Azerbaijan Journal of High Performance Computing, Vol 5, Issue 2, 2022, pp. 318-325
https://doi.org/10.32010/26166127.2022.5.2.318.325

AzJHPC
Azerbaijan Journal of High Performance Computing

*Correspondence: Andrei Gurtov, Linköping University, Sweden, Linköping, andrei.gurtov@liu.se

Registration of Drones Through Blockchains

Ayla Babazade[1], Andrei Gurtov[2]

[1]*Azerbaijan State Oil and İndustry University, Baku, Azerbaijan, aylababazadeh2000@gmail.com*
[2]*Linköping University, Linköping, Sweden, andrei.gurtov@liu.se*

Abstract

This paper explores the potential use of blockchain technology to register drones. Using blockchain, a unique and tamper-proof identifier can be assigned to each drone, enabling real-time tracking, secure data exchange, and improved compliance with regulations and laws. This paper argues that integrating blockchain into drone registration can increase security, transparency, and efficiency.

Keyword: Unmanned Aircraft, Internet of Things, Drone Operations, Blockchain, Global Navigation Satellite System.

1. Introduction

Drones are autonomous flying robots that are now an integral part of the Internet of Things (IoT) ecosystem. The success that enables drones to support IoT communcations is primarily the success that cellular networks have brought to IoT, which has been a significant development path. This success is also driven by innovations in image processing, the enormous power of data centers, and the development of predictive algorithms for efficient and autonomous decision-making (Hashem, Y., Zildzic, E., & Gurtov, A., 2021, November). All these technologies, integrated into unmanned IoT networks, have taken significant steps in transitioning from various wireless technologies (WiFi, LoRa, Sigfox, ZigBee, etc.) to a globally connected infrastructure with IoT devices communicating and sharing information.

Drones are flown to enhance the life experience in many applications such as agriculture, rescue operations, pipeline inspection, filming, and delivery of goods and medicine (Alladi, T., Chamola, V., Sahu, N., & Guizani, M., 2020). However, due to their increasing popularity, new challenges have arisen regarding managing drone flight locations, reducing collisions, and protecting UAs from cyberattacks (Lin, C., He, D., Kumar, N., Choo, K. K. R., Vinel, A., & Huang, X., 2018). Legacy IoT architectures have many advantages in monitoring IoT networks, primarily through cloud server mediation that facilitates drone exchange between different service providers (Abdo, J. B.,Demerjian,J.,Chaouchi,H.,Barbar,K.,&Pujolle,G.,2013,December). However, when moving to decentralization, rates can be managed autonomously by replacing the broker with a blockchain (Abdo, J. B., & Zeadally, S.2020). The latter has emerged as a revolutionary technology to reduce these problems and provide transparency, trust, security, and privacy (Lin, J., Shen, Z., Miao, C., & Liu, S., 2017).

Blockchain is a digital ledger with an immutable time stamp that is distributed and managed by many computers and allows digital information to be distributed, but not changed (Dragonchain, July 14, 2019). Blockchain technology makes it easy to introduce trust to a group or network. Thus, there are two mandatory prerequisites for the application of blockchain: a business network - which can be local, national, or international (a store, an airline ticket agency, a car rental company, a real estate broker) and untrusted or anonymous participants (buyers, sellers, agents, managers, producers, consumers, suppliers). A familiar example of these two premises involves a man who wants to buy a used car from a stranger. Experts predict that the blockchain market will grow at an average annual growth rate of about 83 percent by 2022 (Phoneweek, 2018). The Volpe Center of the US DOT has previously reviewed the ideas behind blockchains and detailed their application in the transportation industry (Merrefield, C., 2018).

2. How Blockchain Could Support UAS Operations

Blockchain technology is expected to create a framework that stakeholders in the commercial drone industry can use as it can provide security and identity management and a supporting role in aircraft traffic control, UA conflict management, and flight permission (Deep Aero Drones, May 10, 2018). Blockchain has already been used to solve some of the trust and integrity issues of UA. Flight data recorders (also known as “black boxes”) can provide information that can help investigators learn what a UA was doing before an incident. A blockchain-based flight recorder will do this in real-time, allowing law enforcement to act proactively rather than reactively. One company has proposed a blockchain-based “black box” drone system that would allow industry regulators to track and analyze drone flight data, insurance companies to insure drones based on reliable third-party data, and pilots to ensure regulatory compliance (UAS Vision, March 11, 2019). With NASA and the FAA making an industrywide effort to standardize unmanned traffic management, in 2018, Boeing announced the development of a traffic management system for all drones using artificial intelligence (AI) and blockchain technology (Coinidol, July 18, 2018). The system will effectively track all drones flying along the selected transport corridors. It will also incorporate a standardized software interface to support industrial control, package delivery, and other important commercial applications. Google’s Project Wing has tested its own UA air traffic control (ATC) platform, which plans to use the company’s cloud computing infrastructure to process large numbers of expected flight paths and correct them in a fraction of a second (Lumb, D., June 7, 2017).

NASA has proposed a blockchain-based framework for the FAA’s Automatic Dependent Surveillance (ADS-B) system to ensure aircraft privacy by preventing fraud, denial of service, and other risk factors (Reisman, R., 2019). Walmart has the plan to create a network of autonomous robots controlled and authenticated through a blockchain network (CoinWire, September 5, 2018). Their patent application for a blockchain-based authentication system allows mobile autonomous electronic devices to identify and communicate with each other to minimize the time that components of the delivery process must be trusted (Campbell, R., June 1, 2017; Wilmoth, J., August 30, 2018). Walmart's proposal documents a system in which multiple robots deliver a package along various links in the supply chain using wireless signals to communicate and authenticate each other (Lillian, B., May 18, 2017).

IBM has received a patent for using blockchain to secure a fleet of drones (Hashem, Y., Zildzic, E., & Gurtov, A., 2021, November). Their blockchain will store data about UA flights, allowing air traffic controllers to control an ever-increasing number of drones. The chain will chronicle the path of each UA overtime. When the operation is performed, the corresponding UA parameters will be sent to one or more computing nodes in the system for verification and the creation of a new block. Once a new block is calculated, it will be added to the interested party's UA blockchain. Among many other advantages, blockchain infrastructure helps identify non-compliant UA, as such activities are recorded in a secure ledger. A permissioned blockchain may contain a variable block time that changes in response to external triggers. For example, suppose a recreational drone flies too close to a restricted flight area. In that case, it can activate a risk flag and increase network time to provide airspace controllers with additional information about the UA and, if applicable, its operator (Wilmoth, J., September 20, 2018). Machine learning for drone navigation and data analysis is also driving numerous developments.

Along with artificial intelligence, blockchain is seen as a way to make drones safer and easier to regulate and track (Deoras, S., April 20, 2018). Blockchain is also being used to address drone cyber security issues such as flying over people and property, interfering with commercial aircraft, and addressing privacy issues (Chantz, H., 2016). Blockchain can provide security by providing confidential and secure communication (Deoras, S., April 20, 2018). Encrypted blockchain identifiers allow the flexibility to define trust models between devices. For example, a blockchain-based repository for package delivery can record transaction data such as time, location, resources, and delivery date and make the data available to authorized users (Deoras, S., April 20, 2018).

3. Processing of Data

3.1. Registering a New Account

In order to connect to the network, any device (such as UA) must first register with the genesis operation. Based on the MAC address, the most recent timestamp, and a random salt hash value, each device generates its private key before registering. Preloaded policies for each host also define what actions to take when messages are received (Ahamed Ahanger, T., Aldaej, A., Atiquzzaman, M., Ullah, I., & Yousufudin, M ., 2022).

3.2. Data Hashing

Each node stores all other nodes' public keys, private keys, and subsequent blocks in sequence. Before data exchange, procedures such as hash function and digital signature must be performed on all devices. Compared to other lightweight hash functions (such as Quark, PHOTON, and SPONGENT), Keccak is a high-performance hash function in both code size and cycle count. Thanks to the extensive use of hash functions such as block hash, previous hash, reputation root, transaction root, and message digest for each transaction, the 160-bit output is reduced to 80 bits to save memory.

3.3. Verification of the Data

If the two digests match, the data's integrity and the transaction's consistency in the peer-to-peer network are verified. Regardless of whether the request is genuine, the list of policies is checked to see if it meets all of its requirements. Individual UA reputation values decrease when a transaction is rejected due to data integrity inaccuracies or if it violates a set of policies communicated to other UAs through a report transaction issued by recipients of rejected transactions. As a result, the reputation of the person who correctly reports hostile behavior increases. For example, each reporting transaction will trigger a voting procedure where each node votes on the result of its verification and the reputation value of the suspected UA in a distributed voting mechanism.

3.4. Estimation of Reputation Measure

A distributed reputation evaluation mechanism is adopted to confirm the validity of the received blocks, which reduces the cost of block verification. Merkle Patricia Trie stores the reputation value of all nodes in the proposed architecture. Each UA group is led by a master UA and supported by many conventional UAs. Using the reputation score, the system tracks the reliability of each node. Unless the UAs are programmed to transmit many spam or malicious messages, it will be difficult for them to take over the system. To calculate the reputation of a connected node, a node considers the quality of service provided by its peers.

3.5. Distributed Voting System

The ID-based vote distribution method has several functions. A distributed consensus protocol similar to DPoS is proposed to agree on the received data. As a result, the committee that created the block is elected by voting. The reporting operation is known to be used to alert authorities of suspicious UA activity. However, a hacked UA can disrupt system availability by inventing reporting operations to generate appropriate UAs. As a result, the voting mechanism must evaluate the legitimacy of each reporting transaction. In addition, the voting procedure is used to resolve cases where there are many disagreements. Polling operations are used to compare the GNSS data of the UA with the GNSS data of other UAs in the no-fly zone, for example, when a UA suddenly finds itself in or near a no-fly zone without any foresight. If it does not match, a GNSS spoofing attack is very likely, and the UA should alert its neighbors so they can take measures to mitigate the threat.

3.6. Consensus Protocol

In distributed and multi-agent systems such as UAs, the consensus method is crucial for building trust and reliability in the network. A detailed explanation of how the system works, including the rules for forming the selection blocks of committee.

3.7. Generation of Blocks

Accumulating transactions in a block can cause communication delay or slowdown the transmission speed in the network if the block creation rate is uncertain. Otherwise, if mining happens too often, the nodes of the blockchain system may become overloaded with processing. The presented design is based on creating blocks in the right place; therefore, setting the block generation rate is recommended. Each block is created at a certain time interval, requiring a regular mining cycle. After creating the previous block, the mining process moves to the next round. Since different jobs have different communication requirements, the time interval between two block generation steps can be set individually. The mining time interval, average block size, and periodic memory emptying time interval are all variables that can be used to model the data storage capacity of the UA network. Indeed, the limit ensures that each device has enough memory to store data on the blockchain until the next memory release.

4. Future work in this area

The use of blockchain technology in drone registration can bring several benefits, such as increased security, transparency, and immutability of the registration process. Possible future work in this area could include:

1. Decentralized drone identification: Using blockchain, a unique and tamper-proof identifier can be assigned to each drone, which can help track and regulate their usage.

2. Real-time tracking: By integrating GNSS and other location-based technologies with blockchain, real-time tracking of drones can be achieved, enabling authorities to monitor their movements and usage patterns.

3. Smart Contract-based flight plans: Smart contracts can enforce regulations and restrictions on drone flights, such as no-fly zones, altitude restrictions, and flight plans, making the process more efficient and automated.

4. Secure data exchange: With blockchain, sensitive information such as flight data and usage history can be securely exchanged between stakeholders such as drone manufacturers, operators, and regulators, improving data privacy and secu-

rity.

5. Improved compliance: By having a centralized, secure, and transparent drone registration process, it will become easier for authorities to monitor and enforce compliance with regulations and laws, ensuring the safe and responsible usage of drones.

Conclusion

Drones are an integral part of the Internet of Things (IoT) and have numerous applications such as agriculture, rescue operations, pipeline inspection, filming, and delivery of goods and medicine. With their increasing popularity, new challenges have arisen regarding managing drone flight locations, reducing collisions, and protecting UAs from cyberattacks. Blockchain technology has emerged as a solution to these problems and provides the desired level of transparency, trust, security, and privacy. Blockchain technology is expected to support the commercial drone industry by providing security and identity management, supporting aircraft traffic control, UA conflict management, and flight permission. The use of blockchain helps identify noncom pliant UAs, improves cyber security, and provides air traffic controllers with additional information about the UA and its operator. Future work includes decentralized drone identification, real-time tracking, Smart Contract-based flight plans, secure data exchange, and improved compliance.

Reference

Abdo, J. B., & Zeadally, S. (2020). Multi-Utility Market: Framework for a Blockchain Exchange Platform for Sustainable Development. *arXiv preprint arXiv:2007.07096.*

Abdo, J. B., Demerjian, J., Chaouchi, H., Barbar, K., & Pujolle, G. (2013, December). Broker-based cross-cloud federation manager. In *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)* (pp. 244-251). IEEE.

Ahamed Ahanger, T., Aldaej, A., Atiquzzaman, M., Ullah, I., & Yousufudin, M. (2022). Distributed Blockchain-Based Platform for Unmanned Aerial Vehicles. *Computational Intelligence and Neuroscience, 2022.*

Alladi, T., Chamola, V., Sahu, N., & Guizani, M. (2020). Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications, 23***,** 100249.

Campbell, R. (June 1, 2017). *Walmart Taps Blockchain Tech to Track Delivery Drones.* https://www.ccn.com/ walmart-taps-blockchain-tech-track-delivery-drones

Chantz, H. (2016). Using Blockchain to Address Drone Cybersecurity. *published by securityIntelligence. com, on Aug, 25.* https:// securityintelligence.com/using-blockchain-to-address-drone-cybersecurity

Coinidol. (July 18, 2018)**.** *Boeing to Develop Blockchain and Artificial Intelligence into Drone Traffic System.* https://coinidol.com/boeing-to-develop-blockchain-and-artificial-intelligence-into-drone-traffic-system/

CoinWire (September 5, 2018)**.** *Walmart Proposes Blockchain-Based*

Authentication of Delivery Drones. https:// www.coinwire.com/walmart-proposes-blockchain-based-authentication-of-delivery-drones

Deep Aero Drones (May 10, 2018). *How Is Blockchain Serving the Drone Industry?.* https://medium.com/ deepaerodrones/how-is-blockchain-serving-the-drone-industry-f22f4a1f147

Deoras, S. (April 20, 2018). *How Blockchain and AI Are Important In the Drone Industry***.** https:// analyticsindiamag.com/how-blockchain-and-ai-are-important-in-the-drone-industry/

Dragonchain (July 14, 2019). *What Is Blockchain?* https://dragonchain.com/blog/what-is-blockchain/

Hashem, Y., Zildzic, E., & Gurtov, A. (2021, November). Secure drone identification with hyperledger Iroha. In *Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications* (pp. 11-18).

Lillian, B. (May 18, 2017). *UAV Carries Out Extensive Inspection of Railroad Truss Bridge.* https:// unmanned-aerial.com/uav-carries-extensive-inspection-railroad-truss-bridge

Lin, C., He, D., Kumar, N., Choo, K. K. R., Vinel, A., & Huang, X. (2018). Security and privacy for the internet of drones: Challenges and solutions. *IEEE Communications Magazine, 56*(1), 64-69.

Lin, J., Shen, Z., Miao, C., & Liu, S. (2017). Using blockchain to build trusted LoRaWAN sharing server. *International Journal of Crowd Science, 1*(3), 270-280.

Lumb, D. (June 7, 2017). *Google Tests Air Traffic Control System that Manages Lots of Drones.* https://www. engadget.com/2017/06/07/google-tests-air-traffic-control-system-for-drones/

Merrefield, C. (2018). *What Blockchains Could Mean for Government and Transportation Operations* (No. DOT-VNTSC-18-03). John A. Volpe National Transportation Systems Center (US). https://rosap.ntl.bts.gov/view/dot/34614

Phoneweek (2018). *Blockchain Technology Market in Transportation and Logistics Industry Market 2022 Growth, Share, Region Wise Analysis of Top Vendors, Application.* https://www.phoneweek.co.uk/blockchain-technology-market-in-transportation-and-logistics-industry-market-2022-growth-share-region-wise-analysis-of-top-vendors-application/

Reisman, R. (2019) *Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy.* https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20190000022.pdf

UAS Vision (March 11, 2019)**.** *Red Cat Releases Beta Version of Blockchain-Based 'Black Box' Flight Recorder for UAS.* https://www.uasvision.com/2019/03/11/red-cat-releases-beta-version-of-blockchain-based-black-box-flight-recorder-for-uas/

Wilmoth, J. (August 30, 2018). *Walmart Wants to Build an Army of Autonomous Robots Controlled by Blockchain.* https://www.ccn.com/walmart-wants-to-build-an-army-of-autonomous-robots-controlled-by-blockchain/

Wilmoth, J. (September 20, 2018). *IBM Patent Eyes Blockchain for Drone Fleet Security.* https://www.ccn.com/ ibm-patent-eyes-blockchain-for-drone-fleet-security/

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper, 151*(2014), 1-32.

Submitted: 05.09.2022
Accepted: 28.11.2022