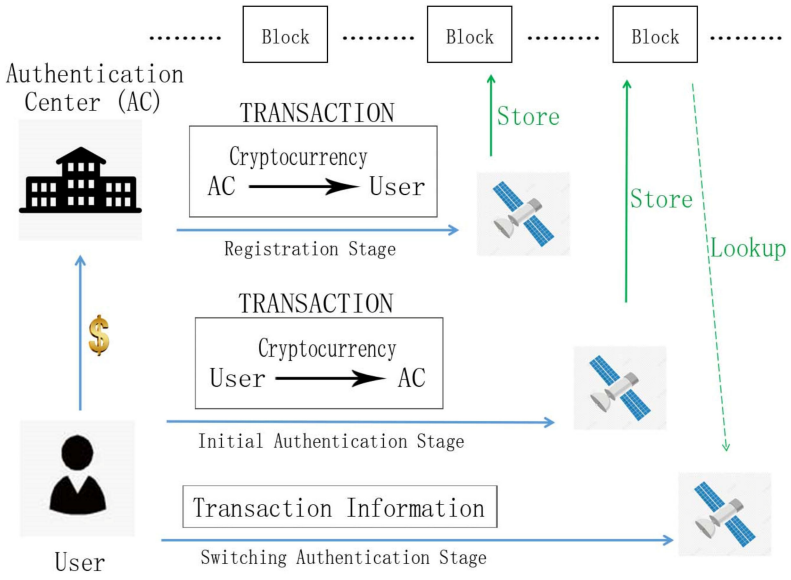

Figure 2. Authentication process based on cryptocurrency.

4. Protocol Design

In this section, we introduce our blockchain-based authentication protocol using cryptocurrency technology (BAPC). We design three authentication stages in BAPC: the registration stage, initial authentication stage and switching authentication stage. As the underlying technology of cryptocurrency, blockchain is mainly responsible for storing relevant data of cryptocurrency. User authentication depends on the support of cryptocurrency technology. In BAPC, the user status is divided into three types: unregistered, registered and waiting for switch. According to these different statuses, users need to experience three different stages: the registration stage, the initial authentication stage and the switching authentication stage. The first two stages only need to be executed once as preparation. When a user leaves the coverage area of the current satellite, it needs to connect to another satellite immediately. At this time, the user is in the status of waiting for switch and only needs to execute the switching authentication stage. The overall three-stage process of the protocol is shown in Figure 3.

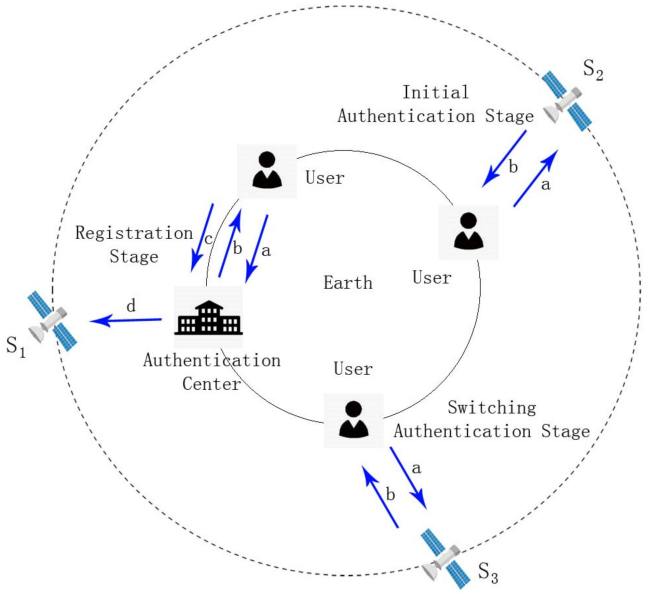

Figure 3. Three-stage process of the BAPC protocol.

4.1. Registration Stage

In the registration stage, users purchase the corresponding cryptocurrency from the ground authentication center as a prerequisite for obtaining satellite services. Authentication center transfers a certain amount of cryptocurrency from the authentication center address to the user address, which is used to provide data authentication, as shown in Figure 4, which is divided into four steps.

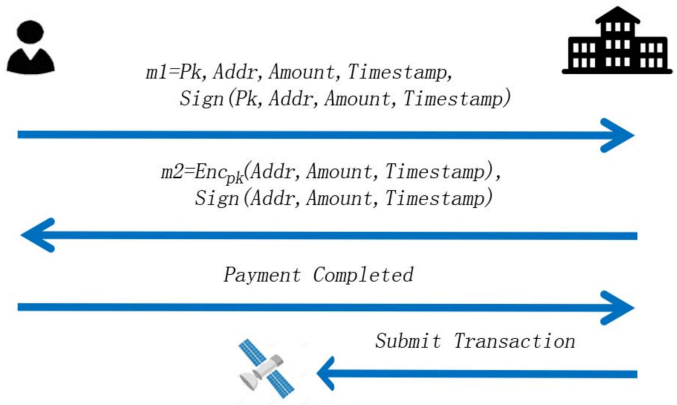

Figure 4. Registration stage.

1. The user uses the key generator provided by the authentication center to generate the private key, public key and corresponding address. The user sends the public key, address, quantity of cryptocurrency to purchase, timestamp, and signature to the authentication center. The calculation method is shown in (1).

$$m1 = Pk, Addr, Amount, Timestamp, Sign(Pk, Addr, Amount, Timestamp) \quad (1)$$

2. After receiving the request, the authentication center verifies the correctness of the public key, address, cryptocurrency quantity, timestamp, and signature. If the verification succeeds, the authentication center returns to the payment channel and waits for the payment. Otherwise, the authentication center rejects the request. The calculation method is shown in (2).

$$m2 = Enc_{pk}(Addr, Amount, Timestamp), Sign(Addr, Amount, Timestamp) \quad (2)$$

3. The user pays and asks for confirmation.
4. If the authentication center confirms the successful payment, it will submit a transaction to the nearest available satellite node. The transaction content includes the authentication center transferring the corresponding amount of cryptocurrency to the user address. Otherwise, the request will be rejected.

4.2. Initial Authentication Stage

When the user has not been authenticated or the authentication has expired and initial authentication is required, the user at this stage sends the initial authentication request to the nearest available satellite and pays the amount of cryptocurrency to obtain the satellite service. Moreover, the user can return all the cryptocurrencies to the authentication center when the user needs to cancel the unexpired service, as shown in Figure 5, which is divided into three steps.

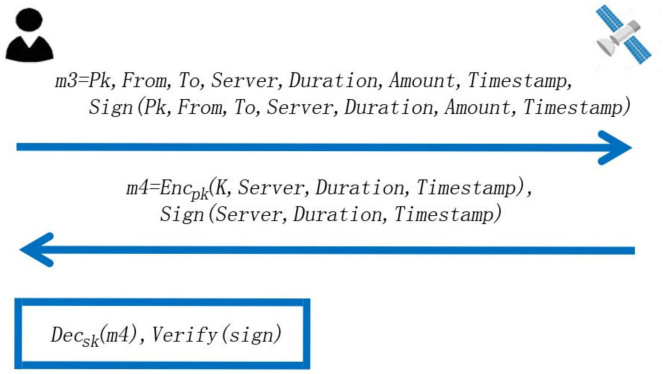

Figure 5. Initial authentication stage.

1. The user submits a transaction to the satellite, and the transaction information includes the user's public key, registered user address, authentication center address, requested service type, service duration, cryptocurrency quantity, timestamp, and signature. The calculation method is shown in (3).

$$m3 = Pk, From, To, Server, Duration, Amount, Timestamp, Sign(Pk, From, To, Server, Duration, Amount, Timestamp) \quad (3)$$

2. The satellite node receives the trade request; verifies the public key, address, service type, service duration, cryptocurrency quantity, timestamp, and signature; and checks whether the balance in the address is enough to pay for services. If authentication is successful, then the transaction is included in the buffer pool waiting for packaging; otherwise, the request is rejected. After the transaction is packaged, the session key, service type, service duration, and timestamp encrypted with the user's public key are returned to the user. The calculation method is shown in (4).

$$m4 = Enc_{pk}(K, Server, Duration, Timestamp), Sign(Server, Duration, Timestamp) \quad (4)$$

3. The user receives the returned information; decrypts it with the private key; obtains the session key; verifies the correctness of the service type, service duration and timestamp; and obtains the service from the satellite with the session key.

4.3. Switching Authentication Stage

When a user leaves the service area of the currently connected satellite, the user needs to find the next satellite to continue using the satellite service. If the service requested by the user in initial authentication stage has not expired, the user can obtain the service by providing transaction information. The user address in the transaction within the blockchain is used as the trusted credential to facilitate data authentication, as shown in Figure 6, which can be divided into three steps.

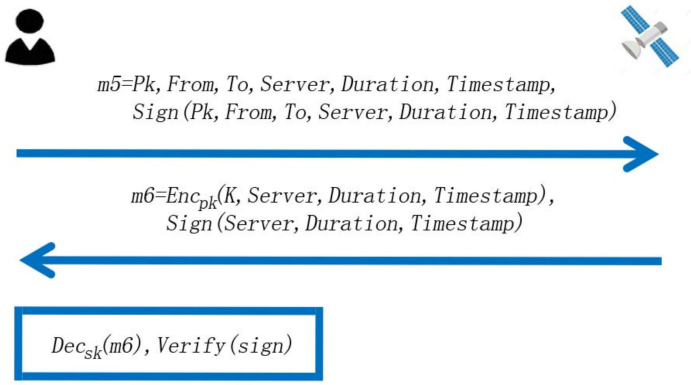

Figure 6. Switching authentication stage.

1. The user sends the public key, user address, authentication center address, service type, service duration, timestamp, and signature to the satellite. The calculation method is shown in (5).

$$m5 = Pk, From, To, Server, Duration, Timestamp, Sign(Pk, From, To, Server, Duration, Timestamp) \quad (5)$$

2. After receiving the information, the satellite node verifies the correctness of the public key, address, service type, service duration, timestamp and signature. According to the data on the blockchain, the satellite node checks whether the address exists corresponding to the user's public key and whether the service time has unexpired. If the authentication succeeds, the new session key, service type, service duration, and timestamp encrypted with the user's public key are returned to the user. Otherwise, the request is rejected. The calculation method is shown in (6).

$$m6 = Enc_{pk}(K, Server, Duration, Timestamp), Sign(Server, Duration, Timestamp) \quad (6)$$

3. The user receives the returned information, decrypts it with the private key, obtains the new session key, and uses the new session key to obtain services from the satellite.

5. Regional Division and Analysis

In this section we introduce the regional division of satellite groups according to the network topology in LEO satellite networks. We describe our regional division method, and then discuss how to reduce the computing overhead and network load.

5.1. Regional Division

In LEO satellite networks, the existing regional division method is used to improve the efficiency of switching authentication within each region. Wei et al. proposed a division method, taking the satellite in the middle position as the main node and establishing links between two adjacent satellites in the same orbit and two adjacent satellites in the adjacent orbit so that the five satellites can be divided into a region [25]. However, given the potential of reverse slits in the satellite network, as well as the instability or disconnection of links between different orbits as the satellite moves to high latitudes, the region will not work properly. In addition, it is more difficult to ensure that there are links between adjacent areas and the normal operation of areas in cross- regional switching authentication. In terms of storage mode, the method proposed by Wei et al. uses the distributed hash table technology, which reduces data redundancy. However, when switching authentication, user authentication information needs to be transmitted through intersatellite communication, resulting in an increased delay of switching authentication.

Aiming at the above problems, we propose a stable regional division method. This method can avoid the situation that a region fails to work properly due to the disconnection of links between satellites. At the same time, each node in the region has a complete blockchain ledger, which can avoid the response delay caused by excessive intersatellite communication when switching authentication. In addition, due to the limited onboard computing capacity, the regional partition method proposed in this paper can reduce the computing burden of the master node and reduce the network load. When dividing the region, considering that the adjacent satellite links in the same orbit are stable and the adjacent satellite links between orbits may change, the five satellites with a relatively close distance in the same orbit are divided into a region. In this region, satellites at both ends can send data to the main satellite in the middle of the region with only one or two hops. When weighing the size of the region, the number of blocks generated per unit time should be reduced as much as possible to reduce the number of broadcasts to reduce the load of inter-satellite links. Therefore, the region should be set larger. However, when generating blocks, the region should be set smaller to ensure the speed of transaction transmission within the region. Therefore, in the network topology of a satellite system, the above two factors are taken into account when dividing regions into appropriate sizes. For example, in the Iridium system, five satellites in the same orbit are divided into one region, as shown

in Figure 7. Since the Iridium satellite system has six orbits with 11 satellites in each orbit, it is divided into 12 regions with two regions in each orbit. The purpose of this division is to ensure a low transmission delay in the region as much as possible and to let all nodes in the region share the computing overhead of the entire region without requiring a single node to undertake all computing. At the same time, transactions are verified by each receiving node, avoiding repeated broadcast of transactions and reducing the load of the entire network.

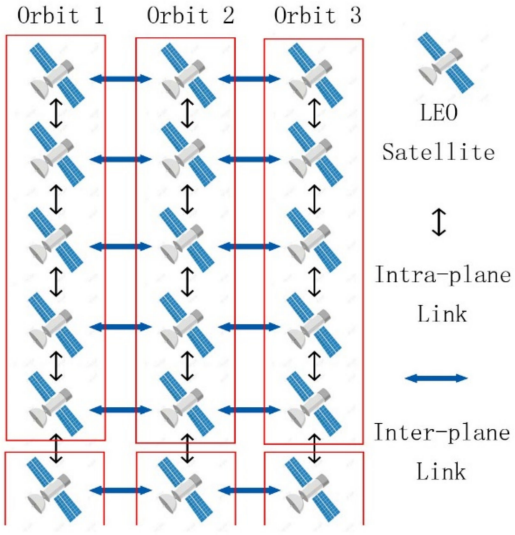

Figure 7. Regional division based on the Iridium satellite system.

5.2. Computational Overhead

In the traditional accounting process, all transactions in the network are verified by the node with the right of accounting alone, which will consume considerable computing power and time for a single node. In this paper, multiple satellite nodes are divided into the same region to share the total computing overhead in the region. When a satellite node receives a transaction, it does not broadcast it but stores it temporarily in the local cache pool. Each region takes turns in bookkeeping. When the region obtains the right of bookkeeping, the master node does not need to verify all transactions in the region alone. Instead, each node in the region first validates the transaction they receive independently. Then, the node forms the transaction tree that passes the verification and calculates the root hash. Finally, the node sends the transaction tree and root hash to the master node. After receiving all transaction trees in the region, the master node forms a larger transaction tree and calculates the final root hash. In this process, each subtree is calculated separately by each satellite node; thus, the calculation in the region is dispersed to each node. Therefore, the master node does not need much calculation, and the partition method reduces the calculation overhead and time of the master node when verifying transactions and calculating hashing.

5.3. Network Load

In a traditional blockchain, when a node in the network receives a transaction, it broadcast the transaction immediately, and wait for miners to compete for the right of bookkeeping and package the transaction, at which point a large number of transactions are constantly transmitting around the network. In this paper, after regional division, each node calculates the transaction received separately; therefore, when the satellite node receives the transaction, there is no need to broadcast. After each satellite node in the region completes the verification transaction and calculates the hash, it sends the valid transaction and hash results to the master node, and then the master node broadcasts after completing the packaging of the transaction and the generation of new blocks. In this way, the transaction need to broadcast only once in the network, which can avoid repeated

broadcast of the transaction and reduce the amount of data transmitted in the network and significantly reducing the network load.

6. Protocol Comparison and Security Analysis

In this section, we compare our proposed protocol with two other authentication protocols in terms of computing overhead and key security against replay attacks, denial of service attacks and impersonation attacks.

6.1. Computational Overhead

The comparison results are shown in Table 1. In the *X*/*Y*s in the table, *X* represents the calculation times of user operations, and *Y* represents the calculation times of satellite operations. In *X*/*Y*/*Z*, *X* remains the same, *Y* represents the calculation times of satellite operations before the switchover, and *Z* is the times after the switchover. In communication times, users send messages to satellites, satellites to users or satellites to satellites as communication. We compare three protocols: Fast-access, Handover and our protocol BAPC. The Fast-access and the Handover algorithms are the protocols in [26], and we adopt similar settings in our simulation. Compared with other related protocols, BAPC is better in computing overhead. According to the analysis, two comparison protocols require hash operation, but BAPC does not require hash operation. In addition, the operation of asymmetric encryption, signature and verification operation in BAPC is one times on both the client side and satellite side, which is at the average computation level compared with other protocols. In terms of communication times, the comparison protocols are 2 and 4 times, and BAPC is 2 times, which is less.

Table 1. Calculation comparison of the authentication stage.

Operation Type	Fast-Access	Handover	BAPC
Hash Operation	1/1	-/-/2	-/-
Asymmetric Enc/Dec	1/1	-/-/1	1/1
Signing Operation	1/1	1/1/1	1/1
Signature Verification	1/1	1/-/2	1/1
Communication Times	2	4	2

6.2. Key Safety

When the user needs to establish a new account, the user uses the key generator provided by the authentication center to directly generate the public key, private key and address locally. In this process, the private key is not transmitted through any channel, and neither the authentication center nor the satellite knows the user's private key. In the cryptocurrency technology, the user address is generated by the user's public key through a predetermined hash algorithm. The user address and the public key form a one-to-one correspondence and are stored in the blockchain. In the authentication process, the attacker attempts to intercept the information and tamper with the information using the attacker's public key and private key, and send it to the satellite. When the attacker is not registered, it does not have a legal public key. Since the attacker's address is not stored in the blockchain, the satellite will not believe such information. When the attacker has registered, since the transaction which is submitted in the registration stage is saved on the blockchain and the attacker's legal public key corresponds to the transaction information, the attacker cannot interfere with other users. Therefore, the public key identity of legitimate users is guaranteed.

6.3. Replay Attacks

BAPC uses timestamp to defend against replay attacks. During the registration stage, users need to pay legal tender to obtain the corresponding amount of cryptocurrency, and attackers cannot benefit from replaying such messages. During the initial authentication stage and switching authentication stage, the user initiates a transaction to obtain the

service, and the timestamp is stored in the transaction information. When an attacker replays such messages, it cannot sign them properly or change the timestamp. When the satellite node receives multiple transactions with the same timestamp, it will judge the later one as an invalid transaction and reject the request from the attacker. If the attacker intercepts the request by the user and then replays the request to obtain the service, the session key returned by the satellite is encrypted with the user's public key, and only the user's private key can be decrypted to obtain the session key. Without the private key, the attacker cannot obtain the service. As to resisting replay attacks, BAPC is similar to the method used by traditional encryption protocols and our protocol can also resist such attacks.

6.4. Denial-of-Service Attacks

BAPC adds to the cryptocurrency system, applying economic costs to defend against the Denial-of-Service attacks. In the registration stage, initiating payment requests requires a small amount of upfront capital. The attacker will therefore spend a large amount of upfront capital if continuously initiating payment requests. During the initial authentication phase, authentication costs cryptocurrencies, which are converted by the cost of capital. If an attacker repeatedly initiates initial authentication, the attacker incurs significant cryptocurrency costs. In the switching authentication phase, a deposit is required before authentication. When the transaction is not verified, a certain margin will be deducted. Because the authentication request initiated by the attacker cannot be authenticated, a large margin is consumed. If normal users continuously initiate requests, the satellite node can limit the number of requests from the same user address within a certain period of time.

6.5. Impersonation Attacks

An attacker may attempt to impersonate a user to send an authentication request to a satellite. However, without the user's private key, the attacker cannot give the correct signature. When the attacker impersonates a user's request to the satellite with his own public key, the request cannot pass the verification of the satellite. Since only the addresses of legitimate users are stored in the blockchain, there is no address corresponding to the attacker's public key. At the same time, the attacker cannot obtain the correct session key from the message encrypted with the public key and cannot use the service. If an attacker impersonates a satellite by sending a message to the user, since the attacker does not have the private key of the satellite, the signature cannot be verified by the user, and the user will discard the message.

6.6. Man-in-the-Middle Attacks

Man-in-the-middle attack is a common means of network intrusion. Man-in-the-middle attack means that the attacker obtains the communication information of both sides through illegal eavesdropping, and then intercepts and tampers with the message to control the whole session. The fundamental reason that man-in-the-middle attack may succeed is that both parties cannot prove their identity through identity authentication. In BAPC, when an attacker intercepts a user's message and tampers with the attacker's public key, the satellite can easily identify the illegal public key. Because the attacker's address cannot be found on the blockchain as legal users save the address on the blockchain through the registration stage. If the attacker uses his registered legal address, the satellite will know that it is communicating with the attacker, not a normal user.

7. Simulation and Evaluation

In this section, we adopt the Iridium LEO satellite network scenario and conduct a performance simulation of our BAPC protocol. The experimental environment is the NS2 platform, which uses the Ethereum key generation algorithm and signature verification algorithm.

7.1. Simulation Parameters

In the simulation, the altitude is set to 780 km, the inclination angle is 86.4°, the orbital period is 6027.14 s, the uplink and downlink bandwidth is 1.5 Mb/s, and the inter-satellite link bandwidth is 25 Mb/s. There are 6 orbits in total, with 11 satellites in each orbit.

In the simulation of the switching authentication stage, 60 ground terminals play the role of users, evenly distributed between 60° S and 60° N. The fields contained in BAPC are set using the actual algorithm, and the size of the related fields is shown in Table 2: 64 bytes for the user public key, 20 bytes for the address, 65 bytes for the signature, 128 bytes for the session key, and 4 bytes for the service type, service duration, timestamp, and quantity of cryptocurrency. Two authentication protocols are used for comparison: In reference [26], the Fast-access protocol is used for in-orbit switching authentication; and the Handover protocol is used for cross orbit handover authentication. In LEO satellite networks, there is still limited work considering blockchain-based authentication. We choose this protocol to compare because their work is closest to ours. They also apply the blockchain technology to the authentication process in LEO satellite networks to help satellites authenticate user identity more efficiently. However, the benchmark protocol uses the identity-based encryption key, while our protocol uses the cryptocurrency technology.

Table 2. Settings of the simulation.

Field	Length/Byte	Field	Length/Byte
Pk	64	Server	4
Address	20	Duration	4
Signature	65	Timestamp	4
Session Key	128	Amount	4

7.2. Switching Authentication Time

We set the maximum number of simultaneous online users of the Iridium satellite system to 150,000 [25]. Assuming that users are evenly distributed, it takes approximately 2 h for a satellite to orbit the earth, and the available service time for a stationary ground user is approximately 10 min in Iridium. Therefore, ground users need to initiate a switching authentication request to the satellite every 10 min, and a single satellite needs to process four user authentication requests every second. The simulation experiment is set to run for 1 h, and the number of users that a single satellite needs to process per second is successively considered in four cases λ: 4, 8, 16 and 32. The simulation results are shown in Figure 8. When processing 4 user requests per second, the response time is 0.026 s for the BAPC protocol, 0.019 s for the Fast-access protocol and 0.044 s for the Handover protocol. As the number of users increases, the response time of each protocol increases linearly. BAPC reduces the response time by 39% to 43% compared with the Handover protocol in terms of the interval between 4 and 32 users.

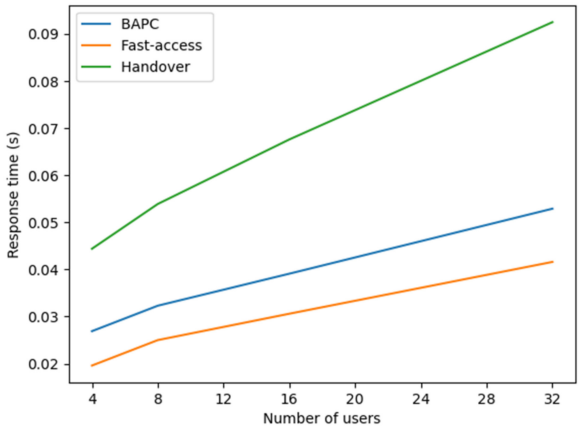

Figure 8. Comparison of the authentication response time.

In general, our BAPC authentication protocol shows a better comprehensive performance other protocols. Compared with the Fast-access authentication protocol, it transmits less data and has no intersatellite communication; therefore, it is slightly superior to BAPC. However, the restrictions are more stringent, requiring satellites in the same orbit. As the satellite moves, satellites in the same orbit do not keep circular coverage of the same location. In practice, users most likely need handover authentication between different orbits. BAPC is better than its Handover authentication protocol.

At the same time, compared with other satellite access authentication protocols, BAPC does not distinguish between intraregional authentication and cross-regional authentication, nor does it require that the satellite for access authentication be in the same orbit or adjacent satellite across orbit. BAPC can be used for different types of switching authentication, which is more suitable for LEO satellite networks with constantly changing links. In addition, user authentication information is basically stored on the blockchain, which has high scalability. Based on blockchain and cryptocurrency, BAPC securely stores user authentication information in a distributed ledger, reducing the cost of communication between users and satellites and bringing lower communication cost with tolerable storage cost. For an increasing amount of data, a certain mechanism can be used to clear the data and maintain sufficient storage space.

7.3. Block Generation Time

We then compare the generation time of blocks without partitioning and after partitioning, as shown in Figure 9. When the number of users processed by a single satellite is 4 per second, the time of block generation is 0.122 s without regional division and 0.053 s after regional division, which reduces the time consumed by 56%. In the case of no regional division, the calculation amount of the primary node is 5 times that after regional division. As the number of users increases, the time of verifying transactions on the primary node keeps increasing. Meanwhile, the ratio of time shortening increases with the increase in the number of users. With 32 users, the time after partition shortens by 74%.

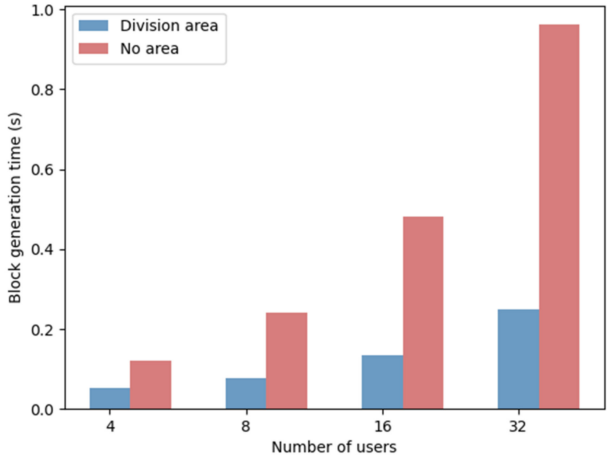

Figure 9. Comparison of block generation time.

7.4. Network Throughput

In the process of block consensus, the broadcast of a large number of transactions will increase the network throughput. This section compares the throughput without regional division and after regional division, as shown in Figure 10. When the number of users processed by a single satellite is 4 per second and no region is divided, the network throughput is 5.139 MB/s in the process of block consensus and 1.462 MB/s after regional division. From a range of 4 to 32 users, with an increase in the number of users, the growth rate of network throughput in divided regions and non-divided regions is similar, and the network throughput decreases by 71% after the region is divided.

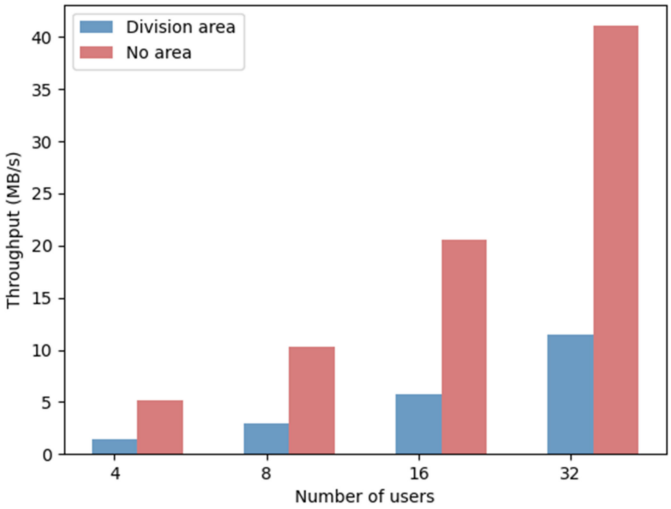

Figure 10. Comparison of network throughput.

7.5. Signature and Verification Time

Python is used to repeatedly test the computation speed of the signature and verification. This test uses Ethereum's generation algorithm of public keys and private keys and address, and signature algorithm and verification algorithm. As shown in Figure 11, it takes 0.003 s or 0.004 s to sign transactions, with similar frequency and an average time of approximately 0.0035 s. The time of signature verification is 0.005 s or 0.006 s with similar frequency, and the average time is approximately 0.0055 s. In the simulation of switching authentication, there is a satellite verification calculation and a satellite signature calculation.

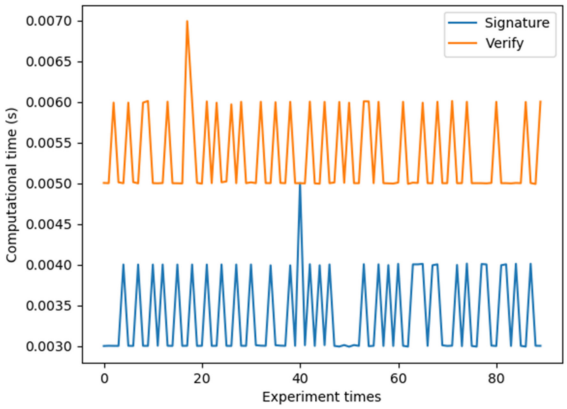

Figure 11. The computational time for signing and verifying transactions.

8. Conclusions and Future Work

In LEO satellite networks, the satellite moves constantly, and so does the coverage area. Therefore, the satellite-ground link needs frequent switching and it is of great significance to study how to ensure reliable and fast switching authentication. This paper proposes an LEO satellite network authentication protocol based on blockchain and cryptocurrency. First, three stages of access authentication are designed. After the registration and initial authentication are completed, users can achieve fast switching authentication. Second, the regional division scheme is studied to improve the efficiency of generating blocks. Finally, we realize the authentication protocol on the NS2 network simulation platform. The experimental results show that compared with other authentication protocols, BAPC has better security. Additionally, it not only greatly reduces the response time of the switching authentication and improves the efficiency of the switching authentication, but also significantly reduces the block generation time and network throughput.

However, as satellites are with limited storage capacity, the ever-increasing volume of blockchain data becomes an urgent problem to be solved. In our follow-up work, how to better optimize the amount of data stored on the satellite side under the condition of ensuring the reliability of authentication information will be studied. Moreover, it is meaningful to conduct experiments on real LEO satellites or emulation platforms. In the future, if there are opportunities, we will make real measurements on LEO satellites.

Author Contributions: Conceptualization, X.D. and L.C.; methodology, J.S.; validation, J.S.; formal analysis, J.S. and L.C.; investigation, X.D., L.C.; data curation, J.S.; writing—original draft preparation, J.S.; writing—review and editing, X.D., L.C.; supervision, X.D.; project administration, X.D.; funding acquisition, X.D., L.C. and J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (Grant No. 61702127), Science and Technology Program of Guangzhou (Grant No. 201804010461), the China Scholarship Council (Grant No. 201908440064, 201908440085), Hundred Young Talents Plan Project of Guangdong University of Technology (Grant No. 220413618), the Guangxi Innovation-driven Development Major Project Platform (No. Guike AA20302002), and the Guangxi Science and Technology Base and Talents Special Project (No. Guike AD21076002).

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

References

1. Liu, J.; Shi, Y.; Fadlullah, Z.M.; Kato, N. Space-air-ground integrated network: A survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2714–2741. [CrossRef]
2. Zhang, N.; Zhang, S.; Yang, P.; Alhussein, O.; Zhuang, W.; Shen, X.S. Software defined space-air-ground integrated vehicular networks: Challenges and solutions. *IEEE Commun. Mag.* **2017**, *55*, 101–109. [CrossRef]
3. Su, Y.; Liu, Y.; Zhou, Y.; Yuan, J.; Cao, H.; Shi, J. Broadband leo satellite communications: Architectures and key technologies. *IEEE Wirel. Commun.* **2019**, *26*, 55–61. [CrossRef]
4. Hu, J.; Cai, L.; Zhao, C.; Pan, J. Directed percolation routing for ultra-reliable and low-latency services in low earth orbit (LEO) satellite networks. In Proceedings of the IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), New Network Architecture Powering Internet-of-Things Workshop, Victoria, BC, Canada, 18 November–16 December 2020.
5. Wei, J.; Han, J.; Cao, S. Satellite IoT Edge Intelligent Computing: A Research on Architecture. *Electronics* **2019**, *8*, 1247. [CrossRef]
6. Ge, H.; Li, B.; Ge, M.; Zang, N.; Nie, L.; Shen, Y.; Schuh, H. Initial Assessment of Precise Point Positioning with LEO Enhanced Global Navigation Satellite Systems (LeGNSS). *Remote Sens.* **2018**, *10*, 984. [CrossRef]
7. Shukla, A.; Gupta, R.; Tanwar, S.; Kumar, N.; Rodrigues, J.J.P.C. Block-RAS: A P2P Resource Allocation Scheme in 6G Environment with Public Blockchains. In Proceedings of the IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [CrossRef]
8. Hyland-Wood, D.; Robinson, P.; Saltini, R.; Johnson, S.; Hare, C. Methods for securing spacecraft tasking and control via an enterprise Ethereum blockchain. Advances in Communications Satellite Systems. In Proceedings of the 37th International Communications Satellite Systems Conference (ICSSC-2019), Okinawa, Japan, 29 October–1 November 2019; pp. 1–16. [CrossRef]
9. Ling, X.; Gao, Z.; Le, Y.; You, L.; Wang, J.; Ding, Z.; Gao, X. Satellite-Aided Consensus Protocol for Scalable Blockchains. *Sensors* **2020**, *20*, 5616. [CrossRef]
10. Hu, Y.; Manzoor, A.; Ekparinya, P.; Liyanage, M.; Thilakarathna, K.; Jourjon, G.; Seneviratne, A. A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain. *IEEE Access* **2019**, *7*, 33159–33172. [CrossRef]
11. Petrovic, R.; Simic, D.; Cica, Z.; Drajic, D.; Nerandzic, M.; Nikolic, D. IoT OTH Maritime Surveillance Service over Satellite Network in Equatorial Environment: Analysis, Design and Deployment. *Electronics* **2021**, *10*, 2070. [CrossRef]
12. Papafragkakis, A.; Kouroriorgas, C.; Panagopoulos, A. Performance of Micro-Scale Transmission Reception Diversity Schemes in High Throughput Satellite Communication Networks. *Electronics* **2021**, *10*, 2073. [CrossRef]
13. Guo, K.; Lin, M.; Zhang, B.; Wang, J.-B.; Wu, Y.; Zhu, W.-P.; Cheng, J. Performance analysis of hybrid satellite-terrestrial cooperative networks with relay selection. *IEEE Trans. Veh. Technol.* **2020**, *69*, 9053–9067. [CrossRef]
14. Kodheli, O.; Lagunas, E.; Maturo, N.; Sharma, S.K.; Shankar, B.; Montoya, J.F.M.; Duncan, J.C.M.; Spano, D.; Chatzinotas, S.; Kisseleff, S.; et al. Satellite Communications in the New Space Era: A Survey and Future Challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 70–109. [CrossRef]
15. Giambene, G.; Kota, S.; Pillai, P. Satellite-5G Integration: A Network Perspective. *IEEE Netw.* **2018**, *32*, 25–31. [CrossRef]
16. Ao, W.; Fu, S.; Zhang, C.; Huang, Y.; Xia, F. A Secure Identity Authentication Scheme Based on Blockchain and Identity-based Cryptography. In Proceedings of the IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET), Beijing, China, 16–18 August 2019; pp. 90–95. [CrossRef]

17. Cao, S.; Dang, S.; Zhang, Y.; Wang, W.; Cheng, N. A blockchain-based access control and intrusion detection framework for satellite communication systems. *Comput. Commun.* **2021**, *172*, 216–225. [CrossRef]
18. Zhang, F.-T.; Sun, Y.-X.; Zhang, L.; Geng, M.; Li, S. Research on certificateless public key cryptography. *J. Softw.* **2011**, *22*, 1316–1332. [CrossRef]
19. Cruickshank, H.S. A security system for satellite networks. In Proceedings of the Fifth International Conference on Satellite Systems for Mobile Communications and Navigation, London, UK, 13–15 May 1996; pp. 187–190. [CrossRef]
20. Wu, Z.; Liu, R.; Cao, H. ECDSA-Based Message Authentication Scheme for BeiDou-II Navigation Satellite System. *IEEE Trans. Aerosp. Electron. Syst.* **2019**, *55*, 1666–1682. [CrossRef]
21. Altaf, I.; Saleem, M.A.; Mahmood, K.; Kumari, S.; Chaudhary, P.; Chen, C. A Lightweight Key Agreement and Authentication Scheme for Satellite-Communication Systems. *IEEE Access* **2020**, *8*, 46278–46287. [CrossRef]
22. Meng, W.; Xue, K.; Xu, J.; Hong, J.; Yu, N. Low-Latency Authentication Against Satellite Compromising for Space Information Network. In Proceedings of the IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Chengdu, China, 9–12 October 2018; pp. 237–244. [CrossRef]
23. Pokhrel, S.R. Blockchain Brings Trust to Collaborative Drones and LEO Satellites: An Intelligent Decentralized Learning in the Space. *IEEE Sens. J.* **2021**, *21*, 25331–25339. [CrossRef]
24. Ibrahim, H.; Shouman, M.A.; El-Fishawy, N.A.; Ahmed, A. Literature Review of Blockchain Technology in Space Industry: Challenges and Applications. In Proceedings of the International Conference on Electronic Engineering (ICEEM), Menouf, Egypt, 3–4 July 2021; pp. 1–8. [CrossRef]
25. Wei, S.; Li, S.; Mo, B.; Wang, J. Regional Cooperative Authentication Protocol for LEO Satellite Networks Based on Consensus Mechanism. *J. Comput. Res. Dev.* **2018**, *55*, 2244–2255.
26. Wei, S.; Li, S.; Liu, P.; Liu, M.; Wang, G. BAVP: Blockchain-Based Access Verification Protocol in LEO Constellation Using IBE Keys. *Secur. Commun. Netw.* **2018**, *2018*, 1–14. [CrossRef]
27. Feng, M.; Xu, H. MSNET-Blockchain: A New Framework for Securing Mobile Satellite Communication Network. In Proceedings of the 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA, 10–13 June 2019; pp. 1–9. [CrossRef]
28. Wei, H.; Feng, W.; Zhang, C.; Chen, Y.; Fang, Y.; Ge, N. Creating Efficient Blockchains for the Internet of Things by Coordinated Satellite-Terrestrial Networks. *IEEE Wirel. Commun.* **2020**, *27*, 104–110. [CrossRef]
29. Clark, L.; Tung, Y.-C.; Clark, M.; Zapanta, L. A Blockchain-based Reputation System for Small Satellite Relay Networks. In Proceedings of the IEEE Aerospace Conference, Big Sky, MT, USA, 7–14 March 2020; pp. 1–8. [CrossRef]
30. Beaujardiere, J.; Mital, R.; Mital, R. Blockchain Application Within a Multi-Sensor Satellite Architecture. In Proceedings of the IEEE International Geoscience and Remote Sensing Symposium, Yokohama, Japan, 28 July–2 August 2019.
31. Suciu, G.; Nădrag, C.; Istrate, C.; Vulpe, A.; Ditu, M.; Subea, O. Comparative Analysis of Distributed Ledger Technologies. In Proceedings of the Global Wireless Summit (GWS), Chiang Rai, Thailand, 25–28 November 2018; pp. 370–373. [CrossRef]
32. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. *Blockchain Technology Overview*; NIST Interagency/Internal Report (NISTIR); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. [CrossRef]
33. Tschorsch, F.; Scheuermann, B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2084–2123. [CrossRef]
34. Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.A.; Felten, E.W. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA, 17–21 May 2015; pp. 104–121. [CrossRef]
35. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA, 22–16 May 2016; pp. 839–858. [CrossRef]
36. Monrat, A.A.; Schelén, O.; Andersson, K. Performance Evaluation of Permissioned Blockchain Platforms. In Proceedings of the IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Gold Coast, Australia, 16–18 December 2020; pp. 1–8. [CrossRef]