Immediate Economic Opportunities for Blockchains in Space

David Hyland-Wood[*†‡] Peter Robinson[*†] Brett Henderson[*] Christopher Hare[*]
Roberto Saltini[§] Sandra Johnson[*] Chris Lewicki[¶‡]

TODO: A survey paper covering the existing blockchains in space trials (e.g. SpaceChain, Blockstream), the cybersecurity work from the ICSSC and SDLT papers, Mandl?s spacecraft tasking approach using smart contracts, and Lobao?s idea for an after-market economy for spacecraft in (e.g.) geosynchronous graveyard orbits.

Nomenclature

TODO: Revisit and probably remove.

n	A blockchain node
N_n	The total number of participating blockchain nodes
v	A validator participating in a blockchain consensus protocol
N_v	The total number of participating validators
Subscript	
i	Variable number

I. Introduction

TODO: Start from scratch.

II. Literature Review

TODO: Remove material unrelated to this paper. Retain and focus on other companies' fielded or proposed economic opportunities.

The application of blockchain technologies to space operations has recently attracted significant attention. Examples of companies currently providing some form of blockchain operations in Earth orbit include the SpaceChain Foundation[a] (two CubeSats in LEO operating nodes of a QTum blockchain), and Blockstream[b] (using five existing telecommunications satellites in GEO to broadcast the Bitcoin data stream). Several other for-profit and non-profit companies have announced plans to build organizations using blockchain technology or deploy systems including blockchain components to the LEO environment; for example, Space Decentral[c], SpaceBridge Logistics[d], SpaceBit Blockchain for Space Alliance[e], and Space Fund[f]

[*] PegaSys, ConsenSys Australia, Brisbane, Queensland, Australia

[†] School of Information Technology and Electrical Engineering, The University of Queensland, Brisbane, Queensland, Australia

[‡] AIAA Member

[§] PegaSys, ConsenSys Australia, Sydney, New South Wales, Australia

[¶] ConsenSys Space, Redmond, Washington, USA

[a] https://spacechain.com/

[b] https://blockstream.com/

[c] https://spacedecentral.net/

[d] http://spacebridge.io/

[e] https://spacebit.com/

[f] https://spacefund.com/

Researchers in several countries have proposed future uses of blockchains in space including:

- use as a property registry[1]
- for identity management, especially for protection against cyber attacks[2,3]
- to “facilitate on-orbit satellite communication data integrity and security”[4]
- to reduce “manual intervention in monitoring and control”[5]
- in “tracking various components of vehicles”[5]
- as a component of “smart services for space traffic management”[6]
- as a means to coordinate the fulfillment of a desired operation carried out by many individual spacecraft[7]

Researchers with government, especially military, connections in China, Russia and the United States are actively investigating uses of blockchains for the access security and data integrity of Earth-orbiting satellites. Published Chinese military interest seems to be focused on preventing “cyber & physical attacks” against space assets,[2] and to allow “multiple departments to participate in the maintenance and update of equipment status”.[8] The Roscosmos State Corporation for Space Activities in Russia is developing a “digital platform for control spacecrafts” [sic] and for “use of ground stations” focused on the “Roskosmos orbital group” of satellites.[6] It has been suggested that “the US military has taken a fancy to the anonymity of blockchain in recording transactions, and has begun to expand to the field of intelligence gathering to achieve covert targeted payments for incentive personnel.” [sic].[8] Mandl, at NASA Goddard Space Flight Center, has proposed using smart contracts on blockchains to create a “Remote Sensing as a Service” offering.[7] In Mandl’s conception, a single Earth observation requirement could be obtained by multiple platforms conducting multiple observations under a variety of conditions until a desired goal is achieved.

The use cases above related to space-based communications security bear resemblance to similar terrestrial use cases for communication security of air traffic control systems[9] and bear significant resemblance to issues encountered in distributed Internet of Things networks (e.g.[10,11]).

Motivations to close security vulnerabilities on spacecraft are generally synonymous with motivations for securing services on the public Internet. Attacks may be conveniently separated into two types: attempts to gain unauthorised control (colloquially known as “hacking”) and attempts to deny service (“jamming” in the context of radio communications[12]). Spacecraft and ground-based systems that control them are at risk of both active hacking and denial-of-service attacks.

Although few spacecraft operators publicly acknowledge cybersecurity incidents, governmental transparency regulations in the United States have allowed evidence of some incidents to be acknowledged. Examples include attacks by Chinese state actors that led to unauthorised access to “networks that control spacecraft” at NASA JPL[13] and acknowledgement that U.S. Air Force satellites are “jammed by commercial equipment easily acquired by state and nonstate actors”.[14] One can reasonably assume that commercial satellite operators and space assets controlled by other national governments have had and continue to face similar challenges.

We therefore begin by ensuring that we match stated domain requirements to a theoretical framework for blockchain applicability. Several researchers (e.g.[15,16] have proposed decision trees to help determine the applicability of blockchains to particular domains. We will follow Wst and Gervais[15] to suggest blockchain properties that could be used to satisfy the goals for space-related use cases. Wst and Gervais determined blockchains are best used when the following criteria are met:

- Storage of state is required;
- The system has multiple writers;
- A trusted third party is not appropriate or not available, or a controlling third party’s network cannot be trusted due to potential intrusion;
- Issues of slow latency or low throughput are acceptable;
- A centrally managed system is inappropriate or not practical.

Wüst and Gervais continue by noting that a permissionless blockchain should be used when the above conditions are met and not all writers are known, and a permissioned blockchain should be used when the above conditions are met and all writers are known. It would seem based upon their analysis that blockchain matches the criteria for an in-space economy where the participants include multiple spacecraft controlled by multiple operators which may change over time. There is certainly no agreed arbiter of a future in-space economy at the time, and it would seem reasonable to question whether one could rapidly arise.

Cybersecurity best practices from the field of computer science could be borrowed and extended to secure spacecraft communications. Relevant approaches used to control remote access to cloud computing resources and weapon systems include multi-factor authentication[17] and multi-party authorisation.[18] Either may be used to secure edge devices by using callbacks to secure external information.

Multi-factor authentication is used to ensure that a user is who they say they are. For example, one may provide credentials to log onto their bank?s IT systems, and then subsequently be asked to confirm their login via an email, message to their mobile phone, or use of a separate hardware token. The second, hopefully independent, confirmation of their identity significantly increases the challenges facing a remote attacker attempting to gain unauthorised access.

Similarly, multi-party authorisation requires a separate party to validate an operation you wish to perform before you are allowed to proceed. In the case of your banking system, your bank may wish to confirm an attempt to close a joint account with the other owner before taking action.

Several of the authors have previously outlined how a blockchain with certain properties and configuration can be used to secure spacecraft communication command channels via multi-factor authentication, multi-party authorisation or both simultaneously.[19] We noted in the same paper that blockchains may be used as trust systems when a central authority may not be able to be trusted, as is the case when the underlying network, network services and/or user accounts may have been compromised.

The space environment imposes limitations and presents challenges that are quite different from the air-conditioned, high-bandwidth terrestrial environments where early blockchain technologies were developed.

Properties of the near-Earth orbital space environment that impose additional limitations on blockchain technologies include:

- Limited computing system resources. Limitations include computational capabilities and memory[20] and storage.[2] Electrical power available to be dedicated to computation is also generally limited, as is the ability of a spacecraft thermal control system to maintain a computing system within operational limits.
- "environmental restrictions including noisy, bandwidth limited, asymmetrical, and interrupted communications links".[20]

Communication delays may be compounded by mission-specific requirements. For example, some space missions include "a requirement for early access to transferred data regardless of its quality".[20] Choices between early, low-quality data and later higher-quality data, coupled with ever-changing relative positions and thus propagation delays, possibilities for communications blackouts due to positions, power availability, errors, or other factors combine to make specific situations unique.

The farther from Earth one operates in space, the more propagation delays affect communications. Such delays are an important facet of space systems design (e.g.[2,20]). Delays are a particularly important design criterion for blockchain consensus algorithms because timeouts are a nearly universal feature of such algorithms to determine when consensus cannot occur, and to denote error conditions.

It is straightforward to determine propagation delays in radio communication if one knows the distances involved since radio waves travel at the speed of light. Propagation delays between Earth and Mars can vary between as little as three and a half minutes each way and as much as twenty four minutes each way depending on the relative positions of the two planets in their orbits. Delays to the outer edge of the main asteroid belt, known as the outer Kirkwood gap, can reach over thirty five minutes in each direction when a spacecraft at the outer Kirkwood gap is in conjunction with Earth. Additionally, available communications bandwidth is degraded as propagation losses increase. It is clear that consensus algorithms used on blockchains for space operations even within the inner Solar System (that narrow toroid defined by Earth, the Moon, Mars, and the main asteroid belt) will need to treat such lengthy propagation delays as a key design criterion.

Spacecraft communicating with controllers solely via relays require certain adjustments to be made to their designs to allow them to maintain fault-tolerant operations.[21] Those adjustments include:

- Provisions for autonomous operations during communications loss due to issues with the relays;
- Control of communications rates by the relays coupled with mechanisms for automated command filtering to prevent spacecraft in a safe mode from receiving commands intended for a non-faulted spacecraft;
- A recognition that pseudo-real-time spacecraft operational command rates will be significantly slower than direct links;
- Designs allowing spacecraft commands to be sent "in the blind", with automatic handling of inappropriate commands on the spacecraft itself;
- Designs that anticipate and automatically handle a greater number of communications disruptions due to the relays.

Some of the limitations noted above are physical and so immutable over time, such as light speed delays, and physical lines of sight. Others are dependent on the state of technology, and are thus likely to change, such as compute, memory, storage, power generation and heat rejection. Economic transactions in space are similarly most likely to start as small in message sizes, bandwidth usage, and in absolute number, but may reasonably be expected to grow by orders of magnitude as an in-space economy develops and becomes a mainstream activity. Any proposed technological solution to treat these requirements as design criteria should therefore take into account those that might change and those that are fixed.

Difficulties in communication with spacecraft have been experienced for decades, and solutions have been implemented in depth. Newer techniques have included experiments with lasers to increase the directionality, and hence the available bandwidth, of direct spacecraft communications. However, regardless of available bandwidth, the limitations above will continue to dominate communication systems. The Consultative Committee for Space Data Systems, an international cooperative body to create space data standards, has been working on this problem since the 1980s. The CCSDS File Delivery Protocol (CFDP) has provided a standard file transfer protocol for transmitting data to spacecraft since 2002.[20] CFDP supports both unreliable and reliable file-oriented data transfer. While these standards are increasingly comprehensive, spacecraft flight software implementations of them are almost always partial (often with cost/implementation-convenient violations of the standards), and not yet available in open-source repositories.

Data transfer over unreliable communication links can nevertheless be made reliable by the use of various error-detection and error-correction schemes. NASA's deep space missions and some commercial telecommunications satellites are currently using forward error-correction Turbo codes[22] for this purpose. Data security considerations for deep space missions has thus far been minimal, as the physical barriers to interacting with these assets are severe.

A useful approach to abstract above current Internet networking protocols for an "interplanetary Internet" was developed to ensure delivery of file-oriented data in a "postal model of communication".[23] This email-like functionality over communications systems with very high degrees of transmission latency was specifically aimed at deep space communications challenges. The effort was confusingly known as Disruption Tolerant Networking at the funding agency, the U.S. Defense Advanced Projects Research Agency (DARPA). Unfortunately, the proposals did not progress to the Standards Track of the Internet Engineering Task Force where they were originally published, and the original research group disbanded around 2005. New work on Delay/Disruption Tolerant Networking currently continues at NASA.[24]

Prototypical implementations of Delay/Disruption Tolerant Networking demonstrated successful operation with delays lasting up to sixty minutes. Round-trip communication delays in the Earth-Moon-Mars-asteroid belt toroid suggest the motivating factor in testing delays of that period.

The notional "heart" of a blockchain is its consensus algorithm. A blockchain consensus algorithm defines the steps necessary for blockchain participants to agree on information to be added to the distributed ledger. It is how the nodes in the network agree (come to consensus on) the next block to be added to the chain.[25]

Existing blockchain consensus algorithms have been recognized by many as limiting the applicability of blockchains to space operations.[2–4, 7, 8] It is particularly important to recognise the engineering tradeoffs inherent in increasing power consumption on spacecraft.[26]

Several researchers have suggested the applicability of Ethereum as a possible blockchain framework (e.g.[27]), but noted that the consensus algorithms currently used on the public production Ethereum blockchain (known as "Ethereum MainNet") are inappropriate for use in space operations.[3, 4, 28] Neither the traditional proof of work (PoW) algorithm nor the forthcoming proof of stake (PoS) consensus algorithm used on Ethereum MainNet or its public test networks provide the properties needed for space operations. For example, Ethereum PoW is intentionally designed to be computationally intensive, and Ethereum PoS relies upon the blockchain having an economically meaningful cryptocurrency to be used for internal operations. Neither algorithm would cope well with blockchain nodes operating in a significantly time-delayed, or low-availability network environment.

Changing the consensus algorithm of an Ethereum system creates a blockchain that is incompatible with Ethereum MainNet, at least under the current state of the art. Those taking this path (e.g. the Enterprise Ethereum Alliance and its members, and those researchers cited in the previous paragraph) are thus proposing "private" or "enterprise" Ethereum blockchains with consensus algorithms and perhaps other properties they deem appropriate for operations in their contexts.

Three groups have suggested the Practical Byzantine Fault Tolerance (PBFT) algorithm[29] as a possible consensus algorithm for near-Earth orbital space operations.[2,4,28] PBFT is a so-called proof of authority (PoA) algorithm, in that certain network nodes are given authority to act as proxies for many other nodes. One presumes those researchers meant to suggest PBFT as modified for use as a blockchain consensus algorithm, e.g. Istanbul Byzantine Fault Tolerance,[30] since PBFT was not itself defined with blockchains in mind. The PBFT family of consensus applications are an imperfect fit for orbital space operations given their reliance on time and connectivity as critical algorithmic components. Timeouts resulting from communications delays, occultation, radio interference, and other communication disruptions are all too common with spacecraft, but are used to determine error conditions in the PBFT family of consensus algorithms. PBFT algorithms would be an even less perfect fit for deep space operations where such communication disruptions are routinely expected. PBFT message sizes also tend to be large in practice, which work against the bandwidth, processing, and storage capabilities of most extant and proposed spacecraft.

As noted by Beldavs, "Central to the economy is money and rules for transacting business, as well as institutions that facilitate business activity such as banks."[1] Blockchains can theoretically fulfill all of those criteria. The two largest, and earliest, public blockchains Bitcoin[31] and Ethereum[32,33] have both created usable currencies (in spite of their volatile prices), have defined rules for transacting business, and include smart contract functionality[34] that may be used to facilitate business activity.

Beldavs suggests that the establishment of property rights and the use of a property registration system are necessary conditions for the establishment of an in-space economy.[1] He asserts that any future property rights over space resources "will need to be compliant with the Outer Space Treaty that excludes conventional real property whose ownership rights are granted by a sovereign state." While he is correct in quoting Article II of the Outer Space Treaty[35] "Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means", it is currently unclear that the Outer Space Treaty will survive large-scale economic activities in space, nor that those with fortunes to be made will voluntarily bind themselves to it. The approach generally taken in the field of economics, i.e. empirically considering the choices humans make given incentives, would tend to indicate that exactly the opposite may happen. The Outer Space Treaty is likely to be replaced by subsequent agreements that both allow and foster an in-space economy. Others have noted that the current legislative structures focus on "the non-militarisation of space, the promotion of scientific endeavours and the mitigation of orbital debris. However, the legislative framework does not presently anticipate the use of orbital planes in LEO for commercial actors or the management of orbital shells for LEO."[36] Effective "natural monopolies" could therefore form (in the absence of new legislation or treaties) by commercial dominance of particularly useful orbital shells. The anticipated dominance of at least one orbital shell by SpaceX Starlink communications satellites is a topical example of such an effective monopoly, and a practical reason to suggest that the current legislation environment is unstable due to the rise of commercial space interests.

Israel has proposed that a lex mercatoria-like system similar to the economies that developed between companies operating away from their home countries during the Age of Exploration may form in space.[27] Blockchains, with their decadal history of performing lex mercatoria-like operations, seem to be a reasonable fit for the likely conditions.

III. Some Immediate Economic Opportunities

TODO: Existing blockchain technologies can be used to suggest at least some immediate applications in space systems operations.

A. Spacecraft Cybersecurity

TODO: Recapitulate and perhaps extend ICSSC and SDLT papers.

B. Service Economies

1. Tasking Spacecraft

TODO: We have software and infrastructure to implement Dan Mandl's proposal for an abstract tasking economy for Earth-observing spacecraft via smart contracts.

2. After-Market Economy Following Primary Mission Fulfillment

TODO: Xavier Lobao's idea for an after-market economy for spacecraft in (e.g.) geosynchronous graveyard orbits.

IV. Conclusions

TODO

V. Further Work

TODO:

- Immediate next steps
  - implementations of some of the above;
  - fieldings of the above;
  - more immediate applications of existing technology;
  - more generalised blockDAG approaches / note the concept of blockchain is changing rapidly;
- Future Research
  - more formal proofs of consensus protocols;
  - more work on consensus for asynchronous networks and blockDAGs;
  - more work on crosschain protocols;
  - greater understanding of economic theories of money especially possible relationships between government regulations/policies/laws/fiat currencies and decentralised cryptocurrencies/tokenised assets.

Acknowledgments

The authors gratefully acknowledge ConsenSys AG for supporting this research, especially its PegaSys division.

References

[1] Beldavs, V., "Blockchains and the emerging space economy," *The Space Review*, 2016.

[2] Cheng, S., Gao, Y., Li, X., Du, Y., Du, Y., and Hu, S., "Blockchain Application in Space Information Network Security," *Space Information Networks*, edited by Q. Yu, Vol. 972, Springer Singapore, pp. 3–9.

[3] Xu, R., Chen, Y., Blasch, E., and Chen, G., "Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness," *Optical Engineering*, Vol. 58, No. 4, Feb 2019, pp. 041609.

[4] Molesky, M. J., Cameron, E. A., Jones, J., Esposito, M., Cohen, L., and Beauregard, C., "Blockchain Network for Space Object Location Gathering," *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Nov 2018, pp. 1226–1232.

[5] Jennath, H. S., Adarsh, S., and Anoop, V. S., *Distributed IoT and Applications: A Survey*, Studies in Computational Intelligence, Springer Singapore, 2019, pp. 333–341.

[6] Skobelev, P. O. and Lakhin, O. I., "Towards the digital platform and smart services for managing space traffic," *International Journal of Design & Nature and Ecodynamics*, Vol. 13, No. 2, Jun 2018, pp. 187–198.

[7] Mandl, D., "Bitcoin, Blockchains and Efficient Distributed Spacecraft Mission Control," Sep 2017.

[8] Gao, Y., Hu, S., Tang, W., Huang, D., Sun, Y., Li, X., and Cheng, S., *Situational Awareness in Space Based Blockchain Wireless Networks*, Vol. 972, Springer Singapore, 2019, pp. 15–20.

[9] Reisman, R., *Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy*, No. 20190000022, Jul 2019.

[10] Dorri, A., Kanhere, S. S., Jurdak, R., and Gauravaram, P., "Lsb: A lightweight scalable blockchain for iot security and privacy," *arXiv preprint arXiv:1712.02969*, 2017.

[11] Dorri, A., Kanhere, S. S., and Jurdak, R., "MOF-BC: A memory optimized and flexible blockchain for large scale networks," *Future Generation Computer Systems*, Vol. 92, 2019, pp. 357–373.

[12] Sowmya, S. and Malarchelvi, P. D. S. K., "A survey of jamming attack prevention techniques in wireless networks," *International Conference on Information Communication and Embedded Systems (ICICES2014)*, IEEE, Feb 2014, pp. 1–4.

[13] No. IG-19-022, Jun 2019.

[14] Creedon, M., *Space and Cyber: Shared Challenges, Shared Opportunities*, Strategic Studies Quarterly, Nov 2011.

[15] Wüst, K. and Gervais, A., *Do you need a Blockchain?*, No. 375, 2017.

[16] Xu, X., Weber, I., and Staples, M., *Design Process for Applications on Blockchain*, Springer International Publishing, 2019, pp. 93–111.

[17] Moussa, M. A. and Chan, C. S., "Plurality-factor security system," Mar 2000.

[18] Carley, J. A., "Near real-time multi-party task authorization access control," Apr 2009.

[19] Hyland-Wood, D., Robinson, P., Saltini, R., Johnson, S., and Hare, C., "Methods for Securing Spacecraft Tasking and Control via an Enterprise Ethereum Blockchain," *Proceedings of 37th ICSSC International Communications Satellite Systems Conference*, October 2019.

[20] for Space Data Systems, C. C., "CCSDS File Delivery Protocol (CFDP)," Jan 2007.

[21] Lewicki, C., Krajewski, J., Ilott, P., and Dates, J., "Phoenix Mars Scout UHF Relay-Only Operations," *SpaceOps 2006 Conference*, American Institute of Aeronautics and Astronautics, Jun 2006.

[22] Berrou, C., Glavieux, A., and Thitimajshima, P., "Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1," *Proceedings of ICC '93 - IEEE International Conference on Communications*, Vol. 2, IEEE, 1993, pp. 1064–1070.

[23] Burleigh, S., Hooke, A., Torgerson, J. L., Fall, K., Cerf, V., Durst, B., Scott, K., and Weiss, H., "Delay-tolerant networking: an approach to interplanetary Internet," *IEEE Communications Magazine*, Vol. 41, No. 6, Jul 2003, pp. 128–136.

[24] Mahoney, E., "Disruption Tolerant Networking," Mar 2016.

[25] Hyland-Wood, D. and Khatchadourian, S., "A Future History of International Blockchain Standards," *Journal of the British Blockchain Association*, Vol. 1, No. 1, Jun 2018, pp. 3724.

[26] Lyke, J., Mee, J., Edwards, A., Pineda, A., DeBenedictis, E., and Frank, M., "On the energy consequences of information for spacecraft systems," *2017 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*, Oct 2017, pp. 104–109.

[27] Israel, B., "Space Resources in the Evolutionary Course of Space Lawmaking," *American Journal of International Law*, Vol. 113, 2019, pp. 114–119.

[28] Mital, R., de La Beaujardiere, J., Mital, R., Cole, M., and Norton, C., *Blockchain application within a multi-sensor satellite architecture*, No. 20180006549 in NASA Technical Report, Apr 2019.

[29] Castro, M. and Liskov, B., "Practical Byzantine Fault Tolerance," *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, Feb 1999.

[30] Lin, Y. T., "Istanbul Byzantine Fault Tolerance - Issue #650 - ethereum/EIPs," Jun 2017.

[31] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[32] Buterin, V., "Ethereum White Paper," 2013.

[33] Wood, G., "Ethereum: A Secure Decentralised Generalised Transaction Ledger, Ethereum project yellow paper 151," 2014, pp. 39.

[34] Szabo, N., "Smart Contracts," 1994.

[35] on the Peaceful Uses of Outer Space, U. N. C., *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, Vol. 610 UNTS 205, 1967.

[36] Green, T., Neumann, P., and Grey, K., "Mitigation of anti-competitive behaviour in telecommunication satellites and management of natural monopolies," International Astronautical Federation (IAF), Oct 2018.