Blockchain Properties for Near-Planetary, Interplanetary and Metaplanetary Space Domains

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

Blockchain technologies have demonstrated new and interesting ways to construct terrestrial economies, including the well-known public cryptocurrencies, but also as means to facilitate business-to-business (B2B) and business-to-consumer (B2C) transactions. Some have recently proposed uses for blockchains in space. This paper identifies desirable blockchain properties that could be used to construct future in-space economies.

Three general economic domains are anticipated, each with their own communications limitations that drive the selection of applicable blockchain properties: Operations in orbits around planetary bodies where realtime communication is possible (e.g. within cislunar space around Earth or cisdeimotic space around Mars), operations across interplanetary space between spheres of influence where pseudo-realtime communication is possible (e.g. Earth-Mars or Earth-asteroids), and operations in metaplanetary space within the Solar system but beyond the limit of pseudo-realtime communication. Blockchain properties are suggested for each domain, with a focus on the selection of blockchain consensus algorithms. Evaluation is performed on the readiness of extant technologies to operate in each domain.

Added hyphenation for blockchain, blockchains and economies to fix some box overfull issues

Modified the following sentence

Nomenclature

b Average block size, a function of the number of transactions per block
n The number of blockchain nodes in a network

I. Introduction

Blockchain technologies have demonstrated new and interesting ways to construct terrestrial economies, including the well-known public cryptocurrencies, but also as means to facilitate business-to-business (B2B) and business-to-consumer (B2C) transactions. This paper identifies desirable blockchain properties that could be used to construct in-space economies.

Modified the following sentence

An in-space blockchain can serve as a natural basis for an in-space economy due to the ability of a blockchain to establish a trust environment of peers in consensus, and a facility to execute smart contracts when and if certain (perhaps difficult) activities are provably undertaken. Many, although certainly not all, of the smart contracts implemented to date execute economic agreements; we suggest that general trend is likely to continue into activities in space. It is therefore not too early to think about the properties required by an in-space blockchain.

Modified the following sentence

Spacecraft face challenges not present with terrestrial computing systems. Due to launch costs, limitations in means of making or carrying electrical power, and the challenges of dissipating heat in a vacuum, available power and computation capabilities are much more limited on spacecraft than they are terrestrially. Moreover, computation, non-volatile and volatile memory options are constrained by the limits

*PegaSys, ConsenSys Australia, Brisbane, Queensland, Australia
†School of Information Technology and Electrical Engineering, The University of Queensland, Brisbane, Australia
‡AIAA Member
§ConsenSys Space, Redmond, Washington, USA
¶PegaSys, ConsenSys Australia, Sydney, New South Wales, Australia
‖ARC Centre of Excellence for Mathematical and Statistical Frontiers, Queensland University of Technology, Brisbane, Australia

imparted on microelectronics in order to operate reliably in hard radiation environments. Spacecraft have to cope with great distances leading to significant light speed delays in communication, and occasional inability to get a line-of-sight to communications nodes in the same network. Such distances create challenges in data integrity verification, communications acknowledgements, store-and-forward and multi-path considerations, compounded by free-space path losses resulting in bandwidth constraints. This swathe of challenges introduced by spacecraft necessitates the invention of new kinds of blockchains to serve those needs.

Three general economic domains are anticipated, each with their own communications limitations that drive the selection of applicable blockchain properties: Operations in orbits around planetary bodies where realtime communication is possible (e.g. cislunar space within the orbit of Earth's moon or "cisdeimotic" space within the orbit of Mars' moon Deimos), operations across interplanetary space between spheres of influence where pseudo-realtime communication is possible (e.g. Earth-Mars or Earth-asteroids), and operations in metaplanetary space within the Solar system but beyond the limit of pseudo-realtime communication. Blockchain properties are suggested for each domain, with a focus on the selection of blockchain consensus algorithms. Evaluation is performed on the readiness of extant technologies to operate in each domain.

This paper will review current implementations and proposals for blockchain uses in space (Section II). We will then determine desirable blockchain properties for the three domains (Section III):

Modified the following sentence

(a) Near-planetary space

(b) Interplanetary space

(c) Metaplanetary space

Figure 1 illustrates the three domains with a toroid of interest for medium-term in-space economies. The toroid is defined for convenience with an inner edge at the Earth-Sun L_1 point, an outer edge at the outer limit of the main asteroid belt at the strong Kirkwood gap at 3.27 AU from the Sun (where asteroids are in a 2:1 mean-motion resonance with Jupiter, also known as the Hecuba gap), and with upper and lower bounds ±20 degrees from Sun center above and below the plane of the ecliptic.

Finally, we will report our conclusions and suggest directions for future work.

II. Literature Review

The application of blockchain technologies to space operations has recently attracted significant attention. At least two companies currently provide some form of blockchain operations in Earth orbit: SpaceChain Foundation[a] has launched two CubeSats into LEO, operating nodes of a QTum blockchain, and has deployed a multi-signature cryptocurrency wallet experiment via Nanoracks on the International Space Station. Blockstream[b] leases bandwidth on five existing GEO telecommunications satellites to broadcast the Bitcoin data stream.

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] (i.e. secure command and control)
- 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]

[a] https://spacechain.com/
[b] https://blockstream.com/

Researchers with government or military connections in China, Russia and the United States are actively investigating uses of blockchains for 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.

Added the following subsection to give some organisation to the lit review

A. Applicability of Blockchain Technology

The space-based communications security use cases above 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]).

The first question that we ought to answer is whether a blockchain is a legitimate solution for these use cases. We therefore begin by ensuring that we match stated domain requirements to a theoretical framework for blockchain applicability. Several researchers (e.g.[12,13]) have proposed decision trees to help determine the applicability of blockchains to particular domains. We will follow Wüst and Gervais[12] to suggest blockchain properties that could be used to satisfy the goals for some space-related use cases. Wüst and Gervais determined blockchains are best used when all of 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, and a centrally managed system is inappropriate or not practical.

Modified the following sentence to highlight the first research question that we aim to answer

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. Using their guidelines, we find that an in-space economy where the participants include multiple spacecraft controlled by multiple operators which may change over time, matches the criteria for a blockchain. There is certainly no agreed arbiter of a future in-space economy at this time, and it would seem reasonable to question whether one could arise due to the currently rapid decentralization of spacecraft ownership.

The small number (in distributed computing terms) of extant and expected spacecraft could allow for a "closed economy" wherein participants may be well known and require either permission or at least registration to join or leave a network. Such permissioned networks trade off software complexity (especially the need to manage cryptographic keys) with simpler runtime requirements (due to the ability to know, and therefore to some degree trust) participants.

Several of us (Hyland-Wood, Robinson, Saltini, Johnson and Hare) have previously outlined how permissioned 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.[14] We proposed using such a system to secure spacecraft command channels in the presence of cybersecurity attacks against networks that control spacecraft.

It also seems appropriate to apply blockchains to the building of in-space economies because they have been successfully used to build terrestrial economies. As noted by Beldavs,[1] "Central to the economy is money and rules for transacting business, as well as institutions that facilitate business activity such as banks.". Blockchains can theoretically fulfill all of those criteria. The two largest, and earliest, public blockchains Bitcoin[15] and Ethereum[16,17] have both created usable currencies (in spite of their volatile prices), defined rules for transacting business, and included smart contract functionality[18] that may be used to facilitate business activity.

Added full stop between these two sentences

Beldavs[1] further 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

Added full step between these two sentences

quoting Article II of the Outer Space Treaty[19] "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.".[20] 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 orbital shells by SpaceX Starlink, OneWeb, and Amazon Kuiper communications satellites are topical examples of such effective monopolies, and a reason to suggest that the current nation-based legislative environment (as defined in Article VI of the Outer Space Treaty[19]) is unstable due to the rise of commercial space interests.

Israel has proposed that a *lex mercatoria*-like system may form in space, similar to the economies that developed between companies operating away from their home countries during the Age of Exploration.[21] Blockchains, with their decadal history of performing *lex mercatoria*-like operations, seem to be a reasonable fit for the likely conditions.

Added full stop between these two sentences

Added subsection

B. Challenges with Deploying Blockchains in Space

The second question that we ought to answer is whether blockchains can actually be deployed in space. This because 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.

Added the following sentence to highlight the second research question that we aim to answer

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

- *computing system resources*. Limitations include computational capabilities, memory[22] 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 conditions.* Limiting environmental conditions include "noisy, bandwidth limited, asymmetrical, and interrupted communications links".[22]

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".[22] Choices between early, low-quality data (including "lossy" data and/or partial data sets) 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.[2,22] Delays are a particularly important design criterion for blockchain consensus algorithms because timeouts are often used 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 to 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, as illustrated in Fig. 1) will need to treat such lengthy propagation delays as a key design criterion.

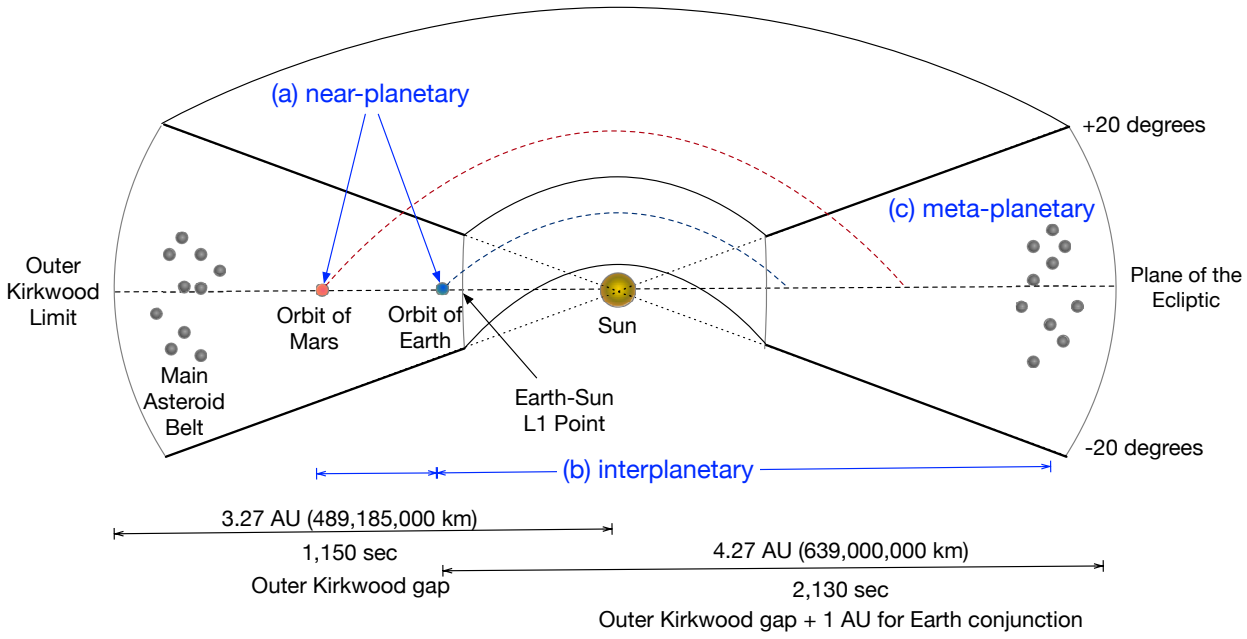

Figure 1. A toroid of interest for a near-future in-space economy

Spacecraft communicating with controllers solely via relays require certain adjustments to be made to their designs to allow them to maintain fault-tolerant operations.[23] Those adjustments include designs that anticipate and automatically handle a greater number of communications disruptions due to the relays, and designs allowing spacecraft commands to be sent "in the blind" with automatic handling of inappropriate commands on the spacecraft itself. Such considerations provide important design criteria for any distributed computing scenario.

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 treating 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.[22] 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[24] 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".[25] 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.[26]

Prototypical implementations of Delay/Disruption Tolerant Networking demonstrated successful operation with delays lasting up to sixty minutes. Round-trip communication delays within 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.[27]

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.[28]

Several researchers have suggested the applicability of Ethereum as a possible blockchain framework (e.g.[21]), 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.[3,4,29] 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[30] as a possible consensus algorithm for near-Earth orbital space operations.[2,4,29] One presumes those researchers meant to suggest PBFT as modified for use as a blockchain consensus algorithm, e.g. Istanbul Byzantine Fault Tolerance,[31] since PBFT was not itself defined with blockchains in mind. The PBFT family of consensus applications are a possible, but 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. However, blockchains using PBFT algorithms located terrestrially or in orbits with certain restrictions (i.e. those with continuous communication ability, including those in geosynchronous orbits and those in LEO/MEO orbits with communications relays) may still be a reasonable component of integrated space systems.

III. Desired Blockchain Properties

Several logical blockchain-spacecraft relationships are possible, and each relationship implies a different overall systems architecture. Figure 2 illustrates four possible architectural relationships between a blockchain and a spacecraft. A spacecraft may act as a regular blockchain node (a), or as a mining node, sometimes also known as a writer or a validator (b). A spacecraft may simply read information from a blockchain (c) or request transactions be written to a blockchain (d). These possible relationships imply

very different computation capacity and radio bandwidth onboard spacecraft, especially due to overall message traffic and average message size. We will suggest a blockchain-spacecraft relationship suitable for each of the target domains.

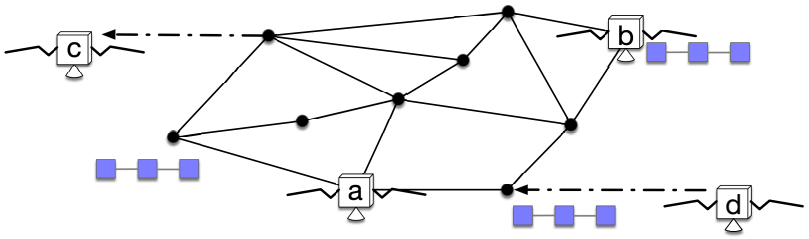

Figure 2. Possible blockchain-spacecraft relationships

Table 1 compares the possible relationships between spacecraft and blockchains in terms of the relative amount of message traffic necessary to participate in each manner, and the relative degree to which onboard software would need to change to support blockchain operations of each type. By far the most compelling relationship between a spacecraft and a terrestrial blockchain is for the spacecraft to read information from the blockchain, as illustrated in Fig. 2(c) and compared in Table 1. The costs for such read operations are minimal in terms of both message traffic and the degree of software changes. Most existing spacecraft do not have the computational capability to operate a blockchain node, although that restriction seems likely to ease as newer compute buses become space qualified.

Table 1. Comparison of possible blockchain-spacecraft relationships

Relationship	Message traffic to/from satellite	Changes needed to onboard software
(a) Regular node	High	High
(b) Mining node	High	High
(c) Read-only	Low	Low-Medium
(d) Write request	Low	Medium

A. Near-Planetary Economies

Terrestrial distributed computing systems may choose to access sub-millisecond timing signals available via global navigation satellite systems (GNSS) or atomic clock broadcast signals. Spacecraft in Earth orbit can similarly leverage such signals to develop and maintain a common sense of time, even when relativistic corrections must be made. Spacecraft in Earth orbit also naturally suffer less from extreme time delays or communication loss than those in deep space.

With a common notion of time and relatively short time delays, devices within cislunar space can effectively join terrestrial blockchains that use time as an intrinsic part of their consensus algorithms. Developing similar systems around Mars (say, within cisdeimotic space) will require similar infrastructure to that used around Earth. One tradeoff that must be made is the limitations imposed by light speed delays on block creation speed. That is probably acceptable as long as the number of space-to-space transactions is relatively small.

It is possible, and probably preferred, to treat most orbiting spacecraft as edge devices as opposed to expecting them to run blockchain node software. In such a scenario, spacecraft may read transactions from, or propose transactions to, a blockchain operated terrestrially. Blockchain nodes on spacecraft are anticipated to remain special-purpose devices deployed on few spacecraft for some time to come.

1. *Consensus Algorithm Selection for Near-Planetary Space*

Blockchain consensus protocols build on decades of experience creating consensus in distributed computing systems. The most commonly used families of consensus protocols include the proof of work (PoW) algorithms used by the public Bitcoin and Ethereum networks, the proof of stake (PoS) algorithms such as

the Ethereum network is attempting to migrate to using, and proof of authority (PoA) algorithms used in private, consortium or "enterprise" blockchains where key participants are known.

Neither PoW nor PoS algorithms provide the properties needed for space system operations. All PoW algorithms are intentionally designed to be computationally or memory intensive. It is clearly undesirable for spacecraft to perform unnecessary computation, especially when those computations may not result in a successful transaction. PoS algorithms rely upon the blockchain having an economically meaningful cryptocurrency to be used for internal operations. We suggest the PoA family of algorithms have several properties appropriate for near-planetary and interplanetary scenarios, including agreement on a single chain of transactions and thus immediate finality of each block.

PoA protocols may be conveniently separated into those that guarantee immediate finality of created blocks, those that guarantee eventual finality and those that do not guarantee finality. A block is said to be final only if it has been added to the blockchain of an honest node and both its position and content may not be changed under any future circumstance (e.g. a network fork, or a rebalancing of the blockchain at a later time). A blockchain consensus protocol provides immediate finality only if any block is final as soon as it is added to the blockchain provided that there are no more faulty nodes than the maximum threshold allowed by the protocol. In other words, immediate finality guarantees that the blockchain cannot fork. A blockchain consensus protocol guarantees eventual finality if blocks become final only after they have been on the chain for a "sufficiently long" time. In the case that blocks added to the chain never become final, such as in the Clique PoA protocol,[32] then the consensus protocol is said not to guarantee finality.

Another property to be considered when choosing PoA protocols, and consensus protocols more generally, is whether they are tolerant to nodes that act maliciously, are faulty, or suffer communications failures. Such nodes are commonly called Byzantine.[33] The ability of a network to correctly operate in the presence of Byzantine nodes is called Byzantine fault tolerance (BFT).

Finally, the type of network that a consensus protocol is designed for must be considered. Networks can be divided into three types: synchronous, asynchronous and partially synchronous.[34] The maximum message delay in synchronous networks is bounded by a known amount of time, and unbounded in asynchronous networks. In partially synchronous networks, either the maximum message latency is finite but unknown or the network is guaranteed to reach a state of synchrony in a finite but unknown time after experiencing an initial state of asynchrony.

We argue that the properties of immediate finality, BFT and the ability to operate on partial synchronous networks are very compelling features for space system operations because they allow for immediate reads of the information known to be on the chain, provide a high level of security and allow for patchy communication which is usually the case for space communication. The Enterprise Ethereum Alliance is considering adoption of immediate finality and BFT in their client standard.[35]

PoA protocols that provide immediate finality and Byzantine fault tolerance include Honey Badger,[36] Tendermint,[37] DBFT (Democratic BFT),[38] and IBFT 2.0.[39] Table 2 summarizes the key properties of these protocols, and indicates our choice of IBFT 2.0 as most appropriate for the near-planetary domain due to its ability to deal with lost messages. A more complete evaluation of these and other PoA protocols is available.[14]

Table 2. Proof of Authority Consensus Algorithms with Immediate Finality and Byzantine Fault Tolerance

Algorithm	Message traffic to reach consensus	Average message size	Resilience to lost messages
Honey Badger	$O(n^2)$	O(b)	No
Tendermint	$O(n^2)$	O(b)	No
DBFT	$O(n^2)$	O(b)	No
IBFT 2.0	$O(n^2)$	O(b)	Yes

B. Interplanetary Economies

Deep space probes today typically act as edge nodes in a CFDP network. They check in directly with Earth as a routine part of their operations. These direct-to-Earth communications may one day yield to

communication with other regional centers, such as a Martian outpost or asteroid mining operations, as part of a more diffuse interplanetary network.

We must anticipate that multiple hub nodes will evolve at areas of exceptional deep space activity, such as Lunar, Mars and asteroid operations, and eventually settlements at each and economic encounters between them. Such networks are likely to be complicated as some nodes implement the ability to relay or even foster direct spacecraft-to-spacecraft communication, thus operating more as routers than as edge nodes.

Just as one can imagine a GNSS service around Mars or Earth's Moon, one can also imagine local blockchains that use those services to create economies on those bodies. A need would then naturally arise for swapping tokens or cryptocurrency between such near-planetary economies.

1. *Consensus Algorithm Selection for Interplanetary Space*

Two general approaches to an interplanetary blockchain are possible with current technologies: One could either develop a new blockchain specifically for interplanetary economic trades, or use so-called crosschain approaches to foster interaction between two planetary blockchains.

Ideal properties for an interplanetary blockchain would include an asynchronous consensus algorithm due to the difficulties inherent in creating a robust and continuous available interplanetary communications network. Byzantine fault tolerance would again be a desirable property due to the economic incentives present for theft. It is well known by the FLP theorem[40] that a deterministic system that can withstand at least one faulty node can guarantee both consistency and termination. There are, however, at least two extant indeterministic systems that could provide both asynchrony and BFT: Hedera Hashgraph[41] and Honey Badger.[36] A limitation of both algorithms is the number of nodes in the network must be known (and agreed to) by all participants, which seems like a reasonable practical restriction for an interplanetary blockchain.

Crosschain protocols may be used to transfer tokens or cryptocurrency between blockchains (e.g.[42,43]), or to enable crosschain smart contract dependencies to be satisfied in atomic ways ([44]). Future development of such crosschain mechanisms is anticipated to allow for safe effective transfers of assets between blockchains and generalized computation across blockchains. Both types of actions would be necessary to build an interplanetary economy.

C. Local Autonomy in Metaplanetary Space

Perhaps we will one day deploy enough spacecraft that some will meet in deep space. Two spacecraft of different manufacture from different countries or companies may benefit from local, autonomous economic transactions. For example, a spacecraft needing fuel might negotiate for that resource from an automated mining rig on an asteroid, comet, or moon. The spacecraft might trade cryptocurrency, sensor readings, items of exploratory or scientific value, etc, for the fuel it needs. Blockchains give us models upon which to envision and perhaps build such micro-economies.

Such spacecraft would, however, be quite unlikely to act as nodes participating in a remote blockchain. Even within our relatively small toroid of interest (that is, excluding operations near or on the Jovian or Saturnian moons or trojans), one-way message delays can exceed half an hour due to light speed limitations alone. Occultation, alignment, power restrictions or maintenance might cause that best-case scenario to be exceeded. Consensus formation, with its multiple message negotiations, could require days to reach agreement on a single transaction. BFT algorithms entail a relatively large amount of message traffic, which is an obvious problem for metaplanetary deployments. Surely some degree of local economic autonomy is to be preferred. It would be advantageous to complete spacecraft-to-spacecraft transactions locally, and simply report the result of such pre-approved transactions to Earth. This is the *lex mercatoria*-like concept as proposed by Israel[21] and previously described in general terms by some of us.[45]

1. *Consensus Algorithm Selection for Metaplanetary Space*

Developing common knowledge of time between two spacecraft meeting in deep space is anticipated to be a significant issue. GNSS timing signals are not currently available in deep space, and are challenged by non-realtime communications, and offline device clock-drift at endpoints. It may make the most sense for such spacecraft to negotiate a common time as part of a communications protocol upon meeting.

We would need to develop at least the following to implement a metaplanetary economic scenario between unknown spacecraft:

- a protocol for *lex mercatoria*-like machine-to-machine negotiation in deep space;
- a protocol for reporting *lex mercatoria*-like transactions to a blockchain of record.

Two current technology choices form a basis for progress. Firstly, perceived need for privacy in corporate transactions has led to the development of blockchain systems in which all participants are strongly identified via public key cryptography. Remote off-chain trades may be agreed between parties locally, and recorded to a blockchain of record if both parties report the same transaction. Secondly, a multiple signature scheme, such as BLS Threshold Signatures[46] may be used to construct a transaction record, thus ensuring neither party can cheat during reporting *post facto*. Up-front message traffic could therefore be minimized or even avoided.

IV. Conclusions

A few researchers have proposed and identified use cases for blockchains in space.

In this paper, we first revisited some these use cases through the lens of the theoretical framework proposed by Wüst and Gervais[12] to confirm that blockchain is the appropriate technical solution for them.

Second, we determined desirable blockchain properties to construct future in-space economies in three domains: Near-planetary, interplanetary and metaplanetary.

We identified two ways blockchains could be immediately deployed within cislunar space. One way is to modify the software of extant spacecraft to read from or propose writes to terrestrial blockchains. Another is to deploy specialist hardware capable of supporting full or partial blockchain node software. We proposed IBFT 2.0 as the consensus protocol most suited for low-transaction rate usage in near-planetary space.

We noted that access to precise timing signals and assumptions regarding communications reliability were critical components of most existing consensus protocols. The lack of either in deep space environments constituted key limiting factors in the interplanetary and metaplanetary scenarios.

Blockchain properties were suggested for each domain, with a focus on the selection of blockchain consensus algorithms. We showed that existing blockchain technologies are capable of immediate use within cislunar space. We then proposed two consensus algorithms (Hedera Hashgraph and Honey Badger) and two general approaches for building interplanetary economies. Finally, we suggested general steps necessary for development of technologies suitable for the formation of economies in deep space.

Reworded a bit the first half of the Conclusions to match the two research questions added to the introduction

V. Further Work

We would need to develop message-oriented crosschain protocols for interplanetary use suitable to the blockchains actually proposed for use, possibly using CFDP as a foundational protocol. The metaplanetary scenario would require the development of a protocol for *lex mercatoria*-like machine-to-machine negotiation in deep space and a protocol for reporting *lex mercatoria*-like transactions to a blockchain of record (presumably one located on a planet or moon). We aim to formally analyze all of those protocols for correctness, safety and liveness.

This paper represents our current best understanding of how to use distributed computing systems to build economies in space, but the field is moving extremely rapidly. We do not even have a common conception of what a blockchain is, much less a proper theoretical framework to evaluate the many different approaches to blockchains currently being built. The early blockchains sacrificed the concept of privacy for forms of anonymity. Perceived needs for increased privacy is driving researchers to create blockchains where only parties to a transaction may see the details. Thus, we expect to see distributed systems researchers continue to develop, evaluate and prove the correctness of more generalized blockchain-like systems based upon directed acyclic graph (DAG) data structures. Although none of the current transaction DAGs match all space requirements, any new DAG approaches should be considered to determine their applicability to space domains.

A similar problem is our poor understanding of consensus algorithms. Very few consensus algorithms have been formally proven to be correct. We thus require more formal proofs of consensus algorithms.

Space applications would also benefit from the development of new consensus algorithms with substantially reduced message-passing requirements. Moreover, new work on cross-chain protocols would be helpful in facilitating increased cooperation across vendors, technology choices and domains. Finally, emerging space law may enable (or limit) technology choices for in-space economies.

Acknowledgments

The authors gratefully acknowledge ConsenSys AG for supporting this research, especially its ConsenSys Space and PegaSys divisions.

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

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

[14]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.

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

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

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

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

[19]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.

[20]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.

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

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

[23]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.

[24]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.

[25]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.

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

[27]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.

[28]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.

[29]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.

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

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

[32]Szilágyi, P., "Clique PoA protocol and Rinkeby PoA testnet," Technical Report EIP 225, Ethereum Foundation, https://github.com/ethereum/EIPs/issues/225, March 2017.

[33]Lamport, L., Shostak, R., and Pease, M., "The Byzantine generals problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, Vol. 4, No. 3, 1982, pp. 382–401.

[34]Dwork, C., Lynch, N., and Stockmeyer, L., "Consensus in the presence of partial synchrony," *Journal of the ACM (JACM)*, Vol. 35, No. 2, 1988, pp. 288–323.

[35]"The Enterprise Enhanced BFT Specification," Tech. rep., Enteprise Ethereum Alliance, https://github.com/EntEthAlliance/enhanced-bft, 2019.

[36]Miller, A., Xia, Y., Croman, K., Shi, E., and Song, D., "The Honey Badger of BFT Protocols," *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, ACM Press, 2016, pp. 31–42.

[37]Buchman, E., Kwon, J., and Milosevic, Z., "The latest gossip on BFT consensus," *arXiv:1807.04938 [cs]*, Jul 2018, arXiv: 1807.04938.

[38]Crain, T., Gramoli, V., Larrea, M., and Raynal, M., "DBFT: Efficient Leaderless Byzantine Consensus and its Application to Blockchains," *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, IEEE, Nov 2018, pp. 1–8.

[39]Saltini, R. and Hyland-Wood, D., "IBFT 2.0: A Safe and Live Variation of the IBFT Blockchain Consensus Protocol for Eventually Synchronous Networks," Preprint arXiv:1909.10194, ConsenSys AG, https://arxiv.org/abs/1909.10194, September 2019.

[40]Fischer, M. J., Lynch, N. A., and Paterson, M. S., "Impossibility of distributed consensus with one faulty process." Technical report, Massachusetts Inst of Tech Cambridge lab for Computer Science, 1982.

[41]Baird, L., "The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance," Technical report, Hedera Hashgraph LLC, May 2016.

[42]Thomas, S. and Schwartz, E., "A protocol for interledger payments," Tech. rep., 2015.

[43]Sporny, M. and Longley, D., "The Web Ledger Protocol 1.0: A format and protocol for decentralized ledgers on the Web," Draft community group report, World Wide Web Consortium, https://w3c.github.io/web-ledger/, June 2019.

[44]Robinson, P., Hyland-Wood, D., Saltini, R., Johnson, S., and Brainard, J., "Atomic Crosschain Transactions for Ethereum Private Sidechains," *arXiv preprint arXiv:1904.12079*, 2019.

[45]Hyland-Wood, D., Lewicki, C., Hare, C., Robinson, P., and Henderson, B., "Lex Mercatoria Deal-making Between Small Spacecraft In The Outer Solar System," November 2019.

[46]Boldyreva, A., "Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme," *International Workshop on Public Key Cryptography*, Springer, 2003, pp. 31–46.