Article

A Blockchain Protocol for Authenticating Space Communications between Satellites Constellations

Mohamed Torky [1,*,†] , Tarek Gaber [2,3,†] , Essam Goda [4,†] , Vaclav Snasel [5] and Aboul Ella Hassanien [6,*,†]

1   Department of Computer Science, Higher Institute of Computer Science and Information Systems, Culture & Science City, 6th of October City 3226010, Egypt
2   School of Science, Engineering and Environment, University of Salford, Manchester M50 2EQ, UK
3   Faculty of Computers and Informatics, Suez Canal University, Ismailia 8366004, Egypt
4   College of Computing and Information Technology (CCIT), Arab Academy for Science, Technology and Maritime Transport (AASTMT), Giza 3650111, Egypt
5   Department of Computer Science, VSB Technical University of Ostrava, 70032 Ostrava, Czech Republic
6   Faculty of Computers and Artificial Intelligence, Cairo University, Cairo 12613, Egypt
*   Correspondence: mtorky86@gmail.com (M.T.); aboitcairo@fci-cu.edu.eg (A.E.H.)
†   Scientific Research Group in Egypt (SRGE).

Abstract: Blockchain has found many applications, apart from Bitcoin, in different fields and it has the potential to be very useful in the satellite communications and space industries. Decentralized and secure protocols for processing and manipulating space transactions of satellite swarms in the form of Space Digital Tokens (SDT) can be built using blockchain technology. Tokenizing space transactions using SDTs will open the door to different new blockchain-based solutions for the advancement of constellation-based satellite communications in the space industry. Developing blockchain solutions using smart contracts could be used in securely authenticating various P2P satellite communications and transactions within/between satellite swarms. To manage and secure these transactions, using the proposed SDT concept, this paper suggested a blockchain-based protocol called Proof of Space Transactions (PoST). This protocol was adopted to manage and authenticate the transactions of satellite constellations in a P2P connection. The PoST protocol was prototyped using the Ethereum blockchain and experimented with to evaluate its performance using four metrics: read latency, read throughput, transaction latency, and transaction throughput. The simulation results clarified the efficiency of the proposed PoST protocol in processing and verifying satellite transactions in a short time according to read and transaction latency results. Moreover, the security results showed that the proposed PoST protocol is secure and efficient in verifying satellite transactions according to true positive rate (TPR), true negative rate (TNR), and accuracy metrics. These findings may shape a real attempt to develop a new generation of Blockchain-based satellite constellation systems.

Keywords: blockchain; Proof of Space Transactions (PoST); satellites constellations; satellites communications; satellites authentication

1. Introduction

According to the space report 2020 Q2 analysis Global Space Economy Grows in 2019 to \$423.8 Billion, this growth represents a 2.2% increase from the 2018 global space economy which was estimated at \$414.75 billion [1]. It is very difficult to imagine our modern life without satellite-based services such as digital maps, navigation, mobile communication, etc. Such services are mainly based on various types of space technologies and satellite transactions [2]. The design of new generations of satellite systems has become dependent on different types of emergent technologies such as Artificial Intelligence (AI) [3–5], Internet of Things (IoT) [6–8], Edge Computing [9–11], and quantum computing [12–15], etc. Blockchain technology has fast become also one of the major technologies that can be used for solving many challenges in the global space industry [16–18]. Blockchain can

create many opportunities such as satellite-as-a-service business models, managing the space supply chain, and even how to build satellite payloads. Moreover, blockchain will make a major transformation in the next generation of financial transactions. Transferring the Bitcoin Blockchain via satellite will make a quantum leap in global financial transactions and grant a robust alternative to terrestrial networks. The Blockstream Satellite network [19] represents a practical application of utilizing blockchain-based satellites for processing and broadcasting the bitcoin to the entire planet without the need for the Internet. For Instance, in 2017, a technical error by Google briefly caused more than half of Japan to lose its connection to the internet. While internet access was returned within the hour, the Japanese faced slow connection speeds, which directly affected financial transactions, and online trading was halted. In this scenario, broadcasting the bitcoin blockchain via satellite would have ensured that the financial transactions are not been halted. Moreover, blockchain remained in sync with the rest of the globe and thus, unaffected by internet disconnect [20]. Moreover, the common characteristics of blockchain technology such as robustness, trust, security, transparency, decentralized connections, and time stamping transactions make it a key technology for managing and securing space communications because it cannot be hacked or centrally controlled. These characteristics make blockchain a qualified technology for providing various services in the space industry [20] such as:

- *Enhancing the Satellite Value Chain*: Blockchain as a smart contract can be used for launching and operating satellites, accessing transparent information for insurance purposes, and monitoring space operations. Moreover, satellites can also be basic sources of space transactional data for upgrading blocks and verifying the integrity and origin of these data patterns.
- *Enabling Cloud Services in Space*: levering both blockchain and AI can enable a cloud transformation and processing in space. Blockchain over satellite removes the dependence on terrestrial networks for the storage, broadcasting, or processing of space data, hence eliminating significant vulnerabilities for a data breach or distortion. testing, and launching. In the future, the blockchain-satellite system will depend on a cloud constellation for managing data centers in orbits where companies can upload their data and bypass the ground networks; this will help the governments and companies to get information from different sources and orbits in space [20].
- *Designing Open source Satellite*: Large space companies started to develop blockchain-based open-source satellite networks for providing many services to end-users on the ground and enabling them to directly access satellite services. For instance, Singapore-based Space Chain [21] has begun to build the world's first open-source Blockchain-based satellite network. Space Chain permits end users to develop and run decentralized applications by accessing the open-source satellites in space.

1.1. Problem Statement

Most of the global space agencies have begun to rely on launching satellites in the form of a constellation (or swarm) that work together to accomplish a specific space mission instead of relying on a single satellite [22]. Unlike a single satellite, a constellation can grant permanent global coverage everywhere at any time on Earth. Therefore, at least one satellite is available to respond to ground instructions at any time everywhere. Many types of satellite constellations have been launched for various missions, for example, navigational satellite constellations (e.g., global positioning system (GPS)). But, a satellite constellation is vulnerable to some cyber-attacks that aim to disrupt one satellite or all satellites of the constellation such as hacking, spoofing, interference, and jamming attacks [23]. For instance, hacking the very small aperture terminal (VSAT) (VAST is a small-sized ground station utilized to transmit/receive data, audio, and video signals over a satellite communication network, excluding television broadcasting) is the most common hacking technique which aims to access uplink and downlink data from/to VSAT device [24]. Moreover, the failure to encrypt uplink/downlink data can expose satellites and ground stations to spoofing attacks [25]. In addition, jamming the control link of the uplink data may noise ground

stations' commands sent to a satellite or a constellation system. On the other hand, hijacking and control of satellite signals transmitted between two satellites or between satellites and ground stations represent another important security challenge in space communication. Therefore, authenticating space transactions, especially regarding satellite constellation networks is one of the important issues. In response to these challenges, a novel blockchain protocol for managing and securing satellite transactions called Proof of space transactions (PoST) is proposed. This protocol is based on a new concept called space digital tokens (SDT). The main objective of the proposed PoST is to manage and authenticate satellite communications using blockchain.

To achieve these objectives, the following assumptions have to be existing:

1. Satellites revolve around the earth within a swarm (or a constellation). An international association or a space agency can manage each swarm.
2. The satellite communication within/between constellations is conducted through a peer-to-peer network.
3. The Blockchain statue is shared with all satellites in the same swarm.

1.2. Paper Contribution

The main contribution of this study is three folds:

1. Modeling the space transactions as Space digital tokens (SDT) and using these tokens in proposing a novel PoST protocol which was then used in proposing a new authentication protocol for satellite communications and transactions using the blockchain technology.
2. The PoST and the authentication protocol were also evaluated by prototyping them and their performance was measured using five metrics: read latency, read throughput, transaction latency, and transaction throughput.
3. The PoST protocol was also compared and discussed with the most related work.

1.3. Paper Structure

The rest of this paper is organized as follows: Section 2 presents the literature review. Section 3 discusses the concept, of space digital tokens (SDT). Section 4 discusses a proposed blockchain protocol, Proof of space transaction (PoST). Section 5 presents the simulation results. Section 6 discusses the obtained results, and Section 7 presents the conclusion and future work.

2. Literature Review

There is a relatively small number of literature that is concerned with integrating blockchain technology with space industry applications. Clark et al. [26] proposed a blockchain-based reputation system for developing a decentralized and secure system for satellite relay networks. The authors investigated and validated the network performance using average latency, computational complexity, and storage considerations for a variety of use cases. Feng and Xu [16] studied the security problem for mobile satellite communication networks (MSNET). The authors proposed a new security framework for securing mobile satellite communication networks based on reformulating satellite communication networks as delay-tolerance networks (DTN). The blockchain is used with DTN to (1) secure data transactions and (2) resist the unexpected cyber-attacks that target mobile satellite networks by integrating blockchain with the practical satellite constellation management algorithm. Wei et al. [27] proposed a fast and efficient access verification protocol called Blockchain-based Access Verification Protocol (BAVP) that depends on integrating identity-based encryption and blockchain technology for authenticating LEO-satellite constellations. The BAVP represents a good alternative instead of the traditional centralized authentication protocols that work for MEO/GEO satellite networks. The simulation results on the OPNET platform clarified good results of the reliability, effectiveness, and fast-switching efficiency of the proposed protocol. Also, Xu et al. [28] proposed a blockchain-based access control mechanism for addressing both access authorization issues and identity authentication

in the distributed space network environment. The author implemented the proposed mechanism on both resource-constrained edge devices and more powerful devices and deployed it on a local private Ethereum blockchain network for evaluating the computational and timeliness performance of the proposed access control mechanism. Satellite data broadcasting is another problem that has been investigated in blockchain adoption in the space industry. Zhang and Liu in [29] introduced a new blockchain protocol that works based on satellite broadcasting communications instead of the traditional Internet for data dissemination. Simulation results clarified that the proposed technique achieved a lower communication cost and can improve the throughput of the blockchain system to 6,000,000 TPS with a 20 Gbps satellite bandwidth. From the literature, it can be noticed that there is no solution aiming to manage and authenticate satellite communications using blockchain. There is no work addressing the management of transactions between two satellites in the same constellation (or swarm) or transactions between two/more satellites in different constellations. These will be addressed in this paper.

3. Space Digital Tokens (SDT) Concept

In this section, a new concept called Space Digital Token (SDT) is proposed. The SDT is a way of tokenizing space transactions as digital tokens that can be processed using a blockchain protocol for authenticating space transactions. SDT can be broadcasted within a swarm of satellites network called a satellites constellation. Hence, blockchain can work in this scenario as an authenticator for all communication patterns that can occur within a specific satellite's constellation. SDT can also be used for processing sensing data between satellites and orbital debris, hence, blockchain can works in this scenario as a tracking system for detecting the expected space collisions between satellites and orbital debris. Figure 1 depicts the modeling of space digital tokens using blockchain. It explains how space transactions can be modeled as Space Digital Tokens (SDT) and processed using a blockchain protocol. SDT can be either a transaction exchanged from a satellite to a satellite within a P2P satellite network or maybe in the form of sensing data between a satellite and orbital debris. The blockchain protocol is responsible for verifying the new space transactions to add a new valid block to the blockchain. All space stakeholders would be then able to access the newly added blocks through the connected dashboard to the blockchain platform that manages a satellite constellation.

The main advantages of tokenizing space transactions as SDT and processing them using blockchain technology can be described as follows:

(1) Better Control of satellite transactions: It would be easier to track, process, validate, and secure all space-related activities when space transactions are tokenized into secure digital tokens. Furthermore, managing and processing them via a smart contract-based blockchain system will facilitate satellite transaction self-verification and execution. Hence, this will lead to a little dependency on the ground stations. In addition, the intended space stakeholders will have better control to allow or deny access to their satellites and spacecraft or share data from or to a satellites network.

(2) Faster transactions management: Space transaction management relies heavily on compliance and responsiveness. When it comes to automating different space transaction patterns like satellite-to-satellite (S2S), ground station-to–satellite (G2S), and user- to-satellite (U2S), blockchain could be helpful. Blockchain-based systems would minimize the time taken by a space message to get to the ground station. This could be achieved as the blockchain can, in real-time, manage down/uplink G2S or S2G transactions.

(3) Security: Traditional satellite communication systems rely on a single-point-of-access model that introduces significant security issues. Blockchain would help in the decentralization of space networks where space transactions are cryptographically encrypted and tampered-proof. Moreover, blockchain can help space agencies to track and monitor their satellite constellations in a controlled and flexible manner. This

help to detect satellite/constellations attacks that seeks to tamper with the satellite software system using space bots [30].
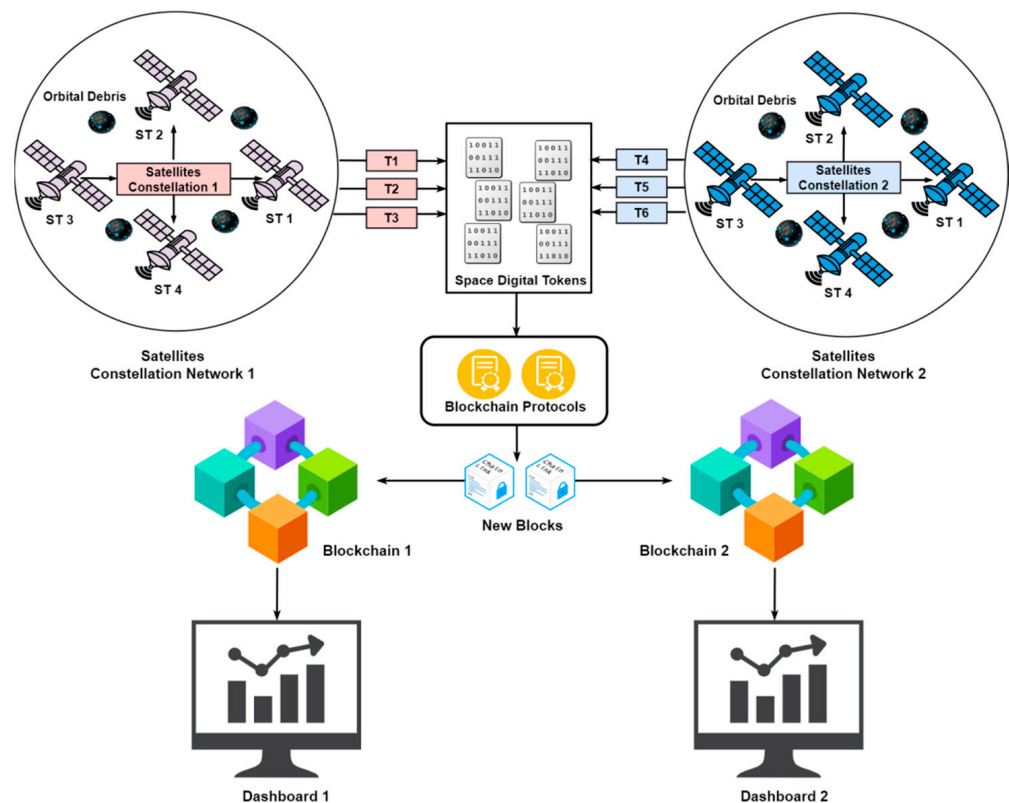

Figure 1. Modeling space digital tokens using Blockchain.

4. Proof of Space Transactions Protocol

Proof of Space Transactions (PoST) is a novel proposed blockchain protocol that can be utilized to verify space digital tokens (SDTs) within/between satellite constellations. PoST methodology requires representing each satellite within a constellation with a private key and a piece of cryptographic evidence for authenticating a specific SDT. When a new SDT is triggered between two satellites, the source of a transaction has to share the cryptographic evidence of this transaction with the rest of the satellites constellation to confirm the validity of the triggered SDT. In addition, the target satellite requests the Nonce code of the last block of the Blockchain. Once the target satellite confirms the Nonce code, a new block is added to the blockchain. Figure 2 explains how the PoST protocol verifies and authenticates an SDT that has been exchanged between two satellites within the same constellation through eight steps.

Step 1: Satellite A creates a new transaction (i.e., SDT) with satellite B.

Step 2: Satellite B asks for the cryptographic evidence (i.e., proof) associated with the issued SDT

Step 3: Satellite A replies with the SDT proof to satellite B

Step 4: Proof of Space Transactions (PoST) protocol is automatically called to verify the validity of the conducted transaction between satellites A, and B

Step 5: Satellite B asks the nonce code of the last block in the Blockchain to establish the new connection with satellite A

Step 6: Satellite A sends the required nonce code to satellite B

Step 7: A new valid transaction is conducted between satellites A and B

Step 8: The details of the new transaction between satellites A, and B are stored in a new block, then added to the Blockchain.
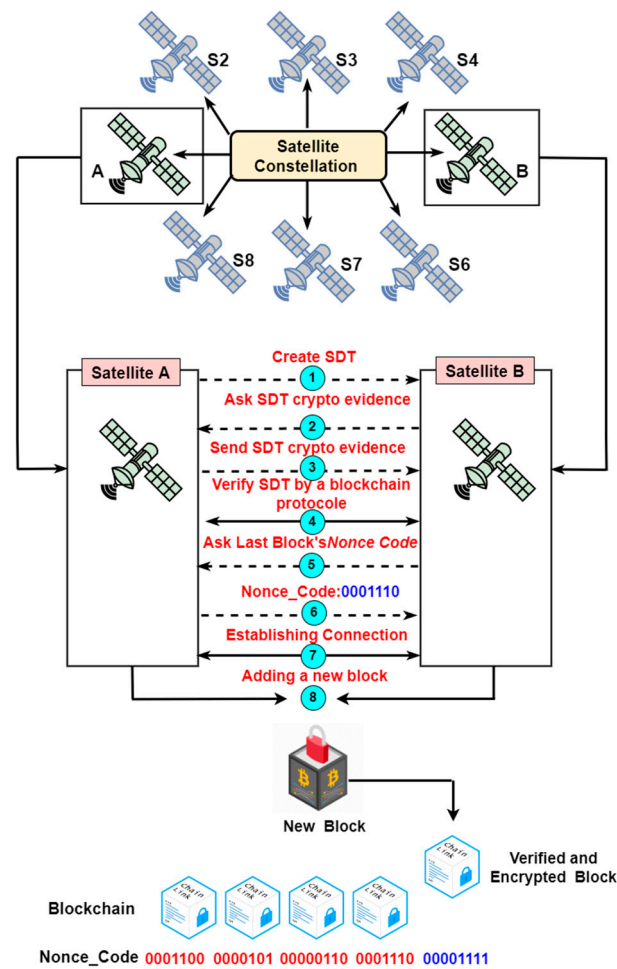
Figure 2. Proof of Space Transactions (PoST) protocol: Authenticating SDTs between two satellites within the same satellites constellation.

Algorithm 1 specifies how the proposed Blockchain protocol, PoST can implement the previous eight steps to verify the created SDTs (i.e., satellite transactions) between two satellites within the same constellation as a smart contract.

Algorithm 1: PoST for authenticating two satellites in **the same** constellations

---

Input: Satellite Constellation **S** = (**S1**, **S2**, S3, . . . , Sn)
Input: Space Digital Tokens: **SDT** = (SDT1, SDT2, . . . , SDTn)
Output: Blockchain + new Block
Procedure: *PoT* for authenticating two satellites in the same constellations
For all transactions in SDT
S1 = *Create* (SDT$_i$.S2).
S2 = *Ask* (SDT$_i$.*Crypto evidence*).
S1 = *Send* (SDT$_i$.*Crypto evidence*).
Verify (SDT$_i$, S3, S4, ... , Sn)
IF (SDT$_i$ is valid)
    S2 = Ask (last block's Nonce code).
    S1 = Send (last block's Nonce code)
    Connect (S1,S2)
    New block = Add (SDTi)
  Blockchain = Blockchain + New block
Else
   *Reject* (SDT$_i$)
End Procedure

On the other hand, Figure 3 depicts the authentication methodology of PoST between two satellites in different constellations through nine steps. It is similar to the verification method of a transaction between two satellites in a single constellation, but there are two pieces of crypto pieces of evidence are required here to establish a valid transaction between two satellites in different constellations:

1. Satellite *B* asks for the cryptographic evidence from satellite *A* that proves the validity of the constellation which follow the same Blockchain protocol
2. Satellite *B* asks for the cryptographic evidence from satellite *A* that proves the validity of the issued SDT between satellites *A*, and *B*
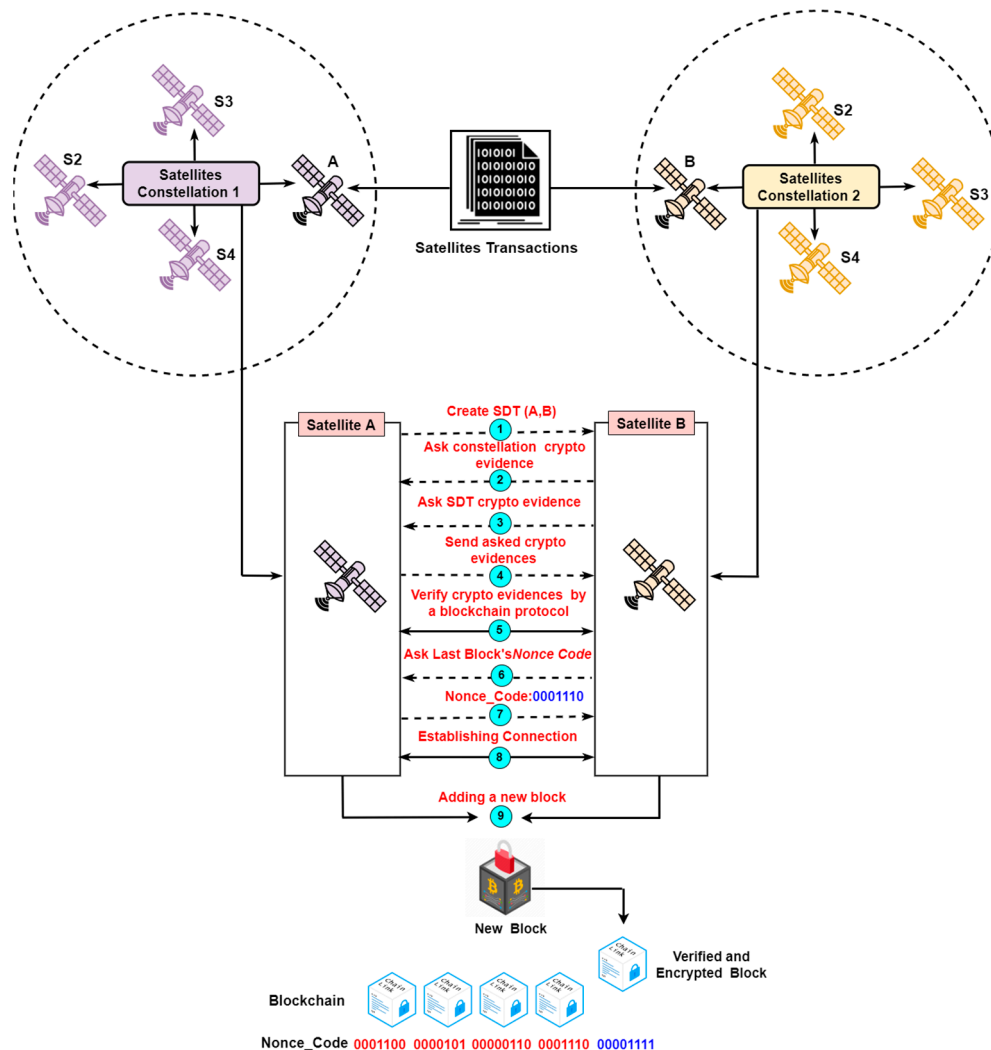
Figure 3. Proof of Space Transactions (PoST) protocol: Authenticating SDTs between two satellites within different satellite constellations.

When satellite *A* responds with the two required cryptographic pieces of evidence, steps 4–8 that implement the verification methodology of PoST protocol between two satellites in a single constellation are performed in the same way to verify a transaction between two satellites in two different constellations. Algorithm 2 specifies the authentication methodology of the proposed PoST protocol to verify SDTs between two satellites within two different constellations.

Algorithm 2: PoST for authenticating two satellites within **different** constellations

---

Input: Space Zones Z = (Z_1, Z_2, Z_3, . . . , Zn)
Input: Space Digital Tokens: **SDT** = (SDT1, SDT2, SDT3, ——SDTn).
Output: Blockchain + new Block
Procedure: *PoT* for authenticating two satellites within different constellations
For all transactions in SDT
Create (SDT_i, $Z_1.S_1$, $Z_2.S_1$).
$Z_2.S_1$ = Ask ($Z_{1,2}$.Crypto evidence).
$Z_2.S_1$ = Ask (SDT_i.Crypto evidence).
$Z_1.S_1$ = Send ($Z_{1,2}$.Crypto evidence).
$Z_1.S_1$ = Send (SDT_i.*Crypto evidence*).
Verify ($Z_{1,2}$.Crypto evidence, Z_3, Z_4, . . . , Zn)
IF ($Z_{1,2}$.Crypto evidence is valid)
    Verify (SDT_i, $Z_{2.S3,S4, ... ,Sn}$)
   IF (SDT_i is valid)
   $Z_2.S_1$ = Ask (last block's Nonce code).
   $Z_1.S_1$ = Send (last block's Nonce code)
  Connect ($Z_1.S_1$, $Z_2.S_1$)
  New block = Add (SDTi)
  Blockchain = Blockchain + New block
Else
Reject (SDT_i)
Else
Reject ($Z_{1,2}$.Crypto evidence)
End Procedure

5. Simulation Results

To assess the efficiency of the proposed Blockchain protocol, PoST, firstly the PoST was implemented, a dataset was created and then two simulation experiments were conducted. The dataset consists of three swarms of satellites, A, B, and C. each swarm consists of 10 satellites. Table 1 shows the satellite transactions within swarm A, where the size of transactional data is 1049 bytes. Table 2 shows the satellite transactions that have been exchanged between swarm A and B where the size of transactional data is 2049 bytes. Table 3 shows the satellite transactions that have been exchanged between swarm B, and C where the size of transactional data is 3049 bytes. For each transactional data size (i.e., 1049, 2049, and 3049), the proposed protocol has been simulated on six samples of transactions each having 50, 100, 150, 200, 250, and 300 transactions. As there is no benchmark data suitable to evaluate the proposed blockchain protocol, the data set has been created using python random library as depicted in Tables 1–3.

Table 1. Satellites transactions within Swarm A (size of a transaction is1049 bytes).

A/A	S2	S10	S4	S5	S1	S7	S3	S8	SUM
S1	7	10	8	6		6	4	9	**50**
S2		13	19	15	17	10	14	12	**100**
S7	20	24	18	19	25		21	23	**150**
S9	21	25	25	29	27	24	26	24	**200**
S5	38	32	30		33	39	36	42	**250**
S10	45		38	44	36	50	47	40	**300**

Table 2. Satellites transactions between Swarm A, and B (size of a transaction is 2049 bytes).

A/B	S6	S10	S8	S5	S3	S7	S4	S9	SUM
S1	7	4	8	6	7	5	8	5	50
S2	14	12	16	12	8	18	11	13	100
S3	18	23	16	25	14	17	21	16	150
S9	28	23	27	29	33	24	19	17	200
S5	29	38	33	17	29	36	33	35	250
S6	27	43	39	35	41	33	44	38	300

Table 3. Satellites transactions between Swarm B, and C (the size of a transaction is 3049 bytes).

B/C	S10	S6	S4	S1	S7	S5	S3	S8	SUM
S2	5	6	7	4	9	8	4	7	50
S6	13	12	9	17	15	9	14	11	100
S7	21	13	24	15	22	15	23	17	150
S9	26	17	21	28	30	29	24	25	200
S5	30	29	33	39	26	37	32	24	250
S10	34	38	49	33	36	39	40	31	300

Two main simulation experiments were designed to evaluate the performance of the PoST protocol.

The purpose of the first experiment was to evaluate the blockchain performance in managing satellite transactions either exchanged within the same swarm (i.e., a constellation as specified in Algorithm 1) or between two different swarms as specified in Algorithm 2. While the purpose of the second experiment was to evaluate the reliability and authenticity of the proposed PoST.

5.1. Blockchain Performance Results

Four metrics have been used to evaluate blockchain performance. These metrics are read latency (RL), transaction latency (TL), read throughput (RT), and transaction throughput (TT). They can be calculated as in Equations (1)–(4) respectively:
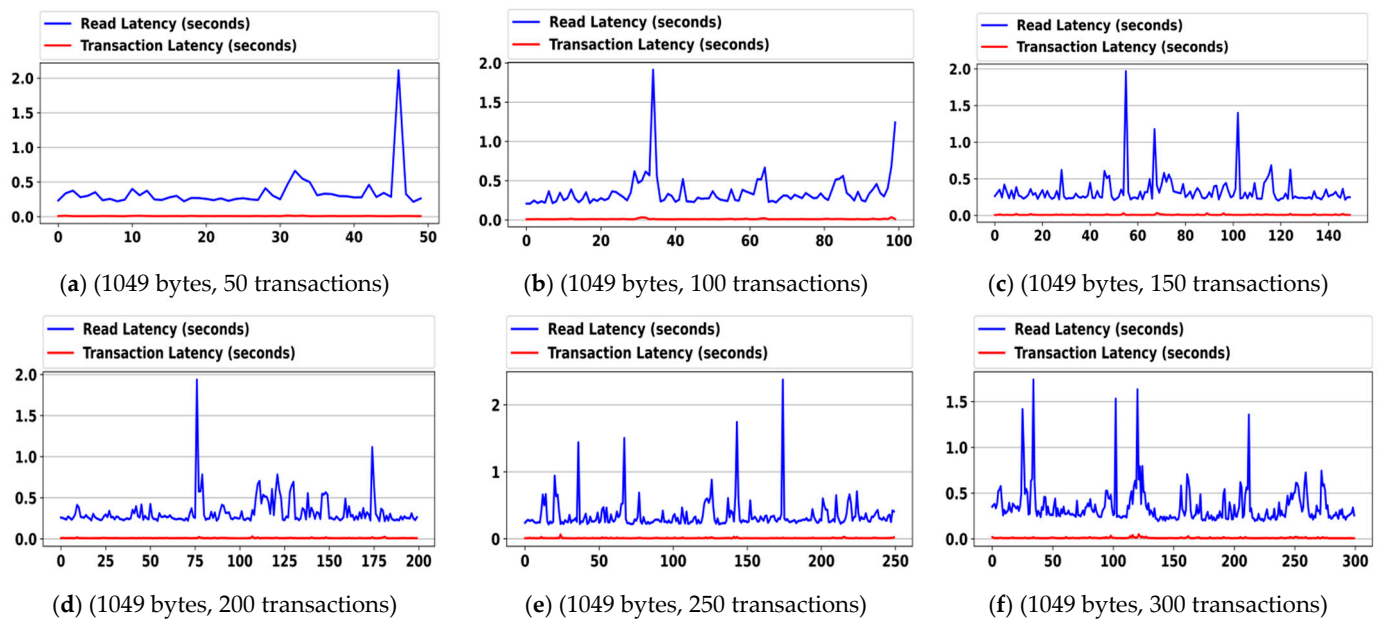
$$RL = \text{Response time} - \text{Submission time} \tag{1}$$

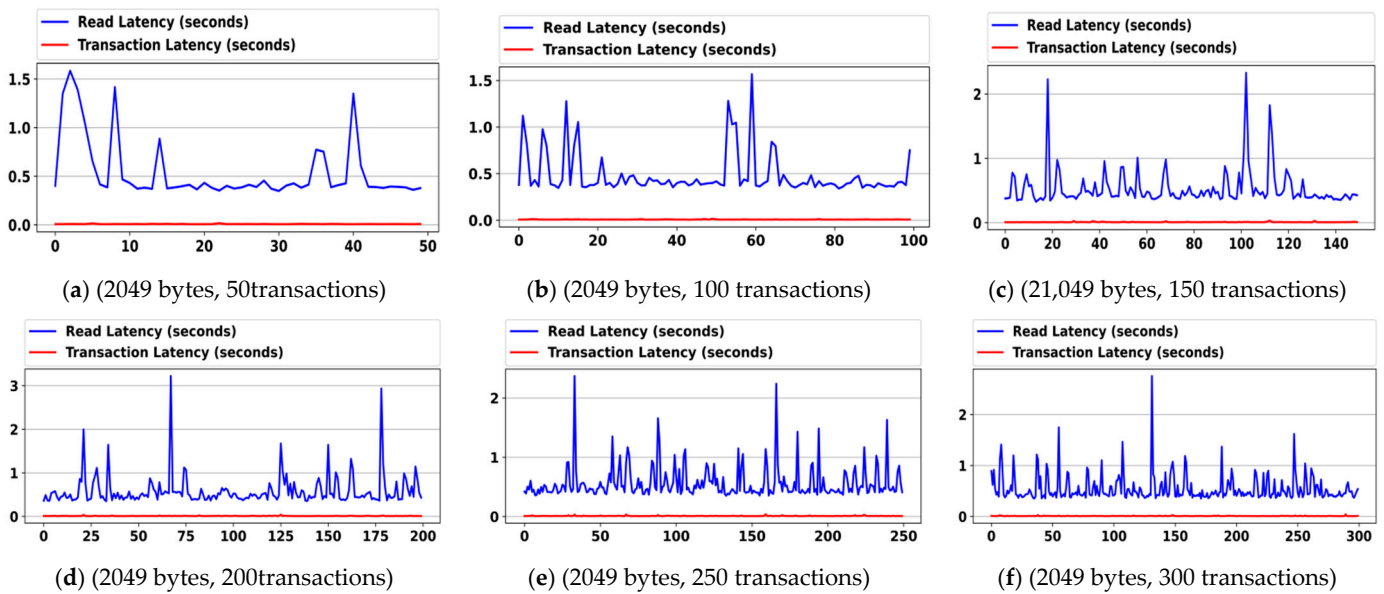$$TL = \text{Confirmation time@network threshold} - \text{submission time} \tag{2}$$

$$RT = \frac{\sum \text{Reads Operations}}{\sum \text{Times in seconds}} \tag{3}$$

$$TT = \frac{\sum \text{Commited Transactions}}{\sum \text{Time in seconds}} \tag{4}$$

Figure 4 depicts the obtained results that clarify the impact of a transactional data size equal to 1049 bytes on RL, and TL after applying algorithm 1 to the dataset depicted in Table 1. Figure 5 depicts the obtained results that clarify the impact of a transactional data size equal to 2049 bytes on RL, and TL after applying Algorithm 2 to the dataset depicted in Ta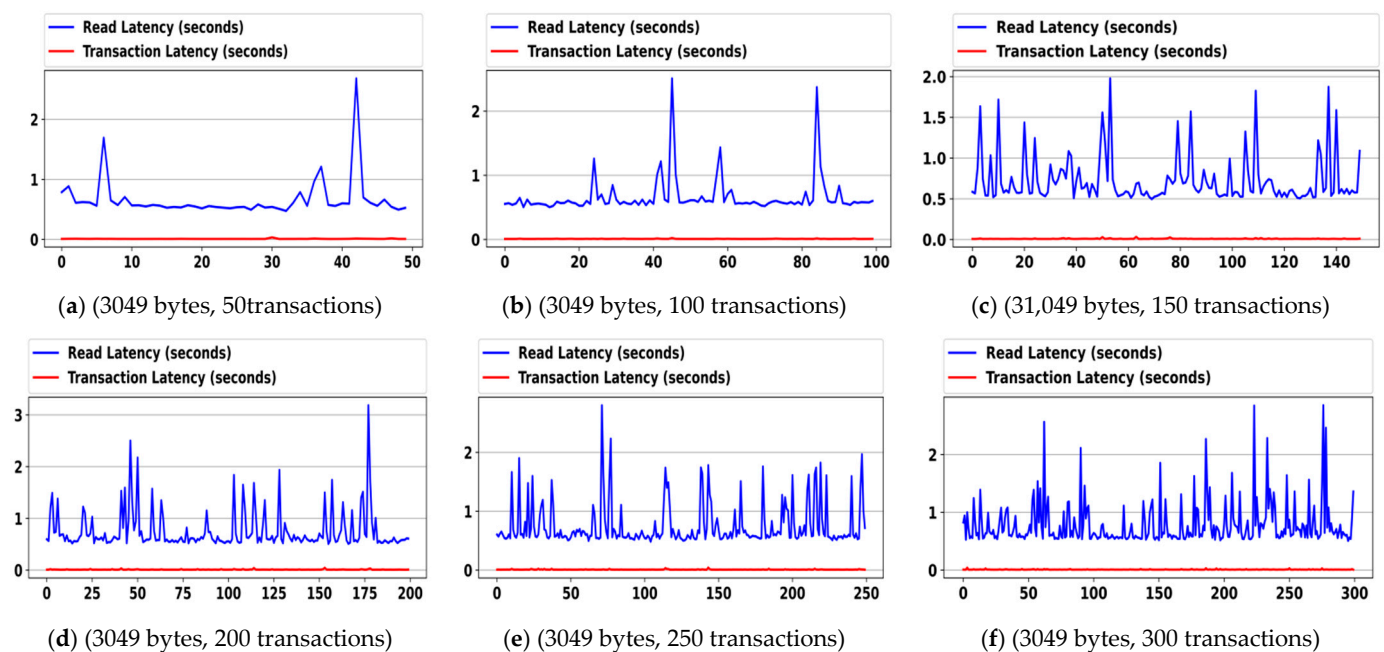ble 2. Figure 6 depicts the obtained results that clarify the impact of a transactional data size equal to 3049 bytes on RL, and TL after applying Algorithm 2 to the dataset depicted in Table 3. On the other hand, Tables 4–6 clarify the impacts of the three categories of transactional data size (i.e., 1049, 2049, and 3049 bytes) and GAS on Reading Throughput (RT) and Transaction Throughput (TT).

(**a**) (1049 bytes, 50 transactions)

(**b**) (1049 bytes, 100 transactions)

(**c**) (1049 bytes, 150 transactions)

(**d**) (1049 bytes, 200 transactions)

(**e**) (1049 bytes, 250 transactions)

(**f**) (1049 bytes, 300 transactions)

Figure 4. Impact of the transactional data size, 1049 bytes on RL, and TL for (**a**) 50, (**b**) 100, (**c**) 150, (**d**) 200, (**e**) 250, and (**f**) 300 transactions.

(**a**) (2049 bytes, 50transactions)

(**b**) (2049 bytes, 100 transactions)

(**c**) (21,049 bytes, 150 transactions)

(**d**) (2049 bytes, 200transactions)

(**e**) (2049 bytes, 250 transactions)

(**f**) (2049 bytes, 300 transactions)

Figure 5. Impact of the transactional data size,2049 bytes on RL, and TL for (**a**) 50, (**b**) 100, (**c**) 150, (**d**) 200, (**e**) 250, and (**f**) 300 transactions.

(**a**) (3049 bytes, 50transactions) (**b**) (3049 bytes, 100 transactions) (**c**) (31,049 bytes, 150 transactions)

(**d**) (3049 bytes, 200 transactions) (**e**) (3049 bytes, 250 transactions) (**f**) (3049 bytes, 300 transactions)

Figure 6. Impact of the transactional data size, 3049 bytes on RL, and TL for (**a**) 50, (**b**) 100, (**c**) 150, (**d**) 200, (**e**) 250, and (**f**) 300 transactions.

Table 4. Results of the impact of the transactional data size **1049** bytes on RT, and TT according to the number of satellite transactions.

#Satellites Trans	(RT)/RPS	(TT)/TPS	Gas	Size (BYTES)
50	112.95	2.95	202,419	1049
100	68.19	1.92	202,419	1049
150	50.90	1.48	202,419	1049
200	41.41	1.20	202,419	1049
250	33.87	0.99	202,419	1049
300	28.32	0.83	202,419	1049

Table 5. Results of the impact of the transactional data size **2049** bytes on RT, and TT according to the number of satellite transactions.

#Satellites Trans	(RT)/RPS	(TT)/TPS	Gas	Size (BYTES)
50	112.7	2.35	375,750	2049
100	71.92	1.19	375,750	2049
150	51.46	1.05	375,750	2049
200	42.21	0.67	375,750	2049
250	34.29	0.49	375,750	2049
300	30.9	0.39	375,750	2049

Table 6. Results of the impact of the transactional data size **3049** bytes on RT, and TT according to the number of satellite transactions.

#Satellites Trans	(RT)/RPS	(TT)/TPS	Gas	Size (BYTES)
50	112.61	1.53	549,084	3049
100	76.39	1.01	549,084	3049
150	55.71	0.72	549,084	3049
200	43.81	0.56	549,084	3049
250	36.98	0.46	549,084	3049
300	31.61	0.38	549,084	3049

5.2. PoST Authenticity and Reliability Results

The next investigation is assessing PoST authenticity and reliability in processing satellite transactions. To do that we reconfigured the used dataset to consist of trusted transactions and fake transactions within an individual swarm and in two different swarms, then we applied the PoST protocol on the reconfigured dataset to test the efficiency of the proposed protocol in accepting trusted satellite transactions and rejecting the fake ones. This can be measured by creating the confusion matrix parameters, then calculating True Positive Rate (TPR), True Negative Rate (TNR), and Accuracy as in Equations (5)–(7). Table 7 summarizes the obtained results.

$$\text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{5}$$

$$\text{TNR} = \frac{\text{TN}}{\text{TN} + \text{FP}} \tag{6}$$

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{7}$$

Table 7. TPR, TNR, and Accuracy of PoST protocol in verifying satellites transaction.

#Transactions	TP	TN	TPR	TNR	Accuracy
100	50	50	100%	100%	100%
200	100	100	100%	100%	100%
300	150	150	100%	100%	100%

6. Discussion

Prior studies that have noted the importance of using blockchain technology in the space industry are still little and immature. However, some reports have shown that Blockchain will be a base technology in developing the next generation of open-source satellites and spacecraft. In reviewing the literature, some research efforts discussed the adoption of blockchain to solve various challenges in the space industry and satellite communications. These challenges are the security and privacy of satellite communications [27,28], and satellite data broadcasting [29]. An initial objective of the study was to propose a new concept called space digital tokens (SDT) to build a new blockchain protocol called Proof of Space Transactions (PoST). The first question in this study sought to determine the efficiency of PoST in managing satellite transactions in the same swarm. The answer to this question shaped various interesting results. Firstly, the impact of the number of satellites transitions (where the size of a transaction is 1049 bytes) on transaction latency of blockchain when PoST is applied is not significant as it did not increase transaction latency by more than 0.05 TPS although the read latency is in a variable relationship with the number of satellite transactions (as shown in Figure 4). This means that satellite

transactions can be quickly processed even with the increasing number of satellite transactions and the variance of reading latency. Moreover, the results showed the impact of the number of transactions on the total read throughout (RT) and transaction throughput (TT) of blockchain is in a reverse relationship. This confirms also that the proposed PoST protocol can quickly process satellite transactions and confirm the efficiency of PoST in managing satellite transactions within a single swarm. The second question in this study sought to determine the efficiency of PoST in managing satellite transactions in different swarms. The answer to this question found that there is not a big impact of the number of satellite transitions (when a transaction size is 2049, and 3049 bytes) on transaction latency of blockchain when PoST is applied, as given in Figures 5 and 6. These results confirm that increasing the number of satellite transactions exchanged between different satellites between different swarms does not increase transaction latency by more than 0.05 TPS, hence, this proves the efficiency of the proposed PoST protocol in managing satellite transactions between different swarms of satellites whatever the number of transactions.

Another important finding is the impact of transactional data size on reading throughput and transaction throughput. The obtained results proved that transactional data size (1049, 2049, and 3049 bytes) is in a reverse relationship with reading throughput and transaction throughput which interpret the efficiency of PoST in processing transactional data between satellites whatever its size in bytes.

The third question in this research was to investigate the reliability of the PoST protocol in verifying the valid transactions within the trusted swarms of satellites. As shown in Table 7, the authentication process achieved 100% in terms of the accuracy, true positive rate (TPR), and true negative rate (TNR) of the PoST protocol. These results can be justified due to the ability of the proposed Blockchain protocol, PoST to recognize all valid transactions and reject all unreliable transactions when applied to three different sets of transactions between satellites. This means that the false positive (FP), and false negative (FN) are zero, and this interprets the optimality of the proposed Blockchain protocol in authenticating and verifying satellite transactions whether these transactions occurred in a single constellation or different ones.

This finding broadly supports the work introduced in [27] regarding using blockchain for verifying satellite access. Although the obtained results are in line with those in [27], PoST has some advantages that make it better than BAVP (Blockchain-Based Access Verification Protocol) proposed in [27]:

(1) PoST has been tested against the key measures of the blockchain (RL, TL, RT, and TT) while the BAVP has not. This makes the results of this study the leading ones.

(2) Although the BAVP achieved good results regarding response time and delay of satellite transactions, it considers neither the size of transactional data nor the frequency of transactions as in the PoST protocol. This may make the results of the PoST protocol more dependable than that of BAVP.

(3) In BAVP, the test scenarios focused on only the computation time of the encryption algorithm, (identity-based encryption (IBE)) used in BAVP compared with RSA without introducing any results about blockchain impacts on the efficiency of BAVP as performed with PoST protocol.

(4) In BAVP, the authors claimed that this protocol has intrinsic resistance against replay attacks, the man in the middle attack, impersonation attack, and denial of service attack, but there is no evaluation confirming this claim. On contrary, the reliability of PoST against fake satellite transactions has been tested and produced good results (see Table 7).

Further research efforts should be undertaken to investigate the effectiveness of the proposed PoST protocol for managing and authenticating other two types of transactions as two case studies:

(1) Investigating how PoST can manage and authenticate the tracking and data relay satellite (TDRS) transactions to improve the amount and speed of uplink and downlink data that could be transferred to or from the TDRS system.

(2)   Investigating how PoST can be used to immunize a satellite constellation against space debris collisions based on the sensing orbital data between satellites and space debris.

7. Conclusions

This study aimed to introduce a blockchain protocol called Proof of space transactions (PoST) to model, manage and authenticate satellite transactions within various constellations (or swarms). The main contribution of this study showed that tokenizing space transactions in the form of space digital tokens (SDT) and processing them using the proposed PoST protocol is a promising solution for managing and authenticating space transactions based on blockchain technology. This study has identified the effectiveness of the PoST protocol based on some simulation experiments that proved the effectiveness of the proposed Blockchain protocol in managing and authenticating satellite transactions in P2P networks.

According to the obtained results, it could be concluded that this study appears to be one of the first mature attempts to thoroughly investigate tokenizing space transactions and processing them using Blockchain. So, these results are expected to improve space communications management and develop a new generation of Blockchain-based satellite systems.

This study could be further enhanced by conducting additional experimental simulations and evaluations to investigate the effectiveness of the proposed PoST protocol for studying two important problems in this study, firstly, managing and authenticating TDRS's satellites, and ground station transactions. Secondly, immunizing a satellite constellation against space debris collisions based on the sensing orbital data between satellites and space debris.

Author Contributions: Conceptualization: M.T.; data curation, M.T. and E.G.; Formal Analysis: M.T. and T.G.; Investigation: M.T. and T.G.; Methodology: M.T.; Senior Administration: A.E.H.; Software: E.G.; Supervision: A.E.H.; Validation: M.T. and T.G.; Visualization: M.T.; Writing—original draft, M.T.; Writing—review and editing: T.G. and V.S. All authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Institutional Review Board.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

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

References

1. Space Foundation Editorial Team. Global Space Economy Grows in 2019 to $423.8 Billion, The Space Report 2020 Q2 Analysis Shows. Available online: https://www.spacefoundation.org/2020/07/30/global-space-economy-grows-in-2019-to-423-8-billion-the-space-report-2020-q2-analsis-shows/#:~{}:text=Global%20Space%20Economy%20Grows%20in,Q2%20Analysis%20Shows%20%2D%20Space%20Foundation (accessed on 19 February 2021).
2. Pelton, J.N.; Madry, S.; Camacho-Lara, S. Satellite Applications Handbook: The Complete Guide to Satellite Communications, Remote Sensing, Navigation, and Meteorology. In *Handbook of Satellite Application*; Springer: New York, NY, USA, 2013; pp. 3–19. [CrossRef]
3. Martin, A.S.; Freeland, S. The Advent of Artificial Intelligence in Space Activities: New Legal Challenges. *Space Policy* **2021**, *55*, 101408. [CrossRef]
4. Nanjangud, A.; Blacker, P.C.; Bandyopadhyay, S.; Gao, Y. Robotics and AI-enabled on-orbit operations with the future generation of small satellites. *Proc. IEEE* **2018**, *106*, 429–439. [CrossRef]

5. Luis, J.J.G.; Pachler, N.; Gerster, M.; del Portillo, I.; Crawley, E.; Cameron, B. Artificial intelligence algorithms for power allocation in high throughput satellites: A comparison. In Proceedings of the 2020 IEEE Aerospace Conference, Big Sky, MT, USA, 7–14 March 2020; pp. 1–14.

6. Fraire, J.A.; Céspedes, S.; Accettura, N. Direct-To-Satellite IoT-A Survey of the State of the Art and Future Research Perspectives. In Proceedings of the International Conference on Ad-Hoc Networks and Wireless, Luxembourg, 1–3 October 2019; pp. 241–258.

7. Routray, S.K.; Tengshe, R.; Javali, A.; Sarkar, S.; Sharma, L.; Ghosh, A.D. Satellite-based iot for mission-critical applications. In Proceedings of the 2019 International Conference on Data Science and Communication (IconDSC), Bangalore, India, 1–2 March 2019; pp. 1–6.

8. Chien, W.-C.; Lai, C.-F.; Hossain, M.S.; Muhammad, G. Heterogeneous space and terrestrial integrated networks for IoT: Architecture and challenges. *IEEE Netw.* **2019**, *33*, 15–21. [CrossRef]

9. Zhang, Z.; Zhang, W.; Tseng, F.-H. Satellite mobile edge computing: Improving QoS of high-speed satellite-terrestrial networks using edge computing techniques. *IEEE Netw.* **2019**, *33*, 70–76. [CrossRef]

10. Wang, Y.; Yang, J.; Guo, X.; Qu, Z. A game-theoretic approach to computation offloading in satellite edge computing. *IEEE Access* **2019**, *8*, 12510–12520. [CrossRef]

11. Denby, B.; Lucia, B. Orbital edge computing: Nanosatellite constellations as a new class of computer system. In Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems, Lausanne, Switzerland, 9 March 2020; pp. 939–954.

12. Bacsardi, L. On the way to quantum-based satellite communication. *IEEE Commun. Mag.* **2013**, *51*, 50–55. [CrossRef]

13. Bedington, R.; Arrazola, J.M.; Ling, A. Progress in satellite quantum key distribution. *Npj Quantum Inf.* **2017**, *3*, 1–3. [CrossRef]

14. Gibney, E. Chinese satellite is one giant step for the quantum internet. *Nat.News* **2016**, *535*, 478–479. [CrossRef] [PubMed]

15. Liao, S.-K.; Cai, W.-Q.; Liu, W.-Y.; Zhang, L.; Li, Y.; Ren, J.-G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.P.; et al. Satellite-to-ground quantum key distribution. *Nat.* **2017**, *549*, 43–47. [CrossRef]

16. Feng, M.; Xu, H. MSNET-Blockchain: A New Framework for Securing Mobile Satellite Communication Network. In Proceedings of the 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA, 10–13 June 2019; pp. 1–9.

17. Li, M.; Wang, L.; Zhang, Y. A framework for rocket and satellite launch information management systems based on blockchain technology. *Enterp. Inf. Syst.* **2019**, *2018*, 1092–1106. [CrossRef]

18. Surdi, S.A. Space Situational Awareness through Blockchain technology. *J. Space Saf. Eng.* **2020**, *7*, 295–301. [CrossRef]

19. Blockstream, The Bitcoin Blockchain from Space. No Internet Required. Available online: https://blockstream.com/satellite/ (accessed on 20 February 2021).

20. Anne, W.-S. Blockchain: The Next Big Disruptor in Space. Available online: http://interactive.satellitetoday.com/blockchain-the-next-big-disruptor-in-space/ (accessed on 20 February 2021).

21. Aditya Chaturvedi, Singapore Startup to Build World's First Open-Source Satellite Network. Available online: https://www.geospatialworld.net/blogs/singapore-startup-to-build-worlds-first-open-source-satellite-network/ (accessed on 20 February 2021).

22. Ulybyshev, Y. Satellite constellation design for complex coverage. *J. Spacecr. Rockets.* **2008**, *45*, 843–849. [CrossRef]

23. Alshaer, M.K. Cyber Attacks On Satellites Review & Solutions. Available online: https://www.academia.edu/18156391/Cyber_attacks_on_satellites_Review_and_solutions (accessed on 31 March 2021).

24. Jim, G.; Raditya, I. Hacking a Bird in the Sky: Hijacking Very Small Aperture Terminal (VSAT). Available online: https://conference.hitb.org/hitbsecconf2006kl/materials/DAY%202%20-%20Jim%20Geovedi%20and%20Raditya%20Iryandi%20-%20Hacking%20a%20bird%20in%20the%20sky.pdf (accessed on 31 March 2021).

25. Wu, Z.; Zhang, Y.; Yang, Y.; Liang, C.; Liu, R. Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey. *IEEE Access* **2020**, *8*, 165444–165496. [CrossRef]

26. Clark, L.; Tung, Y.C.; Clark, M.; Zapanta, L. A Blockchain-based Reputation System for Small Satellite Relay Networks. In Proceedings of the 2020 IEEE Aerospace Conference, Big Sky, MT, USA, 7–14 March 2020; pp. 1–8.

27. Wei, S.; Li, S.; Liu, P.; Liu, M. BAVP: Blockchain-based access verification protocol in LEO constellation using IBE keys. *Secur. Commun. Netw.* **2018**, *2018*, 7202806. [CrossRef]

28. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Exploration of blockchain-enabled decentralized capability-based access control strategy for space situational awareness. *Opt. Eng.* **2019**, *58*, 041609. [CrossRef]

29. Zhang, Y.H.; Liu, X.F. Satellite Broadcasting Enabled Blockchain Protocol: A Preliminary Study. In Proceedings of the 2020 Information Communication Technologies Conference (ICTC), Nanjing, China, 29–31 May 2020; pp. 118–124.

30. Sun, Z.; Deng, H.; Zhong, W.; Wu, X. Attacking satellite path planning based on genetic algorithm. *J. Aerosp. Eng.* **2012**, *25*, 32–38. [CrossRef]