Enhancing Space Security Utilizing the Blockchain: Current Status and Future Directions

2022 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE) | 978-1-6654-7280-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/WISEE49342.2022.9926843

Anastasios N. Bikos
Department of Computer Engineering & Informatics
University of Patras
Patra 265 04, Achaia, Greece
mpikos@ceid.upatras.gr

Sathish A. P. Kumar
Department of Electrical Engg and Computer Science
Cleveland State University
Cleveland, OH, USA
s.kumar13@csuohio.edu

***Abstract*—The Blockchain concept is often mostly associated with Bitcoin and monetary transactions, however, the technology has enormous potential for several industries including the space sector. Cybersecurity enhancement plays a detrimental role in critical core operations inside the space functional flow: from the supply chain, satellite orbital tracking, and digital communications efficacy. The increasing adaption of connected highly advanced technologies exposes satellites, aeronautical drones, space vehicles, and ground stations to new types of cybersecurity risks. Hacking, cyber threats, as well as cyber-crimes in space are new trends. Such industrial ecosystems can benefit from Blockchain & distributed ledger technologies (DLT) that make it possible to intelligently decentralize governance. This work attempts to further demystify the linkage between space and the Blockchain, address the ledger's potential to provide added-on cybersecurity to the critical space core functionalities, via a ready-prototyped DLT/IOTA secure framework (SWIoTA), and finally, illuminate the roles of DLT ledger to secure networks of satellites orbits, as well as space tokenization concept.**

Keywords— Blockchain, Blockchain security, Internet-of-military things, Space, IOTA/DLT, IoT security, Intrusion-prevention system, Predictive IoT security

I. Introduction

The decentralized ledger, or Blockchain, the technology that originates from the cryptocurrencies, plays a detrimental role in offering businesses, corporations, and governments the opportunity to decentralize intermediate functionalities and perform peer-to-peer operations utilizing a distributed blockchain and cyber-secure fully logged transactions [13]. Blockchain has been 'psychologically' conceptualized by the public as a successful venture tool to promote business into economic prosperity, but even the space sector can see enormous advantages from its deployment [2] – [5]. The ledger for space systems might donate fascinating benefits by minimizing industrial intricacy across a plethora range of functional, business, operational, and security applications, including, but not limited to space venture financing and funding, smart contracts, supply chain solutions, Intellectual Property rights constraint management, beneficial networking space communications resource allocation, and most efficient space objects/resource manipulation. In addition to all the above, it is soon expected that several regulatory and compliance schemes that converge the Blockchain to the space business ecosystem will emerge including spectrum allocation and licensing, certification, assurance, and digital legislation [5].

Space exploration requires sophisticated hardware resources that operate in the most extreme environments, such as intelligent sensors, telemetry data, the most agile wireless communication algorithms, and the most accurate orbital planning software. These resources are meant to be characterized as cyber-critical in terms of security, privacy, and authenticity protection. Hereby is where Blockchain technology can provide premises to the previous challenges. The main technical renovation offered by the Distributed Ledger Technology (DLT) for space area is the removal of the "middle men", or the centralized trusted authorities, to fulfill the need for extra consensus and security [6] and [8]. As much as cryptocurrencies are already boosting their performance driving away from central banking authorities, the same could take place for space applications. Space sector entities should consider where they rely upon trusted central authority and where should they infer better cybersecurity, lower transaction costs, and greater efficacy. Although at a preliminary phase, the players in the space industry could understand several benefits of DLT implementation, such as *Transparency*, *Efficiency*, *Privacy and Access*, and *Novel Products & Services*. Especially the latter paradigm emphasizes that decentralizing conventional models and perceptions can lead to new business model creation. For instance, Etherisk (Switzerland) has prototyped a DLT-based re-assurance protocol to establish novel decentralized insurance services and products. Possibly, near-future satellite manufacturers could adopt such a technique and transit single-operator satellites into "multi-tenant" networks of satellites, by exploiting DLT and network standards to share resources in the same manner as ground stations do.

Industry 4.0 revolution is emerging as new evangelist of opportunities for great businesses and start-ups [12], like inside the space sector. Internet-of-Things (IoT) are attached everywhere and already perform significantly for the space challenge. IoT systems are typically known for their low resource constraint requirements, but if desired to co-deploy within the Blockchain context, as per the main scope of this work, a most common like consensus algorithm adapted in Space/IoT should possess high computational complication in order to block malicious cyber activities. There is, undoubtedly, a real mathematical confrontation to instantiate a DLT/IoT ready

Proof of Work (PoW) and/or Proof of Stake (PoS) consensus agreement protocol that is both computationally hard to break and resource-efficient. However, we could underline at this point there is an enormous research effort in this direction to improve the cryptographic elements and operations for popular DLT protocols for IoT devices, such as the *Curl* function of IOTA [8] and [12].

Illustratively, it is of paramount significance to instantiate confidentiality, security protection, and integrity inside such model interaction (Blockchain/IoT for space). Another parallel direction insight is the leverage of Artificial Intelligence for ensuring the cybersecurity awareness of critical space operations via utilizing Machine-learning assisted Intrusion Preventive Systems for IoT. Our pre-built cybersecurity framework (SWIoTA) holds advanced Machine & Deep Learning algorithms that can make the DLT/IoT network pre-sense any type of security attack and provide itself resilience and fast recovery. Our system can be scalable and transactive for the DLT/Space scenario(s), and it can be integrated with existing security tools and implemented in a fully decentralized fashion [6] and [7].

The conceptual analysis of space assets (e.g., satellites, orbital metadata, astronauts, space crafts, and space hardware equipment) can be *tokenized*. The process of space object tokenization into digital assets, or tokens, that can be exploited, transactioned, and processed by the blockchain system is of significant benefit to integrating DLT with the space business context. Tokenizing such space elements would help in the direction of enabling space stakeholders to track and monitor satellite orbital behavior by creating *smart contracts* logged into the Blockchain network in a fully authenticated and transparent manner. With that technical means, it would be possible to convert all the orbital assets that belong to space companies or international space agencies to transceiver digital tokens that can add to new smart contracts and produce *space decision tokens* as newly added blocks to the public Blockchain [4] and [5]. Mainly, conceptualizing the space exploration elements as Blockchain elements gives enormous technological advancement to manage and secure satellite swarm connections using the ledger. In a such promising scenario, implementing swarms of multi-sensor satellite systems to perform earth and space exploration demands the establishment of decentralized platforms for securing space communications patterns effectively. For this reason, cybersecurity resilience is detrimental in terms of importance for these deployments. By investing in predictive analytics IoT platforms and improving the consensus and cryptographic modes of the DLT/IoT protocols [7] the Blockchain will empower space agencies to detect any security attack on a satellite system (seen as a set of Blockchain nodes) that aims to hack the satellite software system.

The rest of the manuscript is structured as follows. Section II concentrates on the applicability benefits of DLT/IoT for the space industry while highlighting important considerations, challenges, and opportunities. Security and consensus Trust are also clearly mentioned here. Section III addresses the opportunities and challenges for DLT/Space integration. Section IV depicts the most typical existing secure frameworks for such integration of Blockchain-Space, together with some security attack references. Finally, section V concludes the current work.

II. Blockchain in the Space Sector

Blockchain is considered a disruptive technology that will cut ties of existing centralized and trusted authorities with a new concept model for decentralized authorization with additional communications speed, cost, and security benefits. Furthermore, the aforementioned traits of the blockchain technology such as cybersecurity, trust, decentralized nature, time stamping capabilities of transactions, and transparency attain it as an elemental technology for administering and cyber-securing space communications, either among satellites or satellites as well as ground stations, due to the fact it cannot be attacked or forged from a central control access point. These main characteristics qualify the blockchain as a leading technology candidate for offering great benefits to the space industry like the following [12]:

- *Leveraging the satellite value chain:* Blockchain, typically a smart contract, can be utilized to establish robustness, efficiency, and trust in the satellite value chain. For instance, applications that are based on smart contracts can be deployed to launch and manage satellites, as well as tele-monitor space operations. Furthermore, satellites can be treated as generators of space transactional data for block upgrades, as well as integrity and origin verification.
- *Enabling the cloud in space:* By enhancing mutually the blockchain and Artificial Intelligence (AI) can lead to cloud transformation and scalability in space. Blockchain over satellite networks eliminates the reliance on terrestrial networks for storage processing and broadcasting, thus neglecting exploits for data breach and distortion. This can be perfected based on space data cloud computation.
- *Ability to track the satellite supply chain:* Blockchain technology by nature is eligible to re-assure and verify data during each stage of development, from procurement to testing and design, and launch. Blockchain can also be used to observe the satellite's motion, share several space data, as well as enforce update rules that require the stakeholder's team consensus.
- *Open-source satellite design:* Space chains can be deployed to provide end-users with blockchain-based open-source satellite networks to directly gain access to satellite services. The Singapore-based Space Chain has recently commenced an effort to construct the world's premier open-source DLT-based satellite network.

Figure 1 is a most typical example paradigm of how a decentralized ledger will leverage inter/intra satellite communications and collaboration networking. Specifically, space digital tokenization, in terms of sensing the orbital debris between a satellite, the modelling of transactions between a Peer2Peer satellite network, and the most cost-effective manipulation of parts and materials of space vehicles can be robustly substantiated with the formulation of space transactions

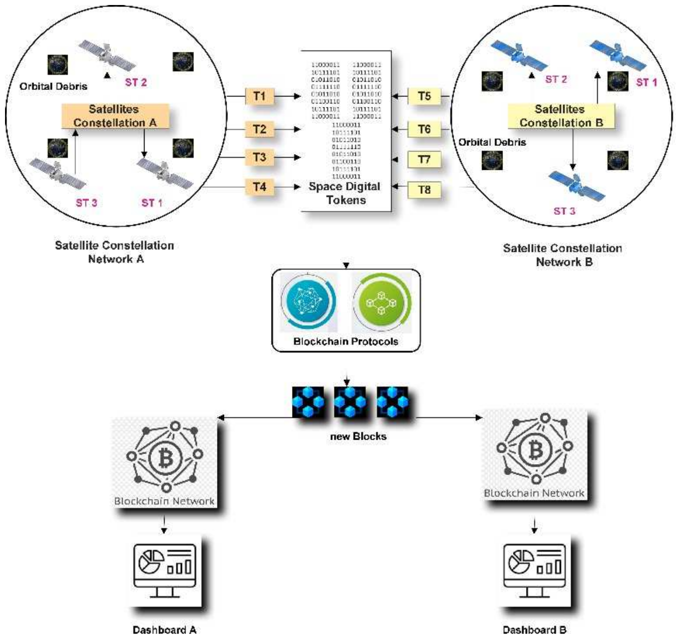

Fig. 1. Blockchain concept for space vehicles: Space digital tokenization

and most typical blockchain protocols (DLT). This space digital token can define such a transaction, whereas the blockchain protocol(s) is mainly responsible for verifying and authenticating the novel space transactions in order to aggregate a new valid block to the original blockchain. In that intelligent terminology, all space stakeholders are then capable to access and manipulate the novel added blocks through a connected dashboard to the space network constellation via the blockchain platform.

Moreover, blockchain is expected to become a business game changer for the space industry, driving the generation of the satellite-as-a-service concept. We can spotlight many drivers and benefits of the various promising DLT space sector applications [4] and [5].

1) Smart Contracts: Smart contracts are mainly self-executing contracts that digitally authenticate the consensus negotiation or validity performance of a Blockchain contract. In the first place, the blockchain-smart contract has to construct, define and specify the uniqueness and validity of the newly created blocks by using a hash code as shown in Fig 2.

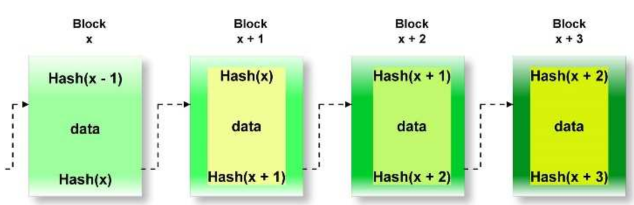

Fig. 2. Example of Blockchain concept: Blocks are linked via hash-pointer to rest blocks [6].

For example, the Proof of Work (PoW) consensus defines that the hash code of a valid block is estimated as in Equation 1, and the legitimate block's hash code must start with a predefined number of adjacent zeros.

$$BCH = Hash(TD + P + Nonce) \quad (1)$$

Where 'BCH' is the Block Hash Code, 'TD' keeps the Transaction Data, 'P' holds the hash code of the previous block inside the chain, and 'Nonce' (Number only once) is a random number that can be utilized only one time for outputting the corresponding BHC. The smart contracts rely on IF / THEN statements that automatically initiate specific events when certain preliminary conditions are being satisfied. Provided the high scalability constraints of space participants, from launch to orbit, and the number of scientists/stakeholders who must observe and administer their company assets, it is reasonable to consider that the space sector defines an enormous momentum to deploy smart contracts.

The European Space Agency (ESA) has recently accomplished a promising framework, named Space 4.0, to mainly make efforts to efficiently define the complicated and automated interactions between political entities, governments, the public/private sector, and business parties. ESA concentrates on 'administrative' DLT/Space applications for robust payments, supplier contracts, procurement, and full automation. ESA incorporates the vision of a sustainable space sector ecosystem closely attached to the economic growth of society and argues that DLT could enhance such a prospect.

2) Supply Chain Applications: Integrating DLT inside the supply chain network and procurement procedures of the space systems project intriguing benefits. For instance, a fully functional audit trail, where everything is logged, and a single source of trust. In terms of security, the supply chain data is being encrypted and confidentiality secured thus making it trivial to modify. Additionally, digital Blockchain transactions can easily recorded back, or audited, thus various risks or hazards can be counterfeited.

The encompassing of DLT inside the Space industry operations can upgrade the company's tracking system because it shall include all supply chain participants: raw hardware materials, peripherals, components, sub-systems, parts, and main functional blocks. For example, if a malfunctioning or defective component is being traced on a satellite bus, even after several months or years of real-life deployment in space, the preliminary contractor of the component could leverage the DLT record system to backward retrieve the part and source upstream. Other supply chain manufacturers could receive alert indications on whether they have utilized this part. Modern aeronautics, aviation, and space participants can share technical information about space system components that include:

- Detection and isolation of cyber threats.
- Accurate management of inventory levels.
- Timely correspondence to product recalls.
- Malfunction detection of parts and components.

One important relevant subject is *Off-the-Shelf (OTS) Quality Control.* Currently, the space industry trend is to migrate towards shorter duration (< 5 years missions) as well as production of a mass number of satellites faster in support of large Low Earth Orbit (LEO) constellations and smaller satellite swarm networks. Manufacturers of such lower cost and greater flexibility satellite systems are spotting for off-the-shelf (OTS) parts to produce such great numbers of satellite missions. In such competitive and strenuous environments, DLT applications for supply chain risk management will become not only detrimental but also a game changer within the commercial space area.

3) Intellectual Property Rights (IPR) Management for Copyrights assurance, Design and Data Licencing: Intellectual Property transfer cannot be easily proven (e.g. assignor and assignee, IP watermark, authorship, transfer date), if the enforcement action is necessary. DLT could immediately solve these challenges by adding an immutable record that tracks the authorship, from the original creator to the complete chain of ownership. Many national and international patent offices could adhere to recognizing DLT as a form of undoubtable evidence for property rights. Finally, the Blockchain could be adapted to "tokenize" digital rights and rights groups. Token-as-a-License (TaaL) refers to the concept of buying and storing digital tokens in a digital wallet with an encoded software license. Thus, TaaL and smart contracts could remove middleware entities from distributing satellite scientific data, like geolocation images, metadata, observations, and analytics. In this manner, these tokens by representing licenses for satellite data usage could work like a compact smart contract [23].

4) Networking and Space Community Resourcing: DLT/IoT manages to provide enormous potential benefits for the space sector to approximate the best effort in space-based data coordination among versatile missions, technologies, and sensors. NASA and commercial space companies are investigating how to combine Artificial Intelligence (AI), DLT, IoT, and communication sensor techniques to administer space missions and infrastructure. Some nice examples are projected below:

- NASA has launched a research project, named the "Resilient Networking and Computing Paradigm", led by Dr. Jin Wei-Kocsis of the University of Akron's Department of Electrical and Computer Engineering. According to the project manager, its main goal asset is to *"achieve scalable decentralized cognitive networks in deep space"*. This research attempt could perhaps lead one day to fully decentralized processing among NASA's space networking nodes.
- NASA – "SensorWeb". NASA is actively interested in adapting smart contracts on the Ethereum blockchain inside its core operations. The main advantage of this attempt is to promote space interoperability among a versatile set of satellite sensors with the help of software and the Internet.
- Network of Blockchain Nodes in Space – "SpaceChain". SpaceChain has been self-described as a "decentralized" space agency able to work with multiple partners. SpaceChain has installed smart hardware on satellites with SpaceChain OS. The first satellite Blockchain node was set into orbit on February 2, 2018. The SpaceChain network enables users to deploy different types of space-based applications on an atomic satellite resource allowing multi-tenancy and faster code execution.
- Open Source Networking Standard for Ground to Space Communications – "EtherSat". EtherSat, Inc. (San Jose, CA) has been investing in an open source standard development to make ground-to-space communications Blockchain aware and more efficient, thus saving capital investment, OPEX, and deployment time.

DLT as much as the Internet will require time to build and take hold. While there exist many drivers that will inevitably push the space industry in the direction of non-centralized authorities, broader technology adoption will require collaboration, involvement, legal acceptance, and standards-setting [5].

III. Blockchain Applicability in Space Information Network Security

A. Scope

Objectively, space information networks contain numerous nodes. These could be segmented into versatile mission areas and some of them could even become clustered. For instance, some satellites are GEO satellites, whereas others orbit in LEO and MEO circles around the globe. Thus, there exist several user data links, inter-satellite links, inner-orbital links, and meta-communication information. The parties inside this network require authenticated-based encryption using keys to resist several attack attempts like Man-in-the-middle. Space nodes can deploy public-key encryption to instantiate identities on the ledger, and only those nodes with the private key holding can decrypt data encrypted with the asymmetric key. Since blockchain timestamps and hash values are being used to connect blocks, when public-key cryptography is deployed, any illegal modifications to the blockchain would be impossible to realize [14] - [15].

Almost every space equipment relies on self-survivability or means of protective self-reconfigurability (self-healing) to repair malfunctioning components while in orbit. Blockchain is based on smart contracts that are self-executing software programs. The benefits of smart contracts during such scenarios would be on the one hand cybersecurity resilience against GPS signal spoofing attacks [11], tampering attacks, while at the self-repair phase, and increased scalable administrative coordination of satellites that need to be fixed, by neighboring ones [16].

The level of achievable decentralization in the space equipment while in orbit is astonishing. DLT is based on Peer-to-Peer networks, and it can easily formulate clusters of satellites based on Spatio-temporal correlation. In this manner, not only

TABLE 1: Summary of Blockchain Challenges and Solutions for SAG-IoT Devices & Applications

Blockchain challenge	In detail	Solution	Key traits
Limited resources	Resource-constrained SAG-IoT devices cannot easily support blockchain maintenance	IoT-friendly consensus mechanisms	Leverage node collaboration, and hybrid blockchain to design ad-hoc consensus protocols
		Off-chain mechanisms	Transfer processing, data, and transactions to off-chain repositories, third parties, and channels
Storage	A trade-off between transaction throughput and cybersecurity trust	Incentives	They are typical robust momentum mechanisms for effective node collaboration in resource sharing and transaction relaying
		Sharding	Parallel split of blockchains into multiple shards and each shard processes transactions individually
Scalability	Expanded SAG-IoT applications have more overhead	Sidechain	Utilization of sidechains attached to the main chain via bidirectional connection
		Editable blockchain	Using the pruning technique to increase available blockchain capacity, and mitigate storage burden without destroying data integrity
Cybersecurity threats	Blockchain-leveraged SAG-IoT devices & applications contain large threat vectors	AI-powered secure blockchain	Utilization of advanced and explainable Artificial Intelligence to create robust intrusion detection and prevention systems
Privacy concerns	The processing and storage of smart contracts in public blockchains are transparent	Privacy-preserving blockchain	Protect smart contracts and transactions via efficient cryptographic procedures and trust platforms
Legal concerns	The public blockchain with anonymous access addresses eliminates the centralized regulation authorities	Regulated blockchain	Avoid unlawful transactions and behaviors in blockchain platforms
Interoperability	A SAG-IoT ecosystem with a plethora of heterogenous consensus, blockchain, and communication exchange protocols	Cross-chain technique	Enable cross-chaining among heterogenous platforms with relay chain, hash-locking, etc.
Latency	The need to reduce space communication latency in blockchain-based SAG-IoT	[25] 2020	A blockchain reputation and routing framework protocol are proposed and evaluated

cyber-physical attacks against those space components can be avoided or minimized, but also lower operational and deployment costs can be guaranteed.

B. Challenges

Storage. Technically, the blockchain requires every space node to be stored. However, most of the space components possess limited storage capabilities. For this reason, quite novel research efforts are underway to find the trade-off between efficient storage and performance for advanced satellite equipment [18]. Some of these attempts rely on algorithms that consider the topological structure of the space information network from the ground segment to the orbital constellation [13].

Consensus. Proof-of-Work, Proof-of-Stake, Delegated Proof of Stake and Practical Byzantine Fault Tolerance are the most common DLT-based consensus algorithms which can decide which nodes possess the administrative rights to create new blocks. For instance, Practical Byzantine Fault Tolerance could neglect additional computational power, however, if (N-1)/3 nodes are forged, a ledger would not be operational. It is therefore a necessity to apply some sort of equilibrium between security ability and computational skills for the consensus protocols to become applicable for space information networks [13].

Transmission Delay. Current space satellite networks operate with GEO, MEO, and LEO satellites. Data transmission delay between GEO satellites and end-users reaches 250 ms–280 ms, MEO satellites and users demand 100 ms, whereas LEO satellites and users need 10 ms–40 ms. The most apparent problem hereby is because the blockchain needs 10 minutes to create a new block, the practically visible time between two LEO satellites is probably less than 10 mins, which can disrupt the whole ledger procedure [13].

IV. Blockchain Solutions For Space Security

We could easily unify the DLT/Space integration applicability paradigm with the space-air-ground integrated networks (SAGINs) as a promising prospect for large-scale coverage and network provisioning of space mobile, UAV, and IoT devices (SAG-IoT). SAGINs comprise three network components: i.e., communication satellites; aerial communications devices such as unmanned aerial vehicles (UAVs), and terrestrial communication networks from the ground stations. The benefits of such technological internetworking solutions are enormous for the space sector, but also Security, Privacy, and Trust issues seem to be more critical than ever before. Blockchain-based SAG-IoT can indeed provide extra decentralization features, increased trust, and flexible resilience due to the high transactional level of operations, but trade-offs between computational and security performance still do exist due to the limited resource constraints of the IoT nature [6]. Per that direction, Table I tries to illustrate the challenges as well as sophisticated solutions for such an aim.

The attack surface in SAGINs is huge: We could name a few like *untrusted data transmission, uncoordinated data delivery, Hijacking of mining data, sensor data tampering, GPS signal spoofing* [11], *Transaction forgery, Double-spending and DDoS attacks, Privacy and Information leakage, Repudiation, and untrusted nodes*. The blockchain operations for Space require strong Cybersecurity measures. As a strong effort to mitigate the security and efficacy issues of smart contracts there has emerged a huge research flow direction towards building secure frameworks, intelligent proactive IoT systems embedded with state-of-the-art Artificial Intelligence and predictive analytics. As shown in Table II, we tabulate some most explicit secure such intelligent implementations that are highly compatible with blockchain/space cohabitation.

TABLE II: Summary of Blockchain Security Solutions for Trustworthy Space Data

Reference	Consensus Protocol	Advantages	Disadvantages	Implementation Platform
[21]	PoW (**no** smart contracts)	Trusted Data Distribution for Satellites	Eligible for DDoS attacks	Ethereum
[22]	Hybrid (**no** smart contracts)	Optimal Resource Management Strategies for Peers and BSs	Security Issues of Compromised Nodes	N/A
[23]	DAG (**no** smart contracts)	Improved Verification Efficiency of Energy Micro-transactions	Blockchain Security Synchronization due to High UAV Mobility	N/A
[24]	PoW (smart contracts)	Defense against Majority Attacks, Eclipse Attacks, and Terminal Device Tampering	Reliance on Network Infrastructures for Blockchain Maintenance	Ethereum
[6], [7]*	DAG-PoW/PoS (smart contracts)	ADS, IDS** Machine-Learning Assisted Security Technology Scalability Energy Efficiency Accuracy***	Broader Threat Detection Landscape under Future work	IoTA/DLT

*Our Work
** Is Intrusion Detection System (IDS), Anomaly Detection System (ADS), Intrusion Protection System (IPS)
*** our IOTA intrusion detection system achieves an accuracy level of 98% (ACC), with an F-measure of 88%.

V. Conclusion

The innovative concept of tokenizing space elements as digital tokens is one of the numerous beneficial properties provided by the decentralization nature, flexibility, and high trust nature of the DLT. Moreover, Blockchain algorithms based on smart contracts can be used to track all space communications transactions in a robust, efficient, and transparent manner. In this work, we presented survey-based research for robust and newly conceptual blockchain-enabled secure frameworks that can ensure information security for space applications. We discussed several security & privacy issues from the integration of Space industry and Blockchain and proved the applicability of our novel cybersecurity framework for the space context scenarios. Finally, we concluded our work with tabulated outputs from our research.

.-

References

[1] Popov, S.Y. (2015). The Tangle. [Online]. Available: https://iota.org/

[2] Banerjee, M., Lee, J., & Choo, K. (2018). A blockchain future for internet of things security: a position paper. Digit. Commun. Networks, 4, 149-160.

[3] Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M., & Choo, K. (2020). A systematic literature review of blockchain cyber security. Digit. Commun. Networks, 6, 147-156.

[4] Torky, M., Gaber, T., Egypt, A.E., Cairo, & Egypt. (2020). Blockchain in Space Industry: Challenges and Solutions. arXiv: Signal Processing.

[5] Karen L. Jones, Blockchain: Building Consensus and Trust across the Space Sector, 35th Space Symposium, Technical Track, Colorado Springs, Colorado, United States of America, Presented on April 8, 2019

[6] Bikos, A.N., & Kumar, S. (2022). Securing Digital Ledger Technologies-Enabled IoT Devices: Taxonomy, Challenges, and Solutions. IEEE Access, 10, 46238-46254.

[7] A. N. Bikos and S. Kumar, ``Reinforcement learning-based anomaly detection for Internet of Things distributed ledger technology," in Proc. IEEE Symp. Comput. Commun. (ISCC), Athens, Greece, Sep. 2021, pp. 1-7.

[8] S. A.Kumar, T.Vealey, and H. Srivastava, ``Security in Internet of Things: Challenges, solutions and future directions," in Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS), Koloa, HI, USA, Jan. 2016, pp. 5772-5781, doi: 10.1109/HICSS.2016.714.

[9] S. Nakamoto, ``Bitcoin: A peer-to-peer electronic cash system," whitepaper, 2009. [Online]. Available: http://www.bitcoin.org/

[10] B. Baek, ``IOTA: A cryptographic perspective," Harvard Univ., Cambridge, MA, USA, Tech. Rep., 2019

[11] Charalambos Konstantinou, Marios Sazos, Ahmed S. Musleh, Anastasis Keliris, Ahmed Al-Durra, Michail Maniatakos, GPS Spoofing Effect on Phase Angle Monitoring and Control in an RTDS-based Hardware-In-The-Loop Environment, IET Cyber-Physical Systems: Theory & Applications, 8 pp., 2017

[12] Hassanien, A.E., Torky, M., Goda, E., Snášel, V., & Gaber, T. (2021). Proof of Space Transactions: A Novel Blockchain Protocol for Secure Authentication of Satellite Transactions.

[13] Cheng, S., Gao, Y., Li, X., Du, Y., Du, Y., & Hu, S. (2018). Blockchain Application in Space Information Network Security. SINC.

[14] Pokhrel, S.R. (2021). Blockchain Brings Trust to Collaborative Drones and LEO Satellites: An Intelligent Decentralized Learning in the Space. IEEE Sensors Journal, 21, 25331-25339.

[15] Guo, Z., Zhang, J., Gao, Z., Wang, A., Pan, C., & Li, X. (2021). Blockchain-Based Multi-party Cooperation and Resource-Sharing Scheme for Space-Air-Ground Integrated Networks. 2021 IEEE 21st International Conference on Communication Technology (ICCT), 947-952.

[16] Bao, Z., Luo, M., Wang, H., Choo, K.R., & He, D. (2021). Blockchain-Based Secure Communication for Space Information Networks. IEEE Network, 35, 50-57.

[17] De Filippi, P., & Leiter, A. (2021). Blockchain in Outer Space. AJIL Unbound, 115, 413-418. doi:10.1017/aju.2021.63

[18] Ibrahim, H., Shouman, M.A., El-Fishawy, N.A., & Ahmed, A. (2021). Literature Review of Blockchain Technology in Space Industry: Challenges and Applications. 2021 International Conference on Electronic Engineering (ICEEM), 1-8.

[19] Reed, H., Dailey, N.D., Carden, R.D., & Bryson, D.E. (2020). Blockchain Enabled Space Traffic Awareness (BESTA): Discovery of Anomalous Behavior Supporting Automated Space Traffic Management.

[20] Wang, Y., Su, Z., Ni, J., Zhang, N., & Shen, X.(. (2022). Blockchain-Empowered Space-Air-Ground Integrated Networks: Opportunities, Challenges, and Solutions. IEEE Communications Surveys & Tutorials, 24, 160-209.

[21] M. J. Molesky, E. A. Cameron, J. Jones, M. Esposito, L. Cohen, and C. Beauregard, "Blockchain network for space object location gathering," in Proc. IEEE 9th Annu. Inf. Technol. Electron. Mobile Commun. Conf. (IEMCON), 2018, pp. 1226–1232.

[22] A. Asheralieva and D. Niyato, "Distributed dynamic resource management and pricing in the IoT systems with blockchain-as-a-service and UAV-enabled mobile edge computing," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1974–1993, Mar. 2020.

[23] L. Jiang, B. Chen, S. Xie, S. Maharjan, and Y. Zhang, "Incentivizing resource cooperation for blockchain empowered wireless power transfer in UAV networks," IEEE Trans. Veh. Technol., vol. 69, no. 12, pp. 15828–15841, Dec. 2020.

[24] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning," IEEE Trans. Ind. Informat., vol. 15, no. 6, pp. 3516–3526, Jun. 2019.

[25] L. Clark, , Y. C. Tung, M. Clark, and L. Zapanta, "A Blockchain-based Reputation System for Small Satellite Relay Networks.," in IEEE Aerospace Conference (pp. 1-8). IEEE. 2020 .