Title

Satellite-Aided Consensus Protocol for Scalable Blockchains

Journal

Sensors, 20(19)

ISSN

1424-8220

Authors

Ling, Xintong

Gao, Zheng

Le, Yuwei

et al.

Publication Date

2020

DOI

10.3390/s20195616

sensors

MDPI

Letter

Satellite-Aided Consensus Protocol for Scalable Blockchains

Xintong Ling [1,2], Zheng Gao [1], Yuwei Le [1], Li You [1,2], Jiaheng Wang [1,2,*], Zhi Ding [3] and Xiqi Gao [1,2]

[1] National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China; xtling@seu.edu.cn (X.L.); zgao@seu.edu.cn (Z.G.); ywle@seu.edu.cn (Y.L.); liyou@seu.edu.cn (L.Y.); xqgao@seu.edu.cn (X.G.)

[2] The Purple Mountain Laboratories, Nanjing 210023, China

[3] Department of Electrical and Computer Engineering, University of California, Davis, CA 95616 USA; zding@ucdavis.edu

* Correspondence: jhwang@seu.edu.cn

Received: 30 August 2020; Accepted: 26 September 2020; Published: 1 October 2020

Abstract: In this work, we propose a satellite-aided permissionless consensus protocol for scalable space–terrestrial blockchains. We design its working principle and workflow by taking full advantage of satellites for extensive coverage and ubiquitous connectivity. Based on the proposed protocol, we demonstrate how such a space–terrestrial blockchain grows and evolves through several typical cases in the presence of adversarial nodes, user misbehavior, and transmission outage. Taking proof of work (PoW) as a benchmark, we assess the system security by considering both adversarial miners and possible colluding satellites. Then, we analyze the maximum blockchain throughput under network capacity limits and evaluate the impact of information propagation delay via a Markov model. Simulation results support that the proposed satellite-aided consensus protocol achieves higher throughput and exhibits greater scalability than PoW.

Keywords: blockchain; consensus protocol; performance analysis; satellite; space–terrestrial network

1. Introduction

Blockchain is currently blossoming in sectors such as internet of things (IoT) [1,2], 6G wireless networking [3,4], edge computing [5,6], sensor networks [7], and smart city [8]. For such a secured distributed ledger technology, consensus protocols serve as the very foundation. Based on specific consensus mechanisms, blockchain spurs miners to participate in maintaining an ordered public ledger via proper financial incentives. PoW, the most popular and recognized consensus protocol, was first introduced in 1992 [9] and developing into a vital part of Bitcoin since its launch in 2008 [10]. The success of PoW-based cryptocurrencies in the last decade indicates its robustness and resilience against misbehaviors and adversarial attacks [10,11].

However, PoW has an obvious weakness, as it consumes immense amounts of resources and energy. The estimated energy consumed by Bitcoin was around 70.05 TWh in 2020 [12], equivalent to the annual electricity consumption of the entire country of Czech Republic. Alternatives to PoW leverage other capabilities instead of intensive computations but often cause new security concerns [13]. Constrained by the consensus protocol (as well as the chain structure), the existing public blockchains exhibit scalability problems. Transactions per second (TPS), as the measure of information throughput in blockchain, is rather low in traditional blockchains, e.g., at most 7 TPS in Bitcoin and 15 TPS in Ethereum [14]. As a benchmark, centralized entities such as PayPal and VISA can achieve hundreds or thousands of TPS [15]. In short, high consumption and low scalability present two main barriers that severely constrain the advances of blockchain technologies.

Currently, there are several works concerned with how to utilize blockchains for the space sector [16–18], such as mobile satellite communication networks (MSNET) [16] and satellite monitoring [17]. However, only a few works and projects were investigating the potential applicability of satellites on blockchain. In both of [19,20], the authors proposed to use satellites as relays to help forward and propagate blocks in a space–terrestrial network. The project of BitSats [21] planned to turn satellites into crucial full Bitcoin nodes in space as early as 2014. Another project named SpaceChain [22] aims to bring an open-source decentralized software model to space and has leased two satellites in February and October of 2018, respectively. More recently, BlockStream [23] a startup in Canada, has launched six satellites to broadcast full Bitcoin blockchain for air-gapped areas across the globe. Another project ChainSat [24] has a similar plan to facilitate an off-grid network for enterprise blockchain ledgers via direct satellite communications. Space Impulse [25] and SupremeSat [26] also are reported to introduce blockchains into the space industry.

Notably, satellites can bring substantial benefits to next-generation blockchain protocols because of the extensive coverage and ubiquitous connectivity. As standardized by, e.g., Digital Video Broadcasting Second Generation Satellite (DVB-S2) and Digital Video Broadcasting Second Generation Satellite Extensions (DVB-S2X) [27,28], the satellites multicast transmission is now mature enough to deliver information to massive terrestrial receivers simultaneously, which would be helpful to solve the scalability issue of blockchain. (We will show how multicast transmissions affect the blockchain scalability in Section 5). Moreover, the latency of the terrestrial peer to peer (P2P) networks (e.g., the Internet) is often long-tailed due to the number of hops [29], whereas the propagation delay of satellite communications is nearly fixed and more controllable [19,20]. Furthermore, satellite systems can significantly reduce the vulnerability against Internet attacks and network interrupts [30,31]. Satellites are becoming the next game changer for blockchains.

However, the existing space blockchain solutions have not fully considered the characteristics of satellite communications, such as delay, link budget, bandwidth, on-board resources [16,32,33]. These solutions rely on the conventional, costly mining such as PoW, and use satellites merely as relays to forward blocks for unserved and under-served areas (e.g., BlockStream and ChainSat), or accelerate information diffusion in the mining network (e.g., [19,20]). Especially, if satellites are deployed as full blockchain nodes (e.g., BitSat and SpaceChain), block verification and chain backup put extra stress on the limited on-board device process and storage capability, which may explain why the project BitSat stalled eventually. Moreover, the uplink is dilemmatic. The uplink has to go through specific authorized ground stations [20], e.g., Blockstream only announced the availability of one-way satellite broadcasting. Ordinary users cannot upload newly mined blocks directly, which actually hurts the decentralization of the blockchain system. Nevertheless, even if ordinary users can upload blocks, high-speed uplinks are required to reduce the transmission delay, which, however, would impose extra cost on ordinary miners and raises the barriers to entry. Even though all these above issues are tolerated within the Bitcoin blockchain, they would become bottlenecks for next-generation high-TPS blockchains in the future.

Therefore, by comprehensively taking the characteristics of satellites into account, we propose a satellite-aided consensus protocol for efficient space–terrestrial blockchains. Our proposed protocol only needs low-speed, one-way multicast transmissions from space to terrestrial, which not only addresses the uplink dilemma but also vastly reduces the transmission delay. By leveraging the features of satellite multicast transmissions, the proposed protocol does not rely on the costly PoW protocol, and is thus eco-friendly and sustainable without consuming tremendous energy on meaningless hash queries. The main contributions of our work include:

- We develop a satellite-aided permissionless consensus protocol for sustainable, scalable blockchains, which, to the best of our knowledge, has never been investigated before.
- Technically, we demonstrate how the satellite-aided blockchain evolves and eventually converges despite various misbehaviors on a case-by-case basis, and show how the transmission outage and possible adversarial participants affect the chain evolution.

- Using the PoW-based blockchain as a benchmark, we theoretically analyze and assess the system performance regarding security and network throughput.
- Simulation results demonstrate that the satellite-aided blockchain exhibits greater scalability and can achieve higher TPS than the traditional PoW-based blockchains.

This paper is organized as follows. Section 2 presents the principle and workflow of the satellite-aided consensus protocol. Section 3 illustrates the possible patterns of blockchain evolution. Sections 4 and 5 calculate the blockchain performance in terms of security and scalability, respectively. At last, Section 6 provides the simulation results, and the paper concludes with Section 7.

2. Satellite-Aided Consensus Protocol

There are essentially three types of orbits classified by the satellite altitude: geostationary earth orbit (GEO), medium earth orbit (MEO), and low earth orbit (LEO) [32–34]. Among them, GEO satellites are stationary relative to the earth's surface so that the doppler shift is negligible and has a lower transmission outage probability than non-GEO satellites [32,35,36]. The GEO satellites work at very high altitudes (≈35,786 km) and can offer the most extensive coverage [37]. Thanks to the low outage probability and wide coverage, GEO satellites are preferred in our proposed protocol. However, the high altitudes of GEO satellites also result in long delays and high path losses [32,35]. Thus, we should design the consensus protocol by taking the drawbacks of GEO into account.

The brief workflow of the satellite-aided consensus protocol is illustrated in Figure 1. The proposed protocol requires low-speed, one-way transmissions only, which effectively reduces the negative impact of round-trip delays. In each round, a GEO satellite periodically multicasts random oracles (typically of hundreds of bits) to the on-ground terminals based on the standards such as DVB-S2 and DVB-S2X [27,28].

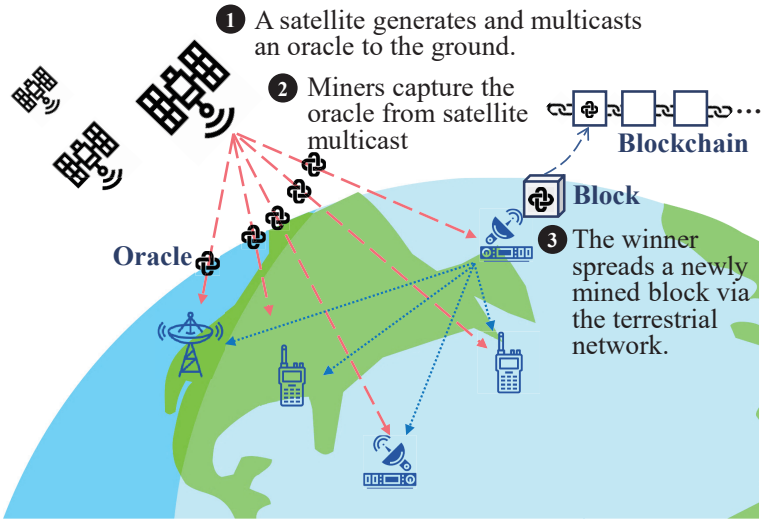

Figure 1. The illustration of the proposed satellite-aided consensus protocol.

These random oracles are digitally signed by the satellite to avoid forgery and required to be included in the generated block for validation. The on-ground miners only need to capture random oracles from space through terrestrial user terminals, such as portable mobile receivers, very small aperture terminals (VSATs), among others [32]. A random oracle will point to a specific terrestrial miner and elect it as a winner of the current round. The winner is granted an opportunity for proposing a new block on the top of the existing chain and spreading it among terrestrial miners. Via satellite multicasting (and also possible terrestrial forwarding), the majority of terrestrial miners receive the random oracle and thus can verify the identity of the winner and validate the corresponding block. Therefore, the satellite-aided blockchain grows as one block is built on the top of others.

We design the above workflow by comprehensively considering the characteristics of GEO satellites. The benefits of our proposed satellite-aided protocol are hence multifold. First, the protocol imposes a minimal burden on satellites with no need to process, store, verify, or even forward blocks in space. Second, since the random oracles are generated by satellites, the uplinks are unnecessary in the proposed protocol, which reduces the delay caused by GEO, solves the uplink dilemma, and further simplifies the space–terrestrial network structure. Third, we only multicast random oracles (hundreds of bits) instead of the whole blocks (typically of megabytes). On the one hand, it can reduce the influence of high path loss of GEO satellites, letting more miners at a low signal-to-noise ratio (SNR) capture the oracles. On the other hand, it lowers the link budget and is scalable for high TPS blockchains. Fourth, our solution does not require miners to perform meaningless hash queries but takes advantage of multicast transmissions to maintain the system consensus in a novel approach, which largely reduces the mining cost and is thus sustainable and green. By leveraging the characteristics of GEO satellites including its extensive coverage and low outage probability, the satellite-aided blockchain is more scalable and can achieve a higher TPS than traditional blockchains. (Please see the analysis in Section 5).

In the satellite-aided consensus protocol, random oracles can be generated based on real-time physical quantities measured by the satellite, such as cosmic rays, hydromagnetic waves, transient radiations, and so forth [38–40]. Hence, the random oracle can be truly random rather than pseudo-random to guarantee mining fairness. However, the corresponding services have to be ordered and purchased from satellite operators to generate and multicast random oracles from the space, which increases the maintenance cost. In fact, there is another tricky approach to obtain oracles. The random oracle can be generated by data packets multicast to the ground for other purposes such as satellite television (TV) and global positioning system (GPS). The consensus protocol gives a pre-defined rule to determine the specific packets (e.g., satellite sources and frequency bands) for oracle generation in each round. In this case, the satellite even do not realize that they participate in generating oracles and maintaining a blockchain, and it is thus unnecessary to purchase any satellite services. However, in this manner, the oracle randomness may be affected and the oracles are more likely to be manipulated by adversaries. Therefore, there exists a trade-off between security and cost in the oracle generation, which should be selected according to the purposes and requirements of blockchain.

Note that it might be risky to directly select winners by random oracles in fear of Sybil attack–malicious users can create many fake identities to increase the winning probability. Hence, we can draw the principle from proof of stake (PoS). The oracle can be interpreted as an index in the list of all the already minted coins so that its owner is the winner of this round [13]. The winning probability is only related to the stake that miners hold and does not increase by creating multiple identities. Therefore, Sybil attacks can be prevented effectively, and satellites do not have to know or maintain a list of legitimate miners.

3. Patterns of Chain Evolution

In this section, we show how such a satellite-aided blockchain extends and evolves. As shown in Figure 2a, an honest winner w_2, after being chosen by the oracle in round r_2, would generate a valid block b_2 on the top of the last block b_1 and multicast it to the rest of the mining network. According to the oracle of r_2, other miners can verify the identity of w_2 and the validation of b_2. Usually, the next winner w_3 would propose a new block b_3 on the top of b_2. As such, the chain will grow and evolve.

However, due to network delays or misbehaviors, exceptions may occur. As shown in Figure 2b, it is possible that the chosen winner w_2 misses the oracle due to the outage of satellite links, and thus does not generate any new block in round r_2. As a result, the winner w_3 of the next round will generate a block b_3 on the top of b_1 directly. While in Figure 2c, w_3 may not receive b_2 in round r_3 due to network delay. Since w_3 has not been informed, it generates a new block b_3 on the top of b_1 directly. However,

in this case, b_2 exists at the same height, resulting in orphaned blocks. The future block extension will determine which block will be finally included in the main chain.

In terms of misbehaviors, a winner w_2 in Figure 2d may generate an invalid block, whereas, in Figure 2e, a miner w_2' who has not been selected, may forge its identity and generate a block b_2'. In the above two cases, other miners can easily find that the block in Figure 2d is invalid and the block in Figure 2e is generated by an illegitimate winner by checking the block and oracle. Hence, these two b_2' in Figure 2d,e will be ignored and excluded from the main chain. Furthermore, in Figure 2f, a malicious winner w_2 may diverge the chain by publishing two or more valid blocks in one single round. As a rule of thumb, benign miners should discard all of them.

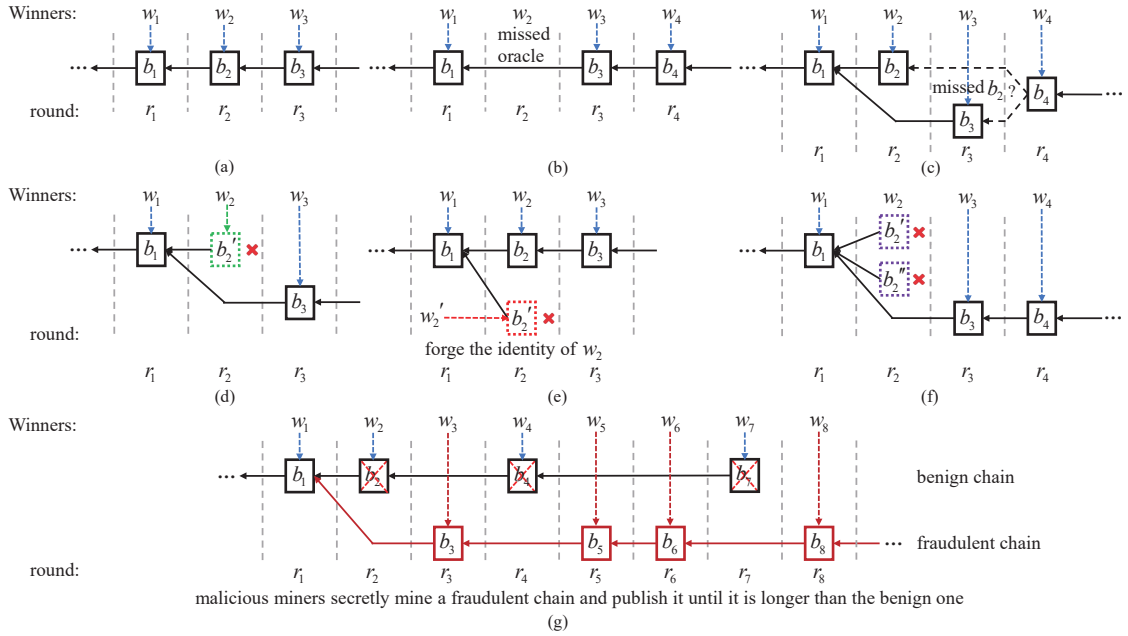

Figure 2. Possible patterns of blockchain evolution based on the satellite-aided consensus. (**a**) Regular extension. (**b**) Oracle missing. (**c**) Block missing. (**d**) Invalid blocks. (**e**) Fraud identity. (**f**) Multi-block in one round. (**g**) Alternative history attack.

Last but not least, the alternative history attack is likely to happen in a satellite-aided blockchain, and could bring disastrous effects to the blockchain systems. When an alternative history attack takes place, an adversary would create a fraudulent branch and secretly mine on it, as shown in Figure 2g. Until the adversarial branch is longer (or heavier) than the original benign one, the adversary will release it to alter a confirmed history. The probability of a successful alternative history attack, also known as the confirmation error probability [11], is thus used as a measure of chain security in this paper.

In a nutshell, Figure 2a is the ideal pattern for blockchain extension, as one block is generated on the top of the chain in each round. Figure 2b,c are caused by the oracle multicast outage and block propagation delay and are thus inevitable in practice. Orphaned blocks may occur in these two cases and their combinations. The possible misbehaviors in Figure 2e,f can be effectively prevented by the proposed protocol. Essentially, the attack in Figure 2g poses an inherent risk of a distributed system, and hence the successful attack probability will be discussed in the following section to assess the resilience of the proposed protocol.

4. Security Implications

In this section, we assess the risk to the satellite-aided consensus protocol in the presence of an adversary. Denote β_t as the fraction of the total terrestrial mining power controlled by an adversary. Hence, in a round, the probability that a benign miner is chosen as the winner is $1 - \beta_t$, and the

winning probability of an adversary is β_t. Moreover, we have to consider that some satellites may be controlled or hacked by an adversary. Let β_s be the fraction of adversarial satellites. Undoubtedly, when an adversarial satellite generates an oracle, an adversarial miner will be selected as the winner. In short, the probability that a malicious miner is selected as the winner is $\beta_s + \beta_t (1 - \beta_s)$, while the probability that a benign miner is selected as the winner is $(1 - \beta_s)(1 - \beta_t)$.

More practically, we should take the possible outage or interrupt of satellite links into considerations. Denote p as the successful transmission probability of satellite links such that the outage probability is $1 - p$. Figure 2b shows that a winner will not generate a block if it does not receive the oracle (with probability $1 - p$). Hence, the growth rate of the benign and adversarial chains can be, respectively, formulated as

$$h = p (1 - \beta_s)(1 - \beta_t), \tag{1}$$

$$f = p (\beta_s + \beta_t - \beta_t \beta_s). \tag{2}$$

Therefore, the overall relative power controlled by an adversary, denoted by β, can be expressed by

$$\beta \triangleq \frac{f}{f + h} = \beta_s + \beta_t - \beta_t \beta_s. \tag{3}$$

From Equation (3), the successful transmission probability p will not directly influence the system security. However, if the adversarial miners have back channels to the colluding satellites, the blockchain faces heightened risk. In the absence of adversarial satellites, the overall adversarial power only depends on the terrestrial miners $\beta = \beta_t$ as $\beta_s = 0$. Obviously, the existence of adversarial satellites makes the chain more vulnerable.

We use the probability of a successful double spending attack, i.e., confirmation error probability, to evaluate the resilience of the proposed protocol. According to the framework on alternative history attacks [41], given the confirmation number k, the confirmation error probability is

$$\mathsf{S}_k(\beta) = \begin{cases} 1 - \sum_{n=0}^{k} \binom{n+k-1}{n} \left(\beta^n (1 - \beta)^k - \beta^k (1 - \beta)^n \right) & \text{if } \beta < 1/2 \\ 1 & \text{if } \beta \geq 1/2. \end{cases} \tag{4}$$

Remark 1. *For $\beta \geq 1/2$, the adversary dominates the chain and always succeeds. For $\beta < 1/2$, the confirmation error probability is exponentially decreasing with the confirmation number k, where the decay rate is the attacker's relative power β. Note that a PoW-based blockchain with adversary mining power $\beta_{PoW} = \beta$ has the exact same confirmation error probability as a satellite-aided blockchain.*

5. Throughput Analysis

5.1. Network Capacity Limits

In the context of blockchain, throughput means the amount of information, e.g., transactions, gets confirmed per second. We would like to characterize the maximum throughput of the satellite-aided consensus protocol. Let us say the maximum block size limit is B bits, and each round corresponds to Δ seconds. Hence, since at most one valid block can be generated in each round, the maximum throughput is B/Δ bps. However, the presence of the adversary and the outage of satellite links degrade the blockchain throughput. Based on the growth rate of the benign chain in Equation (1), the throughput of the satellite-aided consensus is

$$\mathsf{T}_{\text{CPTY}} = \frac{hB}{\Delta} = p (1 - \beta) \frac{B}{\Delta}. \tag{5}$$

Let C(bps) be the capacity of the terrestrial mining network. Obviously, it is impossible to deliver a block with size B within the interval Δ, if $B/\Delta > C$. Hence, the values of B and Δ are constrained by $B/\Delta \leq C$. The maximum throughput of a satellite-aided consensus under capacity limits is given by

$$\mathsf{T}_{\mathrm{CPTY}} \leq p\,(1-\beta)\,C \triangleq \mathsf{T}^{m}_{\mathrm{CPTY}}. \tag{6}$$

As a benchmark, we present the throughput of PoW-based consensus borrowed from a recent work [11]. In PoW, the block generation obeys a Poisson process with mean λ, wherein β fraction of miners are adversarial and the rest are benign. During the period τ, the probability of no benign block is $\exp\left(-\lambda(1-\beta)\tau\right)$. Hence, the growth rate of the benign chain (at least one benign block during τ) is $1-\exp\left(-\lambda(1-\beta)\tau\right)$, and the throughput is

$$\mathsf{T}_{\mathrm{PoW}} = \left(1-\exp\left(-\lambda\,(1-\beta)\,\tau\right)\right) B/\tau. \tag{7}$$

As the block generation rate λ cannot exceed the limit C/B, the limiting throughput $\mathsf{T}_{\mathrm{PoW}}$ is thus bounded by

$$\begin{aligned}\mathsf{T}_{\mathrm{PoW}} &\leq \left(1-\exp\left(-\frac{\tau C}{B}\,(1-\beta)\right)\right)\frac{B}{\tau}\\ &\leq \left(1-\exp\left(\beta-1\right)\right)C \triangleq \mathsf{T}^{m}_{\mathrm{PoW}}.\end{aligned} \tag{8}$$

The equality is achieved if and only if $\lambda = C/B = 1/\tau$.

By comparing $\mathsf{T}^{m}_{\mathrm{CPTY}}$ in Equation (6) with $\mathsf{T}^{m}_{\mathrm{PoW}}$ in Equation (8), we have $\mathsf{T}^{m}_{\mathrm{CPTY}} > \mathsf{T}^{m}_{\mathrm{PoW}}$ if $p\,(1-\beta) \geq 1-\exp\left(\beta-1\right)$. We thus define $y\,(\beta) \triangleq \frac{1-\exp(\beta-1)}{1-\beta}$ as the threshold of p. If the quality of multicast channel is better than a given threshold related to β, i.e., $p > y\,(\beta)$, then the satellite-aided consensus protocol has a larger maximum throughput than PoW.

Note that $y\,(\beta)$ is monotonically increasing in β within $0 \leq \beta < 1$. To show this, for any $\beta < 1$, we have

$$y'\,(\beta) = \frac{(\beta-2)\exp\left(\beta-1\right)+1}{(\beta-1)^2} > \frac{-1+1}{(\beta-1)^2} = 0,$$

where the inequality is because $(\beta-2)\exp\left(\beta-1\right)$ is lower bounded by $(\beta-2)\exp\left(\beta-1\right)|_{\beta=1} = -1$. As a result, for any $\beta \leq 0.5$, if $p > y\,(\beta=0.5) \approx 0.787$, then the proposed consensus protocol has a higher throughput than PoW as $\mathsf{T}^{m}_{\mathrm{CPTY}} > \mathsf{T}^{m}_{\mathrm{PoW}}$ always holds. As a benchmark, the outage probability of China's Beidou navigation satellite system is about 2% [42], i.e., $p \approx 98\%$, which is much higher than the threshold $y\,(\beta=0.5)$. If $p < y\,(\beta=0) = 1-\exp\left(-1\right)$, then $\mathsf{T}^{m}_{\mathrm{CPTY}} < \mathsf{T}^{m}_{\mathrm{PoW}}$.

Remark 2. *The above conclusion implies that the scalability of satellite-aided blockchains is highly related to the quality of the satellite multicast channels. Essentially, high-quality multicast transmissions change the information flow of the satellite-aided blockchain, thereby significantly improving the throughput. As indicated by the above discussions, if the multicast channel is in poor quality, the satellite-aided consensus protocol cannot benefit from the nature of multicast transmissions. Furthermore, since the threshold $y\,(\beta)$ grows with β, better multicast channels with a larger p are thus required if the adversary is more powerful.*

5.2. Propagation Delay

In the above analysis, we considered the capacity limits of $B/\Delta \leq C$. As shown in [29], the spreading delay across, e.g., 90% nodes, via Internet could be quite long. Hence, we define $i(t)$ as the ratio of informed nodes at time t for a specific network. Take $t = \Delta$ as an example, where the round slot is Δ seconds. Hence, $i_{\Delta} \triangleq i(t=\Delta)$ is the ratio of nodes receiving the block in the last round. After the block of last round is published, $1-i_{\Delta}$ fraction of nodes will not receive that block in the next round, potentially leading to orphaned blocks as the case in Figure 2c. However, such orphaned blocks lower the chain growth rate and also affect the blockchain throughput, even without an adversary.

(As a rule of thumb, if two or more forks occur, the next winner will always follow the longest known chain. If these forks are at the same height, the next winner will follow the one which achieves this height earlier).

Now things get complicated. In Figure 3a, starting from a consistent state, the number of possible blockchain states grows exponentially after just three rounds. Note that the ratio of informed nodes after one round, i.e., i_Δ, is the most critical term affecting orphaning. To characterize this complicated problem, we focus on the factor i_Δ and assume $i\left(k\Delta\right) = 1$ for $k = 2, 3, ...$ without affecting the spirit of our results. These countless states can be classified into four categories. We can abstract their states via the minimum height gap between the longest chain and other active forks. In Figure 3a, we start from a consistent state, denoted as S_∞, since there exists a unique active chain. If the next winner receives the last block, it is still in state S_∞. Otherwise, it jumps to the state S_0 with a newly-generated fork. The next block generated on any fork will lead to a longer main chain by one block, i.e., state S_1. Then, in the next round, if the winner follows the longest branch, the blockchain returns to a consistent state S_∞, otherwise it jumps back to the tied state S_0. For any state, if the next winner misses the oracle or is an adversary, no block is generated or released in this round, and the chain goes to the state $S_\times$.

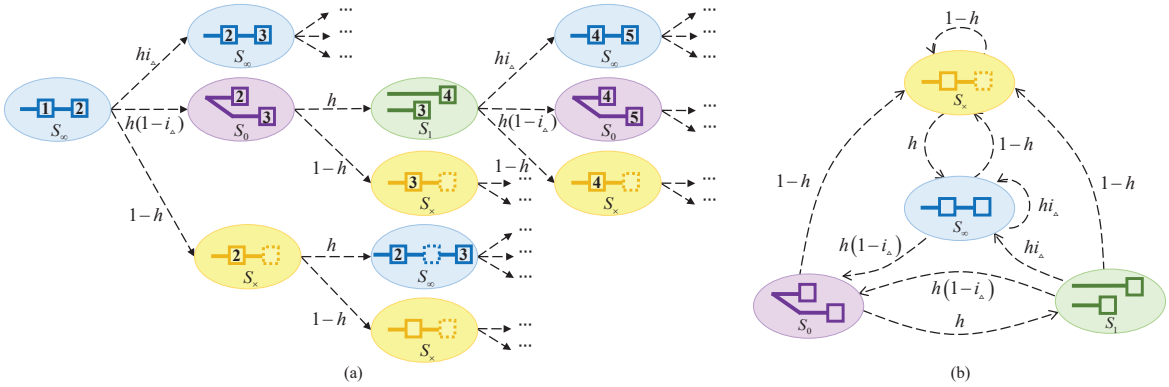

Figure 3. Blockchain evolution affected by information propagation delay. (**a**) The number of chain states skyrockets after three rounds. (**b**) Chain state space and transition diagram.

One can see that these four states form a Markov chain, as shown in Figure 3b. We can mathematically write the probability transition matrix as follows:

$$\mathbf{Q} = \begin{pmatrix} S_0: & 0 & h & 0 & 1-h \\ S_1: & h\left(1-i_\Delta\right) & 0 & hi_\Delta & 1-h \\ S_\infty: & h\left(1-i_\Delta\right) & 0 & hi_\Delta & 1-h \\ S_\times: & 0 & 0 & h & 1-h \end{pmatrix},$$

where h is the growth rate of the benign chain defined in Equation (1). Let $\mathbf{w}$ be the steady-state distribution of the considered Markov chain. The expression of $\mathbf{w}$ can be obtained from $\mathbf{wQ} = \mathbf{w}$:

$$\mathbf{w} = \left(\frac{h^2(1-i_\Delta)}{(1-i_\Delta)h+1} \;\middle|\; \frac{h^3(1-i_\Delta)}{(1-i_\Delta)h+1} \;\middle|\; \frac{h-h^3(1-i_\Delta)}{(1-i_\Delta)h+1} \;\middle|\; 1-h \right).$$

Note that, these four states have different probabilities to extend a new block in the longest chain. By comprehensively considering these states, we can obtain the growth rate:

$$h_{\mathrm{PROP}} = w_0 h + w_1 h i_\Delta + w_\infty h i_\Delta + w_\times h = \frac{h}{1+\left(1-i_\Delta\right)h}.$$

As a result, the blockchain throughput with information propagation delay can be expressed as

$$\mathrm{T}_{\mathrm{PROP}} = \frac{h_{\mathrm{PROP}} B}{\Delta} \leq \frac{h}{1+\left(1-i_\Delta\right)h} C \triangleq \mathrm{T}^m_{\mathrm{PROP}}. \tag{9}$$

Remark 3. *Comparing Equations (6) and (9), we can find the impact of information propagation on blockchain throughput. Only considering at most two-round propagation delay, we can see the maximum throughput degradation by a factor of* $1/\left(1+\left(1-i_{\Delta}\right)h\right)$. *In principle, we cannot control the value of* i_{Δ} *for a given network but can select the proper block size B and the round slot* Δ *based on (9) to maximize the blockchain throughput.*

Usually, propagation delays do not affect the behaviors of colluding adversarial miners so that the growth rate of the adversarial chain will be the same as Equation (2). Therefore, propagation delay not only affects the throughput but also may weaken the double-spending resilience.

6. Evaluation

In this section, we evaluate the proposed satellite-aided consensus protocol from throughput and security aspects. We establish a satellite-aided blockchain simulation system according to the proposed protocol. (Please see github.com/xtling/SatelliteChain for the source code.) In our setting, terrestrial miners form a peer-to-peer network with the same winning probability and the same transmission outage from space. In Figures 4–6, simulation results are shown by markers, whereas analytical curves are illustrated by dashed lines. We require $k = 6$ blocks to confirm a block, and normalize the throughput by the mining network capacity C.

In Figure 4, we illustrate the throughput and security of the proposed protocol in the presence of one adversary. One can see that the simulation results (markers) match our analytical throughput and security results (dashed lines). As shown in Figure 4, both space and terrestrial safety levels (β_s and β_t) compromise the security of the whole blockchain. However, to manipulate the blockchain, an adversary must control a vast number of resources $\beta = \beta_s + \beta_t - \beta_t\beta_s > \frac{1}{2}$ in the mining network.

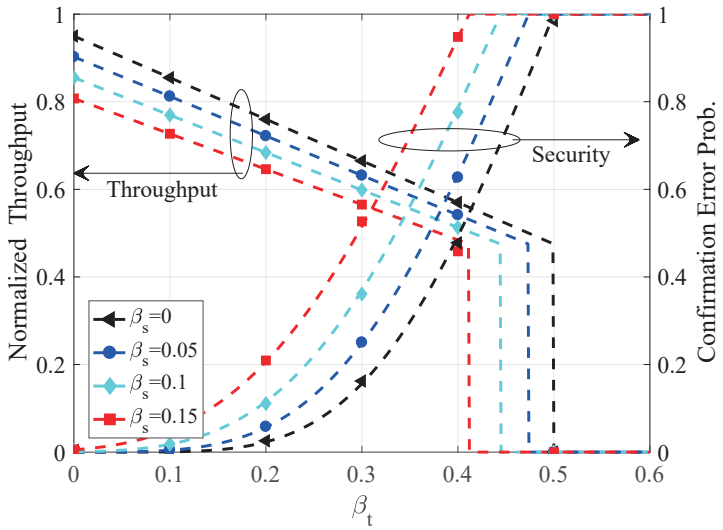

Figure 4. Analytical and simulation results of throughput and safety property of the proposed protocol.

In Figure 5, we compare the proposed satellite-aided consensus protocol with PoW as a benchmark. The throughput and security properties of PoW have been presented in [11,41], respectively. The proposed consensus protocol can achieve much higher throughput than PoW with comparable safety property as PoW. Moreover, one can see that the throughput of the satellite-aided blockchain depends heavily on the quality of satellite multicast channels, which is consistent with the remarks in Section 5.1.

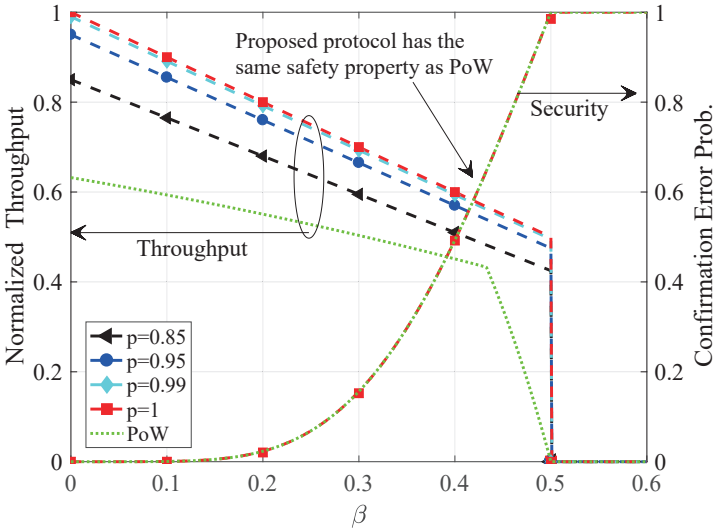

Figure 5. Comparison of the proposed protocol and PoW regarding throughput and safety.

In Figure 6, we demonstrate the impact of network propagation factor i_Δ on blockchain throughput. The analytical results (lines) based on the Markov model is closely matched by simulations (markers). As shown in Figure 6, the network propagation delay leads to more orphaned blocks and degrades the network throughput by a factor $1/\left(1+\left(1-i_\Delta\right)h\right)$ shown in Equation (9). As a guideline for practical design, for a given network with $i(t)$, we must systematically optimize the block size B and round slot Δ to obtain a proper $i(\Delta)$ for higher throughput.

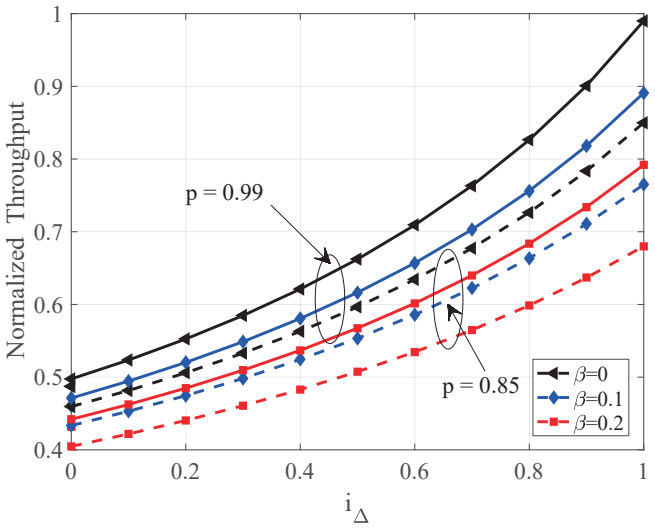

Figure 6. The impact of network delay on the throughput of the proposed protocol.

7. Conclusions and Future Research

Utilizing satellite systems for advanced public blockchains is a promising approach, due to ubiquitous connectivity and wide coverage. Hence, this study proposed a novel satellite-aided consensus protocol for efficient space–terrestrial blockchains. Unlike existing works [19,20], we used satellites as neither full blockchain nodes nor relays. In our study, we do not rely on costly consensus protocols such as PoW but designed a proper working principle according to the space–terrestrial networks' characteristics. We analyzed the system performance regarding throughput and security. In terms of security, we took both adversarial miners and satellites into consideration. In the throughput analysis, we investigated the maximum throughput under the capacity limits and further modeled the

case with propagation delays by a Markov chain. Compared with the traditional PoW, the proposed consensus protocol exhibits higher scalability.

Remark that satellite-aided blockchains also open several interesting future directions.

- Access control. As pointed out in Section 4, a larger fraction of adversarial satellites β_s will increase the confirmation error probability, which means an adversary can make the blockchain more vulnerable by hacking satellites. Therefore, access control is vital to the space–terrestrial blockchains [43]. On the one hand, our protocol does not require (or allow) terrestrial networks to upload data to satellites, which reduces the risks as another advantage. On the other hand, context-aware access control [44] should be considered as a potential approach to safeguard satellites further.
- Multiple satellite coordination. A constellation of satellites can multicast oracles for more extensive coverage, which can benefit space–terrestrial blockchains. Our protocol can easily expand from a single satellite setting to a constellation of participation satellites. However, it might compromise the blockchain security since more vulnerabilities are exposed in a constellation. More works need to be done for a practical space–terrestrial blockchain with multiple satellites.
- Information propagation model. In Section 5.2, we assess the impact of propagation delay by only considering i_Δ, the fraction of informed nodes after one round. However, in the real world, network delays could be long-tailed or even unbounded [29]. A more general information propagation model is needed to characterize the terrestrial network and evaluate the throughput more accurately in future works.

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

Funding: This work is supported in part by the National Key R&D Program of China under Grant 2018YFB1801103. The work of X. Ling is supported in part by the National Natural Science Foundation of China under Grant 61901111; the Natural Science Foundation of Jiangsu Province under Grant BK20190331; and the Research Fund of the National Mobile Communications Research Laboratory, Southeast University, under Grant 2019B02. The work of L. You is supported in part by the National Natural Science Foundation of China under Grant 61801114. The work of J. Wang is supported in part by the National Natural Science Foundation of China under Grants 61971130 and 61720106003; and the Natural Science Foundation of Jiangsu Province under Grant BK20160069. The work of X. Gao is supported in part by the Jiangsu Province Basic Research Project under Grant BK20192002.

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

Abbreviations

The following abbreviations are used in this manuscript:

PoW	proof of work
IoT	internet of things
TPS	transactions per second
MSNET	mobile satellite communication networks
DVB-S2	Digital Video Broadcasting Second Generation Satellite
DVB-S2X	Digital Video Broadcasting Second Generation Satellite Extensions
P2P	peer to peer
GEO	geostationary earth orbit
MEO	medium earth orbit
LEO	low earth orbit
VSAT	very small aperture terminal
SNR	signal-to-noise ratio
TV	television
GPS	global positioning system
PoS	proof of stake

References

1. Ling, X.; Le, Y.; Wang, J.; Ding, Z. Hash Access: Trustworthy Grant-Free IoT Access Enabled by Blockchain Radio Access Networks. *IEEE Netw.* **2020**, *34*, 54–61. [CrossRef]
2. Cao, B.; Li, Y.; Zhang, L.; Zhang, L.; Mumtaz, S.; Zhou, Z.; Peng, M. When Internet of Things Meets Blockchain: Challenges in Distributed Consensus. *IEEE Netw.* **2019**, *33*, 133–139. [CrossRef]
3. Ling, X.; Wang, J.; Bouchoucha, T.; Levy, B.C.; Ding, Z. Blockchain Radio Access Network (B-RAN): Towards Decentralized Secure Radio Access Paradigm. *IEEE Access* **2019**, *7*, 9714–9723. [CrossRef]
4. Ling, X.; Wang, J.; Le, Y.; Ding, Z.; Gao, X. Blockchain Radio Access Network Beyond 5G. *IEEE Wirel. Commun.* **2020**, in press.
5. Xiong, Z.; Zhang, Y.; Niyato, D.; Wang, P.; Han, Z. When Mobile Blockchain Meets Edge Computing. *IEEE Commun. Mag.* **2018**, *56*, 33–39. [CrossRef]
6. Xiong, Z.; Kang, J.; Niyato, D.; Wang, P.; Poor, V. Cloud/Edge Computing Service Management in Blockchain Networks: Multi-leader Multi-follower Game-based ADMM for Pricing. *IEEE Trans. Serv. Comput.* **2019**, *13*, 356–367. [CrossRef]
7. Yang, J.; He, S.; Xu, Y.; Chen, L.; Ren, J. A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks. *Sensors* **2019**, *19*, 970. [CrossRef]
8. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2794–2830. [CrossRef]
9. Dwork, C.; Naor, M. Pricing via Processing or Combatting Junk Mail. In Proceedings of the Annual International Cryptology Conferenc, Santa Barbara, CA, USA, 16–20 August 1992; pp. 139–147.
10. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. In Proceedings of the 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 31 July–3 August 2017.
11. Bagaria, V.; Kannan, S.; Tse, D.; Fanti, G.; Viswanath, P. Prism: Deconstructing the Blockchain to Approach Physical Limits. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS), New York, NY, USA, 17–20 November 2019; pp. 585–602.
12. Bitcoin Energy Consumption Index. Available online: https://digiconomist.net/bitcoin-energy-consumption (accessed on 29 September 2020).
13. Tschorsch, F.; Scheuermann, B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2084–2123. [CrossRef]
14. Poon, J.; Dryja, T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Available online: https://lightning.network/lightning-network-paper.pdf (accessed on 14 January 2016).
15. Sompolinsky, Y.; Zohar, A. Secure High-Rate Transaction Processing in Bitcoin. In Proceedings of the International Conference on Financial Cryptography and Data Security (FC), Berlin, Germany, 26–30 January 2015; pp. 507–527.
16. 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.
17. Devi, M.S.; Suguna, R.; Abhinaya, P.M. Integration of Blockchain and IoT in Satellite Monitoring Process. In Proceedings of the 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 20–22 February 2019; pp. 1–6.
18. La Beaujardiere, J.; Mital, R.; Mital, R. Blockchain Application Within A Multi-Sensor Satellite Architecture. In Proceedings of the 2019 IEEE International Geoscience and Remote Sensing Symposium (IGARSS), Yokohama, Japan, 28 July–2 August 2019; pp. 5293–5296.
19. 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]
20. Zhang, Y.; Liu, X. Satellite Broadcasting Enabled Blockchain Protocol: A Preliminary Study. *arXiv* **2004**, arXiv:2004.14591. Available online: https://arxiv.org/abs/2004.14591 (accessed on 30 April 2020).
21. BitSats. Available online: https://www.coindesk.com/tag/bitsat (accessed on 29 September 2020).
22. SpaceChain. Available online: https://spacechain.com/ (accessed on 29 September 2020).
23. BlockStream. Available online: https://blockstream.com/satellite/ (accessed on 29 September 2020).
24. ChainSat. Available online: https://chainsat.accubits.com/ (accessed on 29 September 2020).

25. Space Impulse. Available online: https://spaceimpulse.com/ (accessed on 29 September 2020).
26. SupremeSat. Available online: http://www.supremesat.com/ (accessed on 29 September 2020).
27. *Digital Video Broadcasting (DVB); Second Generation Framing Structure, Channel Coding and Modulation Systems for Broadcasting, Interactive Services, News Gathering and Other Broad-Band Satellite Applications (DVB-S2)*; ETSI EN 302 307-1 V1.4.1; European Telecommunications Standards Institute: Sophia Antipolis, France, June 2014.
28. *Digital Video Broadcasting (DVB); Second Generation Framing Structure, Channel Coding and Modulation Systems for Broadcasting, Interactive Services, News Gathering and Other Broad-Band Satellite Applications. Part 2: DVB-S2 Extensions (DVB-S2X)*; ETSI EN 302 307-2 V1.1.1; European Telecommunications Standards Institute: Sophia Antipolis, France, June 2014.
29. Decker, C.; Wattenhofer, R. Information Propagation in the Bitcoin Network. In Proceedings of the IEEE P2P 2013 Proceedings (P2P), Trento, Italy, 9–11 September 2013; pp. 1–10.
30. 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]
31. Lin, Z.; Lin, M.; Wang, J.; Huang, Y.; Zhu, W. Robust Secure Beamforming for 5G Cellular Networks Coexisting with Satellite Networks. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 932–945. [CrossRef]
32. Kodheli, O.; Lagunas, E.; Maturo, N.; Sharma, S.K.; Shankar, B.; Montoya, J.; Duncan, J.; Spano, D.; Chatzinotas, S.; Kisseleff, S.; et al. Satellite Communications in the New Space Era: A Survey and Future Challenges. *arXiv* **2002**, arXiv:2002.08811. Available online: https://arxiv.org/abs/2002.08811 (accessed on 20 February 2020).
33. You, L.; Li, K.; Wang, J.; Gao, X.; Xia, X.; Ottersten, B. Massive MIMO Transmission for LEO Satellite Communications. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 1851–1865. [CrossRef]
34. Wang, W.; Tong, Y.; Li, L.; Lu, A.; You, L.; Gao, X. Near Optimal Timing and Frequency Offset Estimation for 5G Integrated LEO Satellite Communication System. *IEEE Access* **2019**, *7*, 113298–113310. [CrossRef]
35. Wang, C.; Bian, D.; Shi, S.; Xu, J.; Zhang, G. A Novel Cognitive Satellite Network with GEO and LEO Broadband Systems in the Downlink Case. *IEEE Access* **2018**, *6*, 25987–26000. [CrossRef]
36. An, K.; Lin, M.; Zhu, W.; Huang, Y.; Zheng, G. Outage Performance of Cognitive Hybrid Satellite–Terrestrial Networks with Interference Constraint. *IEEE Trans. Veh. Technol.* **2016**, *65*, 9397–9404. [CrossRef]
37. Jiang, Y.; Yang, S.; Zhang, G.; Li, G. Coverage Performances Analysis on Combined-GEO-IGSO Satellite Constellation. *J. Electron.* **2011**, *28*, 228. [CrossRef]
38. Van Allen, J.A.; McIlwain, C.E.; Ludwig, G.H. Radiation Observations with Satellite 1958 ε. *J. Geophys. Res.* **1959**, *64*, 271–286. [CrossRef]
39. Judge, D.L.; Coleman, P.J., Jr. Observations of Low-Frequency Hydromagnetic Waves in the Distant Geomagnetic Field: Explorer 6. *J. Geophys. Res.* **1962**, *67*, 5071–5090. [CrossRef]
40. Barth, J.L.; Dyer, C.; Stassinopoulos, E. Space, Atmospheric, and Terrestrial Radiation Environments. *IEEE Trans. Nucl. Sci.* **2003**, *50*, 466–482. [CrossRef]
41. Rosenfeld, M. Analysis of Hashrate-Based Double Spending. *arXiv* **2009**, arXiv:1402.2009. Available online: https://arxiv.org/abs/1402.2009 (accessed on 9 February 2014).
42. Hu, S.; Jiang, L.; Shi, W. Design of BeiDou-based Data Acquisition System for Oil and Gas Wells in Remote Areas. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Kuantan, Malaysia, 30–31 July 2019; pp. 012090–012103.
43. Kayes, A.S.M.; Kalaria, R.; Sarker, L.H.; Islam, M.S.; Watters, P.A.; Ng, A.; Hammoudeh, M.; Badsha, S.; Kumara, I. A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues. *Sensors* **2020**, *20*, 2464. [CrossRef] [PubMed]
44. Kayes, A.S.M.; Rahayu, W.; Watters, P.; Alazab, M.; Dillon, T.; Chang, E. Achieving security scalability and flexibility using Fog-Based Context-Aware Access Control. *Future Gener. Comput. Syst.* **2020**, *107*, 307–323. [CrossRef]