Journal of
Blockchain and Intelligent Computing

Tech Science Press

DOI: 10.32604/jbic.2023.041340

ARTICLE

Time-Efficient Blockchain Framework for Improved Data Transmission in Autonomous Systems

Abdulrahman M. Abdulghani, Wilbur L. Walters and Khalid H. Abed*

Department of Electrical & Computer Engineering and Computer Science, Jackson State University, Jackson, Mississippi, USA

*Corresponding Author: Khalid H. Abed. Email: khalid.h.abed@jsums.edu

Received: 19 April 2023 Accepted: 03 July 2023 Published: 29 September 2023

ABSTRACT

Blockchain technology is increasingly used to design trustworthy and reliable platforms for sharing information in a plethora of industries. It is a decentralized system that acts as an immutable record for storing data. It has the potential to disrupt a range of fields that rely on data, including autonomous systems like Unmanned Aerial Vehicles (UAVs). In this paper, we propose a framework based on blockchain and distributed ledger technology to improve transmission time and provide a secured and trusted method for UAVs to transfer data to the consumer efficiently while maintaining data reliability. The results show that our framework enables fast, easy, and seamless interactions between UAVs data providers and enhances privacy and security, with elapsed time being a key factor. The simulation of the framework revealed that the elapsed time during the transfer of the data via Microsoft Azure, Amazon S3 and the proposed blockchain framework are 1312, 929, and 674 s, respectively.

KEYWORDS

Blockchain technology; autonomous systems; Unmanned Aerial Vehicles (UAVs); data transmission; elapsed time; data reliability

1 Introduction

Blockchain has the potential to significantly enhance the security and robustness of autonomous systems [1]. Providing a decentralized and tamper-evident record-keeping blockchain can help ensure the integrity and consistency of data and facilitate secure communication between nodes [2]. One potential application of blockchain in autonomous systems is the secure management of device identities [3]. By using blockchain to store and verify the identities of nodes in a decentralized manner, it is possible to prevent identity spoofing and ensure that only authorized nodes can access specific networks or resources [4]. This can especially be important in systems where nodes may operate without direct human oversight. Another use case for blockchain in autonomous systems is the secure recording and transmission of data [5]. The decentralized nature of blockchain allows for the creation of tamper-evident records of data, which can help ensure that the data generated by autonomous nodes has not been altered or corrupted in any way [6]. This can be particularly useful when data integrity is critical, such as in healthcare, industrial control systems, and mission-critical military autonomous systems. Moreover, smart contracts are considered an innovation, which plays self-executing contracts with the terms of the agreement that can be used to automate specific processes, and this ensures that smart contracts are carried out securely and transparently [7]. For example, smart contracts could be used to manage the execution of actions by autonomous nodes based on specific triggers or conditions [8]. The use of blockchain technology in autonomous systems can help improve security, reliability, and transparency [9]. However, there are also challenges and limitations to consider because of the potential for scalability issues and the need for robust governance models [10]. Further research is needed to fully understand the potential and limitations of using blockchain in autonomous systems.

Autonomous systems, such as self-driving cars and Unmanned Aerial Vehicles (UAVs), have the potential to revolutionize a wide range of military and industrial applications. However, the reliability and security of these systems are considered critical concerns because any failure or vulnerability can have serious consequences. One challenge in securing autonomous systems is data transmission from the system to a server or other remote locations, which can be vulnerable to interference, tampering, or interception [11]. To address these security concerns, researchers have proposed the use of blockchain technology to secure the transmission of data from autonomous systems. Blockchain is a decentralized, distributed ledger that can securely record transactions, such as data transmission from autonomous systems [12,13]. The decentralized nature of blockchain makes it resistant to tampering and interference because there is no single point of failure that attackers can target [14]. Using cryptographic hashes and consensus algorithms also ensures the integrity of the data because any attempt to modify the data on the blockchain will be detected and rejected. In addition to enhanced security, using blockchain for UAV data transmission can provide other benefits, such as improved efficiency and scalability. By reducing the reliance on centralized servers and intermediaries, blockchain-based solutions can reduce the overhead associated with data transmission, allowing for faster and more efficient data transfer. Blockchain can also support many transactions that require high volumes of data transfer, such as UAVs [15].

The steps we will consider to implement the proposed blockchain framework might be a time-consuming bypass and slower than the traditional transmission methods due to the additional steps and verifications involved in the process. The elapsed time is considered the time the data takes to flow through the blockchain from the first block to the last block, so minimizing the elapsed time is the focus of this research project. The rest of this article is organized as follows: In Section 2, we review the state-of-art UAV data transmission using blockchain. In Section 3, we present the proposed blockchain framework. Section 4 discusses the results, and we provide a conclusion in Section 5.

2 Related Work

The use of blockchain technology for securely transmitting data from UAVs to servers has garnered significant attention in recent years. In this section, we review and examine the potential benefits and limitations of using blockchain for UAV data transmission, so we have focused on relevant studies that have been published since 2018. We also investigate the challenges and considerations involved in implementing blockchain-based solutions related to UAV applications. Our research review of the literature has allowed us to organize the relevant studies into three main categories: UAV data transmission in blockchain, the elapsed time, and the consensus mechanisms.

2.1 UAV Data Transmission in Blockchain

A blockchain-based solution for securing the transmission of data from UAVs to ground control stations was proposed in [16]. The authors proposed a hybrid blockchain that combines the security and reliability of a public blockchain with the privacy and efficiency of a private blockchain, allowing for the secure and efficient transmission of UAV data.

Another study [17] explored the use of blockchain for securing the transmission of data from UAVs to cloud servers. The authors proposed a blockchain-based protocol that utilizes smart contracts to verify the authenticity and integrity of the data transmitted by the UAVs. The protocol also includes a mechanism for dynamically adjusting the blockchain's block size based on the volume of data being transmitted, allowing for efficient and scalable data transfer. While the use of blockchain for UAV data transmission holds promise for improving the security and reliability of data transfer, there are also several challenges like trustworthiness to consider [18,19].

In [20], researchers examined the use of blockchain for secure data transmission in the healthcare industry, and they found that it can improve data security and reduce the time required for data transmission compared to traditional methods. Similarly, the study in [21] explored the use of blockchain for supply chain management, and researchers concluded that it can facilitate faster and more secure data transmission between stakeholders.

In [22], the authors proposed a blockchain-based solution for securing the transmission of data from UAVs to ground control stations in the context of search and rescue operations. The authors proposed a hybrid blockchain that combines the security and reliability of a public blockchain with the privacy and efficiency of a private blockchain and includes a mechanism for dynamic block size adjustment based on the volume of data being transmitted. Moreover, they conducted simulations to evaluate the performance of the proposed solution and found that it achieved improved security and efficiency compared to traditional frameworks.

In [23], the authors proposed using blockchain to secure data transmission in the Internet of Things (IoT) by creating a decentralized network of nodes that can validate and record data transmissions. They demonstrated the effectiveness of their technique through simulations and showed that it could significantly reduce transmission time compared to traditional methods.

In [24], the authors explored the use of blockchain to secure data transmission in wireless sensor networks (WSNs). They proposed a hybrid blockchain-based approach that combines both private and public blockchain elements to improve the efficiency and security of data transmission in WSNs.

The authors in [25] proposed using blockchain technology to improve the security and efficiency of Electronic Health Records (EHR) data transmission in 5G networks. Their framework demonstrated the ability to reduce transmission time and increase the overall security of 5G networks; however, it may come with some costs in terms of data sent for record updates.

Based on our research review, we think that the use of blockchain technology holds promise for securing the transmission of data from UAVs to servers, offering enhanced security and reliability compared to traditional frameworks. While there are challenges and considerations to be addressed in implementing blockchain-based solutions for UAV data transmission, recent research has demonstrated the potential of this technology for this application. Further research and the development of regulatory frameworks and standards will be necessary to fully realize the potential of blockchain for UAV data transmission. Moreover, the challenge is the need for careful design and implementation of the blockchain to ensure that it can meet the performance and scalability requirements of the UAV application. This may include measures such as securing key management as follows:

- Define the structure of a block in the blockchain: Each block contains a set of data and a hash of the previous block. This structure helps ensure the integrity and security of the data in the blockchain.

- Define the structure of the blockchain: The blockchain is a distributed database that consists of a series of blocks that are linked together in chronological order. It should have methods for adding new blocks, validating the chain's integrity, and calculating the elapsed time.
- Obtain the data to be added to the blockchain: The data for the blockchain can be obtained from various sources, such as IoT nodes, sensors, or databases. It is essential to ensure that the data is accurate, relevant, and secure.
- Add the data to the blockchain: For each piece of data, a new block is created and added to the chain. The new block contains the data and a hash of the previous block. This helps ensure the integrity and security of the data in the chain.
- Validate the integrity of the blockchain: It is essential to periodically check the chain's integrity by verifying that the hashes of the blocks are correct. This helps ensure that the data in the blockchain has not been tampered with or corrupted.

2.2 The Elapsed Time

The elapsed time of a secure autonomous system based on blockchain technology can be calculated by determining the total time required to complete all tasks or processes within the system [19]. In the context of UAV data transmission, this may include the time required for the UAV to transmit data to the server or ground control station as well as any additional processing or verification that may be required by the blockchain-based system [20]. To calculate the elapsed time of a secure autonomous system based on blockchain technology, it is necessary to initially identify all the tasks or processes that are part of the system [14,20]. This may include tasks such as data transmission, data verification, and consensus building in addition to any other processes that are required to complete the system's objectives [21]. Next, the time required to complete each task or process should be determined [15]. This may involve measuring the actual time required to complete the task or using estimates based on past performance or other data [22]. Last, the elapsed time of the system can be calculated by adding up the time required to complete all tasks or processes within the system [22]. This will give an overall measure of the time required to complete all tasks or processes within the system, providing a benchmark for evaluating the efficiency and performance of the system [23]. It is important to note that the elapsed time of a secure autonomous system based on blockchain technology may vary depending on several factors, such as the volume of data being transmitted, the complexity of the tasks or processes being performed, and the performance and efficiency of the blockchain-based system [22,24].

Based on our research review, we think that it will be necessary to regularly recalculate the elapsed time to ensure that the system meets performance and efficiency requirements.

2.3 The Consensus Mechanism

A consensus mechanism is a fundamental component of any blockchain system because it is responsible for ensuring that all participants in the network agree on the state of the blockchain and the validity of new transactions. In this part, we discuss the different types of consensus mechanisms that are used in blockchain systems and how they work, including examples of current research in this area. One popular type of consensus mechanism is proof-of-work (PoW), which is used by the original Bitcoin blockchain. In a PoW system, miners compete to solve a computationally complex problem, and the first one to solve it gets to add the next block to the chain [25]. This process consumes a large amount of energy, but it ensures that the blockchain is secure and decentralized because no single entity has the power to control it. Another type of consensus mechanism is proof-of-stake (PoS), which is used by some newer blockchain systems. In a PoS system, the right to add the next block is determined by the number of tokens a participant holds rather than by the ability to solve a computationally intensive problem. This can be more energy efficient than PoW, but it can also be more centralized because those with the most tokens have the greatest influence on the network [26]. The third type of consensus mechanism is proof-of-elapsed-time (PoET), which is used by the Hyperledger Sawtooth blockchain. In a PoET system, each participant is assigned a random wait time, and the first to finish waiting gets to add the next block to the chain. This can be more energy efficient than PoW, but it requires using a trusted third party to assign the wait times [26]. Many other types of consensus mechanisms have been proposed or are under development, including proof-of-activity (PoA), proof-of-capacity (PoC), proof-of-importance (PoI), and proof-of-authority (PoA). Each of these mechanisms has its strengths and weaknesses, and researchers are actively working to improve and optimize them.

Based on our research review, we concluded that the consensus mechanism is a critical component of any blockchain system because it determines how transactions are validated and how the state of the blockchain is maintained. Researchers are actively exploring and improving various consensus mechanisms to find the best balance between security, efficiency, and decentralization.

3 The Proposed Blockchain System

3.1 The Proposed Method

Our proposed method aimed at secure and time-efficient data transmission for an autonomous system using blockchain technology. By leveraging the decentralized and immutable nature of blockchain, it is possible to ensure the integrity and provenance of the data, while also reducing the elapsed time of the transmission process. One potential framework for using blockchain for transmitting image data from UAVs is to store the data on a decentralized file storage system like Inter Planetary File System (IPFS) and use a wallet to record a hash of the data and any relevant metadata using SHA256. This allows for the data to be transmitted directly from the UAV to the server without passing through a central or third-party server, which can help reduce the elapsed time of the transmission process. In addition to using decentralized file storage, we used a peer-to-peer networking protocol (BitTorrent) to transmit the data directly from the UAV to the server. By using a combination of decentralized file storage and peer-to-peer networking, it is possible to achieve both security and efficiency in the transmission process. Additionally, we use a high-bandwidth wireless network protocol (Wi-Fi) as the mean which is more suitable for transmitting large amounts of data quickly and reliably.

Overall, by carefully designing and implementing a blockchain-based system for transmitting image data from UAVs, we can achieve both security and less transmission time in the process. By considering factors such as decentralized file storage, peer-to-peer networking, network protocols, and data transmission optimization, we can significantly reduce the elapsed time of the transmission process while also ensuring the integrity and provenance of the data.

In recent years, there has been an increased interest in using blockchain technology for securing data transmission from UAVs to servers. This is due to the potential benefits of blockchain-based solutions, such as enhanced security and reliability as well as the ability to support decentralized and autonomous systems. However, implementing blockchain-based solutions for UAV data transmission is not without challenges, so it is important to carefully consider the performance of such solutions. The elapsed time of a system refers to the total time required to complete all tasks or processes within the system and is an important measure of the efficiency and performance of the system.

To secure the data transmission from UAVs to servers using blockchain technology in a way that considers the elapsed time, we adopt a structured and systematic framework for the design and evaluation of the system. The proposed blockchain framework consists of the following steps:

1) *Identify the requirements and objectives of the system*: This may include thoughts such as the volume of data to be transmitted, the reliability and security requirements of the system, and any other factors that may impact the design and performance of the system.
2) *Develop a conceptual design for the system*: Based on the requirements and objectives identified in (1), develop a conceptual design for the system that outlines the key components and processes of the system as well as any additional concerns such as security measures or regulatory requirements.
3) *Evaluate the elapsed time of the conceptual design*: Using the conceptual design developed in (2), evaluate the elapsed time of the system. This may involve estimating the time and resources required to complete each task or process within the system as well as any additional expenses that may be incurred in the process of building and operating the system.
4) *Refine the conceptual design*: Based on the results of the elapsed time evaluation in (3), refine the conceptual design as necessary to optimize the performance and effectiveness of the system. This may involve making changes to the system's design, such as simplifying processes or reducing the number of components.
5) *Develop and implement the system*: Based on the refined conceptual design developed in (4), develop and implement the system according to the specifications and objectives. This may involve building and testing prototypes as well as any additional activities that may be required to fully deploy the system.
6) *Monitor and evaluate the system*: Once the system has been implemented, monitor, and evaluate the system's performance on an ongoing basis. This may involve collecting and analyzing data on the elapsed time of the system in addition to any other relevant performance metrics. Based on the results of the monitoring and evaluation, make any necessary improvements to the system to optimize its performance.

By following the proposed systematic framework that considers the elapsed time, we can secure the data transmission from UAVs to servers using blockchain technology in a way that maximizes the benefits of blockchain-based solutions while minimizing the potential challenges associated with their implementation. This can help ensure that the system is trustworthy and effective, and it meets the needs and objectives of the consumers. There are some potential benefits to using blockchain technology to secure data transmission from UAVs to servers. One of the main advantages is enhanced security because blockchain-based systems use decentralized networks and cryptography to ensure the integrity and confidentiality of data transmissions. This can help prevent unauthorized access or tampering with the data and can provide an additional layer of protection against cyber threats. Another advantage of blockchain-based solutions is their ability to support decentralized and autonomous systems. This can be particularly useful in UAV data transmission because it allows for data transmission from multiple sources to multiple destinations without the need for a central authority or intermediary. This can help improve the scalability and flexibility of the system and can enable the system to operate more efficiently and effectively without the need for specialized expertise. While blockchain-based solutions for securing UAV data transmission can offer numerous benefits, it is essential to carefully consider the elapsed time of such systems and adopt a systematic approach to their design and evaluation. This helps ensure the reliability of the system. One major challenge in implementing a blockchain-based system is timing because the network-based complexity can lead to longer implementation times compared to traditional systems. Therefore, it is important to carefully evaluate the trade-offs between the benefits of using blockchain technology and the potential increase in elapsed time.

3.2 Implementation of the Proposed Framework

This section presents a simple method for adding UAVs to a blockchain network, in this case, Hyperledger Fabric in a secure manner with less execution time. The proposed architecture shown in Fig. 1 involves a UAV using its camera to gather image data, which is then published to the blockchain network. The data is distributed to registered subscribers, which are applications within the blockchain network that have been authenticated as users of a particular node. These applications create transactions on the Hyperledger network based on the received data.

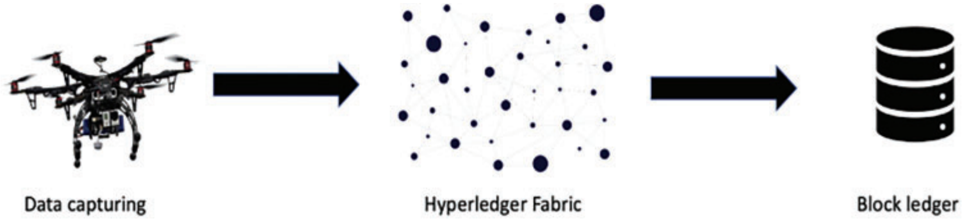

Figure 1: UAV data integration with Hyperledger network

The data on the network is kept secure using distributed databases called ledgers, which store all of the transactions (called blocks) in a chain linked together through hash values. If someone tries to alter the data in the Hyperledger Fabric state database, it will not be accepted by the other peers because the hash value of the preceding block will not match. The presence of these distributed databases among all stakeholders ensures the integrity of the data. Additionally, Hyperledger's distributed nature makes it highly resilient to failures and ensures authorized users can access the data continuously. If one peer becomes inaccessible, the data will still be available through the other peers carrying the ledger databases. Additionally, Hyperledger can handle many transactions per unit of time because it can use cheaper commodity hardware.

The article makes the following contributions to the usage of Hyperledger Fabric in UAV networks. First, it examines how Hyperledger Fabric is used in a special setting, demonstrating how flexible it is beyond conventional use cases. Second, it offers a specialized mechanism that enables safe and effective data transfer while utilizing constrained computational and energy resources, addressing the unique constraints encountered by UAV networks. Third, the study offers useful implementation details that will help in the design of UAVs with Hyperledger Fabric. Last, enhanced data integrity, decentralization, and failure resilience are considered possible advantages of adopting blockchain technology, specifically Hyperledger Fabric in UAV networks, and this makes it a vital contribution to the area of safe and efficient data transfer in autonomous systems.

To ensure that the data is delivered at the optimal time, we implemented the following steps as illustrated in Fig. 2. These steps ensure that the data transmission is secure with minimum elapsed time and improved trustworthiness of the proposed framework.

- *Optimize image file sizes*: Large image files can take longer to transfer, so reducing the file size of the images can help speed up the process.
- *Use a faster network connection*: Transferring data over a faster network connection, such as a Wi-Fi high-speed broadband connection can help reduce transfer times.

- *Implement shredding*: Shredding can help speed up transaction processing by dividing the blockchain shown in Fig. 3 into smaller chunks and processing them in parallel. This can be particularly useful when transferring large amounts of data such as images.
- *Use off-chain transactions*: Off-chain transactions allow certain types of transactions to be settled off the main blockchain, which can help reduce the load on the chain and speed up transaction processing.

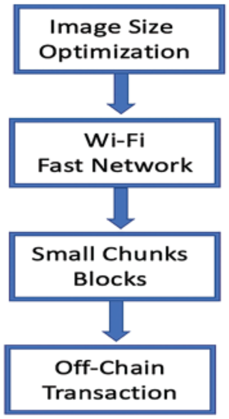

Figure 2: The steps to minimize the time in the blockchain transaction

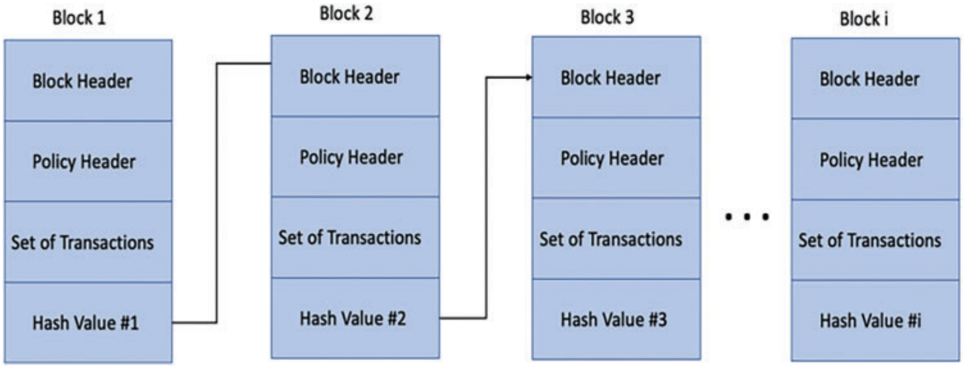

Figure 3: The blockchain structure used in the proposed framework

In this work, we utilized PoW system nodes, called "miners", to compete in solving a complex mathematical puzzle for transaction validation and addition to the blockchain. We employ a modified PoW mechanism for the parallel processing of smaller data chunks as part of the shredding step. The PoW offers strong security and robustness, making it a viable option even in resource-constrained mobile robotics such as UAVs. It is also compatible with existing blockchain ecosystems like Hyperledger Fabric, leveraging their strength and interoperability for UAV networks. PoW provides superior security and resilience compared to other algorithms, particularly in resource-constrained environments, ensuring data integrity and trust in autonomous systems. In addition, in our framework, the subscriber who first completes the proof-of-work for a specific chunk is authorized to add the corresponding block to the chain. This incentivizes efficient processing and reduces overall data transfer time. To maintain proper sequence, we adopt a timestamp-based strategy where each block is timestamped at creation, and the timestamp is included in the block's hash. This arrangement guarantees a reliable and consistent sequence of transactions on the blockchain.

Furthermore, we consider certain transactions for off-chain processing, specifically those involving more compact data. These transactions, identified for their reduced security concerns and efficiency advantages, are eligible for off-chain settlement. This selection maximizes the overall efficiency and security of the system because these transactions can be executed off-chain, relieving the burden on the main blockchain and accelerating transaction processing.

To ensure effective transaction validation, we employ payment channels that establish agreements between parties to exchange payments without relying on the blockchain. By utilizing payment channels, the number of transactions requiring processing on the blockchain can be reduced, resulting in improved efficiency. The utilization of payment channels offers an effective approach to transaction validation while reducing the transaction load on the blockchain.

4 Results and Analysis

To evaluate the performance of the proposed framework, we conducted a series of experiments using a dataset of 5 GB consisting of 2405 high-quality images captured by a UAV [27]. These images were transferred to a local server using two established methods: Microsoft Azure [28] and Amazon S3 [29] to simulate the transmission of data from the UAV to the consumer and measure the time required for the transfer. Additionally, we implemented the proposed framework, shown in Fig. 4, by using a blockchain bypass to improve the security, availability, and elasticity of the data transfer process while minimizing the elapsed time. The results of these experiments are shown in Fig. 5.

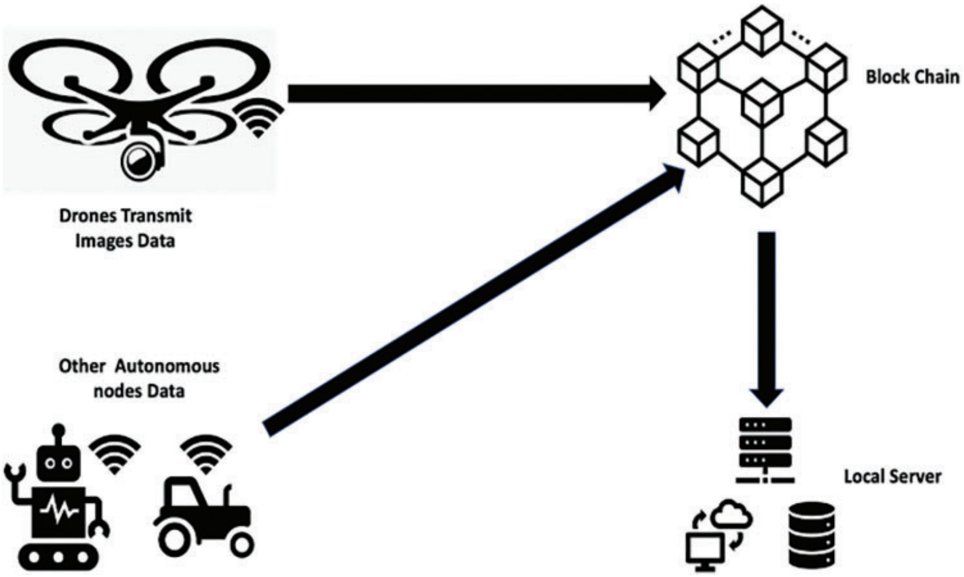

Figure 4: UAVs data transfer through the proposed blockchain framework

The effectiveness of our system is determined by elapsed time parameter for data transfer. This factor is crucial in determining the efficiency of the proposed framework from the moment the UAV captures the data until the appropriate response is sent back to the server. This metric measures the miner's elapsed time in terms of how quickly it can handle incoming transactions. Hence, calculating the elapsed time of the proposed framework and comparing it with other traditional methods is described in (1).

$$\mathrm{Et} = Rc - Tx \tag{1}$$

While (***Et***) represents the elapsed time, (***Rc***) is the receiving time, and (***Tx***) is the transmission time. Moreover, (***Et***) is important because it determines the speed at which the miner can process transactions and contribute to the overall performance of the system. The experiment was conducted using Python 3.9 programming language to simulate the scenarios and calculate the elapsed time. The simulation considered real-world assumptions to get the results shown in Fig. 5, which shows the comparison of the results for the three data transmission elapsed times.

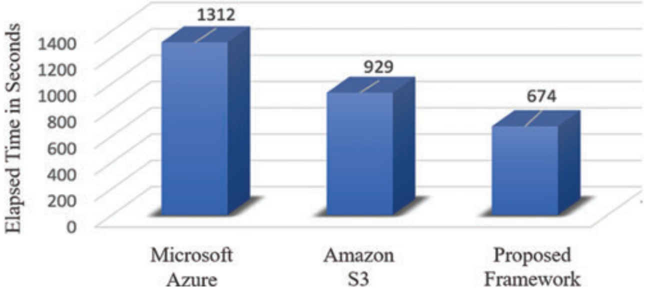

Figure 5: The elapsed time during the transfer of the data via Microsoft Azure, Amazon S3, and the proposed blockchain framework

Based on the data provided, it appears that consuming less time in data transfer is generally beneficial. In this case, the proposed framework provided the shortest data transfer time of 674 s, followed by 929 s obtained from Amazon S3 at and 1312 s obtained from Azure. This suggests that the proposed blockchain was the fastest platform for data transfer in this comparison, followed by Amazon S3 and then by Azure. Although our major focus is the assessment of our suggested framework, we think that there is a need of giving comparative analyses with respect to the necessity for comparisons with comparable methodologies in the experimental part. We purposefully selected Microsoft Azure and Amazon S3, two well-known systems in the realm of data transmission and storage, for comparison in our study. By comparing our suggested solution's performance to those of these well-known platforms, the goal was to show how effective and efficient the proposed blockchain is in terms of data transfer time. Through this comparison, we demonstrate the advantages and potential gains of using blockchain technology in autonomous systems, particularly for UAV data transfer. We provided analytical data on how our framework performs in comparison to existing commercial solutions.

It is worth noting that data transfer times can be affected by various factors, including the size and complexity of the data being transferred, the distance between the sender and receiver, and the overall performance of the network. Therefore, it is essential to consider these and other factors when evaluating the elapsed time of different platforms for data transfer.

5 Conclusion and Future Work

In conclusion, the use of blockchain technology in this context offers several benefits over traditional methods. By leveraging the decentralized nature of the blockchain and distributed ledger technology, data can be transferred securely and reliably without the need for a trusted third party.

This can help reduce the time and resources needed to complete data transfers, making the overall process more efficient. Additionally, the use of blockchain can enhance data privacy and security by providing a secure and immutable record of data transfers. This is especially important in the context of autonomous systems like UAVs, where the data being transferred may be sensitive or critical to the operation of the system. Overall, the results suggest that the proposed method of using blockchain for data transfer in autonomous systems has the potential to significantly improve the efficiency and effectiveness of data transfer, while also enhancing security and privacy. There are a few potential directions for future work that could build on research such as further optimizing the data transmission rate.

Acknowledgement: The authors would like to thank the reviewers for their time and valuable comments.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm their contribution to the paper as follows: study conception and design: A. M. Abdulghani, K. H. Abed; data preprocessing: A. M. Abdulghani; analysis and interpretation of results: A. M. Abdulghani, W. L. Walters, K. H. Abed; draft manuscript preparation: A. M. Abdulghani, W. L. Walters, K. H. Abed. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data is available at http://dronedataset.icg.tugraz.at/.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Jain, N. J. Ahuja, P. Srikanth, K. V. Bhadane, B. Nagaiah *et al.,* “Blockchain and autonomous vehicles: Recent advances and future directions,” *IEEE Access*, vol. 9, pp. 130264–130328, 2021.

[2] R. Alkadi, N. Alnuaimi, C. Y. Yeun and A. Shoufan, “Blockchain interoperability in unmanned aerial vehicles networks: State-of-the-art and open issues,” *IEEE Access*, vol. 10, pp. 14463–14479, 2022.

[3] K. O. Toka, Y. Dikilitaş, T. Oktay and A. Sayar, “Securing IoT with blockchain,” in *The Int. Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, XLVI-4/W5-2021, pp. 529–532, 2021.

[4] F. U. Muram and M. Atif Javed, “Drone-based risk management of autonomous systems using contracts and Blockchain,” in *2021 IEEE Int. Conf. on Software Analysis, Evolution and Reengineering (SANER)*, Honolulu, HI, USA, 2021.

[5] Q. Zhao, S. Chen, Z. Liu, T. Baker and Y. Zhang, “Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems,” *Information Processing & Management*, vol. 57, no. 6, pp. 102355, 2020.

[6] B. Alamri, K. Crowley and I. Richardson, “Blockchain-based identity management systems in health IOT: A systematic review,” *IEEE Access*, vol. 10, pp. 59612–59629, 2022.

[7] T. Xu, “Smart contracts,” *Smart Legal Contracts*, pp. 225–245, 2022. https://doi.org/10.1007/978-3-319-26896-5_7

[8] Z. Wu and J. Liu, “Blockchain-based trusted avionics authentication for secure ground-to-air communication,” in *2022 IEEE/AIAA 41st Digital Avionics Systems Conf. (DASC)*, Portsmouth, VA, USA, 2022.

[9] M. Keshavarz, M. Gharib, F. Afghah and J. D. Ashdown, “UASTrustChain: A decentralized blockchain-based trust monitoring framework for autonomous unmanned aerial systems,” *IEEE Access*, vol. 8, pp. 226074–226088, 2020.

[10] E. H. Abualsauod, “A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network,” *Computers and Electrical Engineering*, vol. 99, pp. 107847, 2022.

[11] W. Xiao, M. Li, B. Alzahrani, R. Alotaibi, A. Barnawi *et al.,* “A blockchain-based secure crowd monitoring system using UAV SWARM,” *IEEE Network*, vol. 35, no. 1, pp. 108–115, 2021.

[12] D. Li, Z. Yang and D. Jia, “A hybrid blockchain for secure UAV data transmission in search and rescue operations,” *IEEE Access*, vol. 10, pp. 243445–243456, 2022.

[13] A. Islam and S. Y. Shin, “BHMUS: Blockchain based secure outdoor health monitoring scheme using UAV in smart city,” in *2019 7th Int. Conf. on Information and Communication Technology (ICoICT)*, Kuala Lumpur, Malaysia, pp. 1–6, 2019. https://doi.org/10.1109/ICoICT.2019.8835373

[14] A. Mitra, B. Bera and A. K. Das, “Design and testbed experiments of public blockchain-based security framework for IoT-enabled drone-assisted wildlife monitoring,” in *IEEE INFOCOM 2021—IEEE Conf. on Computer Communications Workshops (INFOCOM WKSHPS)*, Vancouver, BC, Canada, pp. 1–6, 2021. https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484468

[15] R. Gupta, A. Kumari and S. Tanwar, “Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G Communications,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, 2020. https://doi.org/10.1002/ett.4176

[16] L. Zhao, M. B. Saif, A. Hawbani, G. Min, S. Peng *et al.,* “A novel improved artificial bee colony and blockchain-based secure clustering routing scheme for FANET,” *China Communications*, vol. 18, no. 7, pp. 103–116, 2021. https://doi.org/10.23919/JCC.2021.07.009

[17] J. Rodríguez-Molina, B. Corpas, C. Hirsch and P. Castillejo, “SEDIBLOFRA: A blockchain-based, secure framework for remote data transfer in unmanned aerial vehicles,” *IEEE Access*, vol. 9, pp. 121385–121404, 2021. https://doi.org/10.1109/ACCESS.2021.3106379

[18] K. S. Alqarni, F. A. Almalki, B. O. Soufiene, O. Ali and F. Albalwy, “Authenticated wireless links between a drone and sensors using a blockchain: Case of smart farming,” *Wireless Communications and Mobile Computing*, vol. 2022, no. 3, pp. 1–13, 2022. https://doi.org/10.1155/2022/4389729

[19] S. H. Alsamhi, A. V. Shvetsov, S. V. Shvetsova, A. Hawbani, M. Guizani *et al.,* “Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration,” *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 1, pp. 328–338, 2023. https://doi.org/10.1109/TGCN.2022.3195479

[20] R. Gupta, A. Shukla, P. Mehta, P. Bhattacharya, S. Tanwar *et al.,* “AHAK: A blockchain-based outdoor delivery scheme using UAV for Healthcare 4.0 services,” in *IEEE INFOCOM 2020—IEEE Conf. on Computer Communications Workshops (INFOCOM WKSHPS)*, Toronto, ON, Canada, pp. 255–260, 2020. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020

[21] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava *et al.,* “Enabling drones in the internet of things with decentralized blockchain-based security,” *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6406–6415, 2021. https://doi.org/10.1109/JIOT.2020.3015382

[22] W. Xiao, M. Li, B. Alzahrani, R. Alotaibi, A. Barnawi *et al.,* “A blockchain-based secure crowd monitoring system using UAV swarm,” *IEEE Network*, vol. 35, no. 1, pp. 108–115, 2021. https://doi.org/10.1109/MNET.011.2000210

[23] W. Liang, M. Tang, J. Long, X. Peng, J. Xu *et al.,* “A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3582–3592, 2019.

[24] S. J. Hsiao and W. T. Sung, “Employing blockchain technology to strengthen the security of wireless sensor networks,” *IEEE Access*, vol. 9, pp. 72326–72341, 2021.

[25] G. Jain and A. Jain, “Blockchain for 5G-enabled networks in healthcare service based on several aspects,” *Blockchain Applications for Healthcare Informatics*, pp. 471–493, 2022. https://doi.org/10.1016/B978-0-323-90615-9.00018-9

[26] X. Li, K. Zhang and Y. Xu, “A comparative study of consensus protocols for blockchain networks,” *IEEE Access*, vol. 9, pp. 1–24, 2021.

[27] Dasmehdixtr, “Drone dataset (UAV),” Kaggle, 2019. [Online]. Available: https://www.kaggle.com/datasets/macedocja/uav-images-packet-loss-distortion

[28] Microsoft 2023, “Get started with azure—introduction: Microsoft azure,” Introduction | Microsoft Azure. [Online]. Available: https://azure.microsoft.com/en-us/get-started/

[29] Strand Street Press, “S3. Amazon,” 2002. [Online]. Available: https://aws.amazon.com/s3/?nc1=h_ls