drones

MDPI

Article

Optimizing Performance in Federated Person Re-Identification through Benchmark Evaluation for Blockchain-Integrated Smart UAV Delivery Systems

Chengzu Dong [1], Jingwen Zhou [2], Qi An [1], Frank Jiang [1,*], Shiping Chen [3], Lei Pan [1,*] and Xiao Liu [2]

[1] Centre for Cyber Resilience and Trust (CREST), Deakin University, Geelong, VIC 3216, Australia; dongc@deakin.edu.au (C.D.); a.an@deakin.edu.au (Q.A.)
[2] School of Information Technology, Faculty of Science Engineering & Built Environment, Deakin University, Geelong, VIC 3216, Australia; jingwen.zhou@deakin.edu.au (J.Z.); xiao.liu@deakin.edu.au (X.L.)
[3] CSIRO, Sydney, NSW 2015, Australia; shiping.chen@data61.csiro.au
* Correspondence: frank.jiang@deakin.edu.au (F.J.); l.pan@deakin.edu.au (L.P.)

Abstract: In recent years, edge-based intelligent UAV delivery systems have attracted significant interest from both the academic and industrial sectors. One key obstacle faced by these smart UAV delivery systems is data privacy, as they rely on vast amounts of data from users and UAVs for training machine learning models for person re-identification (ReID) purposes. To tackle this issue, federated learning (FL) has been extensively adopted as a promising solution since it only involves sharing and updating model parameters with a central server, without transferring raw data. However, traditional FL still suffers from the problem of having a single point of failure. In this study, we present a performance optimization method for federated person re-identification using benchmark analysis in blockchain-powered edge-based smart UAV delivery systems. Our method integrates a decentralized FL mechanism enabled by blockchain, which eliminates the necessity for a central server and stores private data on a decentralized permissioned blockchain, thus preventing a single point of failure. We employ the person ReID application in intelligent UAV delivery systems as a representative example to drive our research and examine privacy concerns. Additionally, we introduce the Federated Re-identification Consensus (FRC) protocol to address the scalability issue of the blockchain in supporting UAV delivery systems. The efficiency of our proposed method is illustrated through experiments on energy efficiency, confirmation time, and throughput. We also explore the effects of the incentive mechanism and analyze the system's resilience under various security attacks. This study offers valuable insights and potential solutions for addressing data privacy and security challenges in the fast-growing domain of smart UAV delivery systems.

Keywords: UAV delivery; blockchain; person ReID; IoT; edge computing; federated learning

Citation: Dong, C.; Zhou, J.; An, Q.; Jiang, F.; Chen, S.; Pan, L.; Liu, X. Optimizing Performance in Federated Person Re-Identification through Benchmark Evaluation for Blockchain-Integrated Smart UAV Delivery Systems. *Drones* **2023**, *7*, 413. https://doi.org/10.3390/drones7070413

Academic Editor: Diego González-Aguilera

Received: 4 May 2023
Revised: 19 June 2023
Accepted: 19 June 2023
Published: 22 June 2023

1. Introduction

In recent years, edge-based smart UAV delivery systems have emerged as a popular area of research and development, driven by their potential to revolutionize the way goods are transported and create new business opportunities [1]. This will meet the requirements of real-time communication for the upcoming autonomous vehicles. These systems are increasingly being adopted by various industries, capitalizing on cutting-edge technologies such as edge computing, blockchain, and machine learning [2,3]. Furthermore, the quantum coupon collector protocol could greatly enhance the security and efficiency of blockchain-based UAV delivery systems by offering significant quantum advantages in information transmission and learning, potentially revolutionizing logistics and supply chain management [4,5]. As these systems continue to evolve and become more sophisticated, ensuring data privacy and security has become a critical challenge, especially considering the vast amount of data generated by both users and UAVs [6,7].

Person re-identification, a vital component of smart UAV delivery systems, relies on machine learning models trained using large amounts of data to accurately identify and track individuals [8]. However, sharing and processing these data raises significant privacy concerns, necessitating innovative solutions that prioritize user privacy without compromising system functionality [9]. Federated learning has emerged as a potential solution to this problem, allowing for the sharing and updating of model parameters with a centralized server without transmitting raw data. Despite its advantages, conventional FL is vulnerable to single points of failure, limiting its effectiveness in ensuring data privacy and security [10].

In this paper, we present a novel approach to optimize the performance of federated person re-identification through benchmark analysis in blockchain-enabled edge-based smart UAV delivery systems. Our proposed solution leverages a blockchain-enabled decentralized FL mechanism, eliminating the need for a centralized server and storing private data in a decentralized permissioned blockchain, thus mitigating the risk of a single point of failure. To demonstrate the practical application of our approach, we implement the Fed-UAV framework [8] edge as a testbed and use the person ReID application in smart UAV delivery systems, examining its potential privacy concerns and challenges.

To address the scalability issues associated with blockchain technology and support the demands of smart UAV delivery systems, we introduce the FRC protocol. This innovative protocol enables more efficient processing of transactions and data storage, ensuring that the system can handle the growing volume of data generated by an expanding UAV delivery network.

We demonstrate the effectiveness of our proposed approach through a series of experiments focusing on energy efficiency, confirmation time, and throughput. Additionally, we discuss the impact of the incentive mechanism on system performance and analyze the resiliency of our solution under various security attacks. By providing a comprehensive examination of the challenges and potential solutions associated with data privacy and security in smart UAV delivery systems, our study offers valuable insights that can guide future research and development efforts in this rapidly evolving field.

In summary, this paper makes the following contributions:

- We propose a performance optimization approach for federated person re-identification in blockchain-enabled edge-based smart UAV delivery systems, utilizing a decentralized FL mechanism to address data privacy concerns. Furthermore, we conduct experiments to evaluate the effectiveness of our proposed approach, focusing on energy efficiency, confirmation time, and throughput, while also discussing the impact of the incentive mechanism and analyzing the solution's resiliency under various security attacks.
- We introduce the FRC Consensus protocol, which enhances blockchain scalability to support the growing demands of smart UAV delivery systems. Furthermore, our comprehensive study provides valuable insights into the challenges and potential solutions associated with data privacy and security in smart UAV delivery systems, paving the way for future research and development in this rapidly growing field.

The structure of this paper is organized as follows. Section 2 presents a review of the relevant literature and existing research in the field. Section 3 demonstrates a detailed explanation of our proposed solution, outlining its key system layers and mechanisms. In Section 4, we evaluate the effectiveness of our approach through various assessments and provide an extensive security analysis. Lastly, Section 5 concludes the paper, summarizing our contributions and highlighting possible future research directions.

2. Related Work

In this section, we explore significant contributions made in the fields of federated learning, UAVs, and IoT networks. We focus particularly on studies that have delved into the intersection of these domains. A common thread tying these studies together is

the leveraging of federated learning for various applications within UAV networks while addressing potential security issues.

Zhang et al. [8] proposed a framework called Fed-UAV, using federated learning to address the person re-identification problem in the UAV delivery service. The framework is designed to reduce data transmission between the UAV and cloud server, and experiments on three real-world datasets demonstrate its ability to achieve high accuracy and efficiency while protecting data privacy. However, this proposed framework may have some vulnerabilities such as a single point of failure, which can be caused by the malicious replacement of global model parameters at the centralized cloud server as the data leakage during transmission and storage remains a security issue.

Yazdinejad et al. [11] discussed the challenges and opportunities presented by the growing use of drones in IoT networks, particularly in the context of drone authentication. They pointed out that the traditional machine learning models for authentication have drawbacks in terms of data security, privacy, and scalability. To address these issues, the authors propose a federated learning-based drone authentication model that utilizes the drones' Radio Frequency features. The proposed model employs a deep neural network architecture with Stochastic Gradient Descent optimization performed locally on drones. Homomorphic encryption and secure aggregation methods are used to protect the model's parameters. The experiments demonstrate that the federated drone authentication model achieves high true positive rates during drone authentication and outperforms other machine learning-based models. However, one of the disadvantages of homomorphic encryption is its computational overhead. The encryption and decryption operations can be computationally expensive and may require additional resources, such as computational power and memory, to be performed efficiently. As a result, it may lead to slower processing times, longer latency, and higher energy consumption. Additionally, the complexity of the encryption scheme can make it difficult to implement and maintain in practice, especially in resource-constrained environments.

Pokhrel [12] proposed a framework based on blockchain that facilitates continuous knowledge sharing and collaborative learning for a Low Earth Orbit (LEO) satellite IoT and a swarm of Unmanned Aerial Vehicles. The framework utilizes federated learning features to ensure the accuracy of learning inferences. However, transmission failures that can lead to blockchain forking events are common in a dynamic environment, making energy conservation and delay reduction challenging. To minimize unwanted events and estimate the energy consumption for a given set of miners, block transmissions, and LEOs' or UAVs' mobility. Additionally, the article explains the allocation of mining resources based on deep learning and illustrates the synergistic benefits of FL with blockchain.

Pokhrel [13] proposed a novel approach to federated learning that utilizes blockchain technology and wireless mobile miners on drones in 6G networks for disaster response systems. The focus is on reducing latency and energy consumption to prevent blockchain forking events during operations. The research calculated the probability of forking events to assess system uncertainty and energy loss caused by forked blocks due to channel impairments or mobility. The authors also conducted practical analyses to estimate energy consumption based on parameters such as the number of miners, power consumption during computing and block transfer, and 6G channel dynamics.

Rupa et al. [14] discussed how virtual circuit-based devices, such as drones and UAVs, are being increasingly used for aerial surveying in remote and sensitive areas, but face security and privacy challenges. To overcome these challenges, the authors propose a solution based on blockchain technology that uses Pentatope-based elliptic curve cryptography and SHA to ensure data privacy and stores data on an Ethereum-based public blockchain for secure transactions. The proposed system is evaluated using an IoT-based virtual vehicle monitoring application, and the results show that it is efficient and secure compared to other methods. This methodology protects against data theft by stalkers and plaintext/ciphertext attacks, improving the security and privacy of VC-based device data.

Khan et al. [15] proposed a decentralized machine learning framework that uses blockchain technology to enhance the integrity and storage of data for intelligent decision-making among multiple UAVs. The proposed framework utilizes blockchain for decentralized predictive analytics and applies and shares machine learning models in a decentralized manner. The study evaluates the system using collaborative intrusion detection as a case study, demonstrating the feasibility and effectiveness of using blockchain-based decentralized machine learning in UAVs and other similar applications.

Kumar et al. [16] proposed a secure data-sharing framework that incorporates blockchain and deep learning to address the vulnerabilities of softwarized UAVs that use OpenFlow protocols, which can be a critical concern in combat surveillance. The framework uses blockchain technology to register and validate communication entities in the softwarized UAV environment through a smart contract-based Proof-of-Authentication consensus mechanism. Additionally, a deep neural network architecture-based flow analyzer is included to improve intrusion detection. The proposed framework is compared to standard baseline methodologies, and the effectiveness is demonstrated through security analysis and experimental findings. The framework addresses the vulnerabilities of softwarized UAVs and improves the security of their communication protocols in combat surveillance and other applications.

Liu et al. [17] discussed the security and privacy considerations with the use of 5G for unmanned aerial vehicles and the challenges with centralized authentication approaches. The authors propose a blockchain-based solution that uses multiple signatures based on threshold sharing to build an identity federation for collaborative domains, achieving cross-domain authentication for 5G-enabled UAVs. The proposed approach uses the smart contract for authentication to ensure reliable communication between cross-domain devices. Performance evaluations demonstrate the effectiveness and efficiency of the proposed scheme, providing a secure and privacy-preserving solution for 5G-enabled UAVs.

Gupta et al. [18] examined the potential of UAVs in providing cost and time-efficient solutions for various societal applications but also highlights the data security and privacy issues associated with them. They pointed out that many solutions have been proposed and most of them rely on cryptographic methods, which are computationally expensive. However, only a few researchers have suggested blockchain-based solutions, but these may suffer from high data storage costs and network latency, reliability, and bandwidth issues. To address these challenges, the authors propose an InterPlanetary File System and blockchain-based secure UAV communication scheme over the 6G network. This scheme ensures data security and privacy, reduces data storage costs, and enhances network performance.

Silva et al. [19] proposed a solution to address the challenge of human tracking in various applications, such as surveillance, military operations, and disaster relief services. The proposed solution is a decentralized, distributed deep learning algorithm called Real-Time Privacy-preserving Target Tracking Re-Identification, which is used by cooperative UAVs to track targets in complex and adversarial environments. RPTT-ReID resolves the shortcomings of current tracking algorithms, particularly in maintaining tracking when subjects cross paths or switch identities. The proposed solution is tested on a video dataset of crowded scenes and showed an accuracy between 79.91 and 93.27%. The study was conducted by Grogorev et al. [20] who explored the potential benefits of using multimodal data for person re-identification in computer vision and image processing. The authors collected and labelled a new person re-id dataset using a UAV drone, including pedestrian images and manually annotated attributes. They extracted word embeddings from text descriptions using the continuous bag-of-words model and combined them with image features. The authors employed a deep neural decision forest for pedestrian classification and showed the effectiveness of the proposed model through extensive experiments on the collected dataset.

Nguyen et al. [21] proposed an innovative Internet-of-Drones architecture that utilizes blockchain technology to address the limitation of current drone and UAV-based systems, such as the difficulty of maintaining the quality of service and a lack of flexibility, transparency, security, and traceability. This architecture incorporates different drones, edge

servers, and a Hyperledger blockchain network, and is capable of providing high-level services such as improved human detection accuracy, transparency, traceability, and security. The proof-of-concept design of the proposed architecture showed its ability to offer advanced services, including enhancing the operating time of a drone, improving human detection accuracy, and providing a high level of transparency, traceability, and security.

Jensen et al. [22] examined the possibility of cyber-attacks on UAV systems and proposed the use of blockchain technology as a solution. They provided an overview of blockchain technology, its components and characteristics, and how it can improve system security. The proposed proposal also explored the potential application of blockchain to UAV swarm environments and discussed Hyperledger Fabric as a potential blockchain framework for enhanced security.

Xu et al. [23] focused on the challenges associated with security and energy efficiency in UAV-assisted IoT applications. To tackle these challenges, the authors proposed a blockchain-based data collection system that involves UAVs as edge data collection nodes. These UAVs provided long-term network access to IoT devices through regular cruises and recharging, and are rewarded with charging coins for forwarding data and recording transactions. The proposed system also incorporated an adaptive linear prediction algorithm to reduce energy consumption by uploading prediction models instead of original data. The UAV swarm builds distributed ledgers based on blockchain to prevent malicious attacks. The study presented simulation results to demonstrate the effectiveness of the proposed system in enhancing the security and efficiency of data collection.

The reviewed literature, as listed in Table 1, underscores the promising potential of federated learning in UAV and IoT networks while raising essential concerns around data security, privacy, scalability, and computational efficiency. All the researchers highlighted innovative ways to apply federated learning to solve real-world problems, from person re-identification to drone authentication, and from cooperative learning in LEO satellite IoT to disaster response systems. The concerns about single points of failure, blockchain forking, and computational overhead, however, suggest that further research is needed to fully optimize the integration of federated learning, IoT, and UAV networks. This need for further research offers fertile ground for the exploration of novel frameworks and techniques that can address these challenges and maximize the benefits of federated learning in these cutting-edge technological domains.

Table 1. Related work.

Methodology	Reference	Year	Privacy Preservation
Fed-UAV	[8]	2021	×
Yazdinejad's model	[11]	2021	√
Pokhrel's framework	[12]	2021	√
Pokhrel's approach	[13]	2020	√
Rupa's system	[14]	2020	√
Khan's framework	[15]	2021	×
Kumar's framework	[16]	2022	√
Liu's solution	[17]	2021	×
Gupta's solution	[18]	2021	×
Silva's solution	[19]	2019	×
Grogorev's solution	[20]	2020	×
Nguyen's architecture	[21]	2021	×
Jensen's system	[22]	2019	√
Xu's framework	[23]	2020	×

3. System Design

The section presents the crucial system layers, the blockchain-enabled system workflow design, and the FRC consensus protocol, all of which contribute to the performance optimization of federated person re-identification through benchmark analysis in blockchain-enabled smart UAV delivery systems.

3.1. System Layers

As shown in Figure 1, our system is designed around several key layers, each contributing to overall performance and privacy protection. By leveraging edge computing, federated learning, and blockchain technology, our proposed solution addresses the challenges associated with data privacy and security while maintaining the functionality and efficiency of the smart UAV delivery system. This multi-layered approach provides a robust and scalable solution.

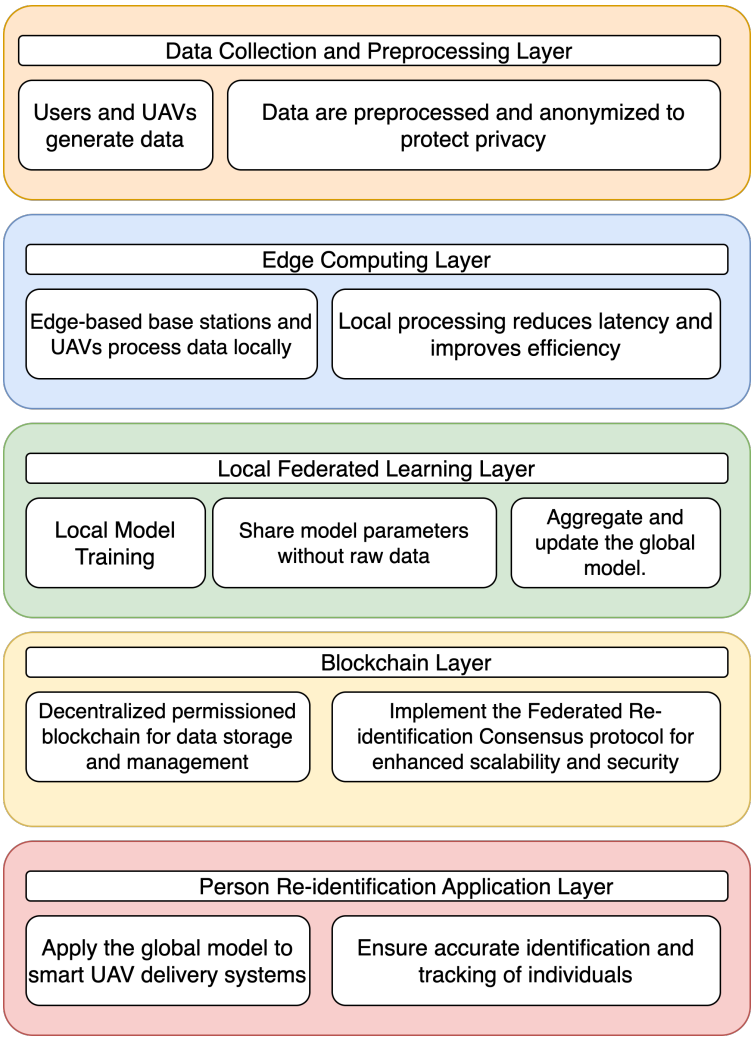

Figure 1. System layers.

- **Data Collection and Preprocessing Layer:** During the normal operation of the smart UAV delivery system, users and UAVs generate data primarily in the form of images or videos captured by the onboard cameras on the UAVs. These images or videos contain visual information about users, which is essential for the person's ReID task. To protect user privacy, it is crucial to preprocess these data by removing personally identifiable information and anonymizing the data. Anonymization techniques may include data normalization, noise addition, or data transformation. These preprocessing steps ensure that sensitive information is not leaked or misused, while still allowing the system to perform accurate person re-identification tasks based on the anonymized data.
- **Edge Computing Layer:** Edge devices, such as UAVs and base stations, process the preprocessed data locally, rather than sending it to a central server. This reduces latency and improves overall system efficiency. Local processing may involve tasks

such as feature extraction, data compression, or other analytics to prepare data for the federated learning process.

- **Local Federated Learning Layer:** Each edge device trains a federated learning model using its locally processed data. This ensures that the raw data remain on the device, preserving privacy. After local training, edge devices share their model parameters (e.g., weights, gradients) with the decentralized FL mechanism, instead of sharing raw data. The shared parameters are used to aggregate and update the global model, which is then distributed back to the edge devices for further training and refinement.
- **Blockchain Layer:** A decentralized permissioned Ethereum blockchain is integrated into the system for secure data storage and management. The Federated Re-identification Consensus protocol is implemented within the blockchain network, addressing scalability issues and ensuring enhanced security during the FL process.
- **Person Re-identification Application Layer:** The global model obtained from the federated learning process is applied to the smart UAV delivery system to perform person re-identification tasks. This enables the system to accurately identify and track individuals, improving the overall efficiency and effectiveness of the delivery process.

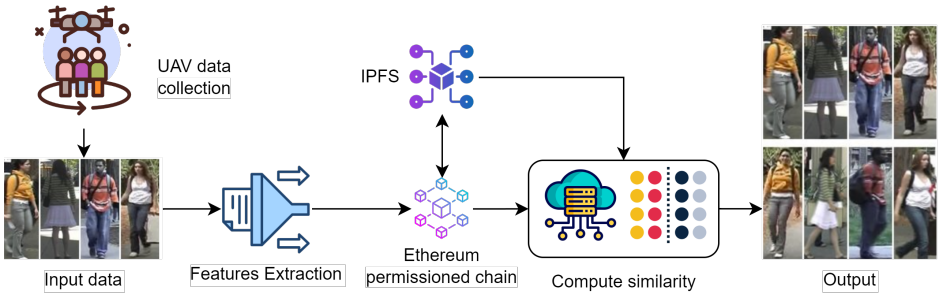

Figure 2. Blockchain-enabled system design.

3.2. Blockchain-Enabled System Design

As shown in Figure 2, UAVs are used for collect data. The data collected by the UAVs are then transmitted to a central system. These data could be in the form of images, videos, or other types of sensor data. Once the data are transmitted to the central system, they are fed into a feature extractor. The feature extractor is a software component that analyzes the data and extracts relevant features from them. These features are then stored in a decentralized storage system such as IPFS (InterPlanetary File System) [24].

The extracted features are stored on IPFS, which is a peer-to-peer network for storing and sharing files in a decentralized manner. The use of IPFS ensures that the data are stored in a secure and distributed manner, making it more resilient to attacks. After the features have been stored on IPFS, the hash ID associated with these features is recorded on a permissioned blockchain such as Ethereum. The use of a permissioned blockchain ensures that only authorized parties can access the data and ensures the integrity and immutability of the data.

During the federated learning process, the data are retrieved from IPFS to obtain the training output. Federated learning is a machine learning technique that allows multiple parties to collaboratively train a machine learning model without sharing their data. The extracted features stored on IPFS are used as training data for the federated learning process. When computing similarity, the federated learning algorithm compares the features stored on IPFS to the features extracted from the local data of each party. By comparing these features, the algorithm can identify similarities and patterns in the data without actually sharing the raw data itself.

UAVs are used for data collection, such as images or videos, which are then used to train local models and perform person re-identification tasks. Each UAV trains its local model with a specified learning rate to adapt to new information and adjust its parameters. After training, the UAVs calculate the local gradients which represent the direction and magnitude of change in the model parameters to minimize the loss function. As shown in

Algorithm 1, the UAVs then compute the Cosine Distance Weight (CDW) between their local gradients and the previous global model to measure similarity and contribution to the global model update. Finally, the local gradients from all UAVs are aggregated using the CDW as the weight, ensuring that each UAV's contribution to the global model is proportional to its similarity with the global model.

Algorithm 1 Fed-UAV with Cosine Distance Weight

Input: Local datasets $\{D_k\}_{k=1}^{K}$, maximum epochs T
Initialize: Global model W^0, learning rates $\{\eta_t\}_{t=1}^{T}$
for $t = 1, \ldots, T$ **do**
  for all $k \in \{1, \ldots, K\}$ **in parallel do**
    Sample a local dataset $D_k^{(t)} \subset D_k$
    Train local model $W_k^{(t)}$ on $D_k^{(t)}$ with learning rate η_t
    Calculate local gradient $G_k^{(t)} = W_k^{(t)} - W^{(t-1)}$
    Calculate Cosine Distance Weight $CDW_k^{(t)} = \frac{G_k^{(t)} \cdot W^{(t-1)}}{||G_k^{(t)}||_2 ||W^{(t-1)}||_2}$
  Aggregate local gradients with weights $CDW_k^{(t)}$: $G^{(t)} = \sum_{k=1}^{K} CDW_k^{(t)} G_k^{(t)}$
  Update global model: $W^{(t)} = W^{(t-1)} - \eta_t G^{(t)}$
Output: Global model W^T

However, the security and privacy of the federated learning process can still be vulnerable to attacks and misuse, posing potential risks to the parties involved. Integrating blockchain technology, such as Ethereum's permissioned chain, can enhance the security and privacy of federated learning while maintaining its original accuracy.

Ethereum's permissioned chain is a decentralized and secure platform that allows multiple participants to engage in secure and private transactions. This permissioned chain provides an additional layer of security and privacy to the federated learning process, ensuring that the model parameters and the identities of the parties involved remain confidential. Moreover, the permissioned chain can protect against potential attacks such as data poisoning, model inversion, and Sybil attacks [25]. Since the permissioned chain uses the FRC consensus protocol, it ensures that all participating nodes agree on the state of the network and the validity of transactions. This consensus mechanism helps prevent malicious nodes from tampering with the model parameters or colluding to manipulate the learning process.

Additionally, Ethereum's permissioned chain offers a transparent and auditable record of transactions. This feature is crucial in federated learning, as it allows all participating parties to verify the integrity of the model parameters and trace the source of any inconsistencies. The transparency provided by the permissioned chain also helps to build trust among the participants and encourages broader collaboration in the federated learning process.

Another benefit of incorporating Ethereum's permissioned chain in federated learning is the ability to use smart contracts. The FRC-integrated smart contracts can enforce specific rules and conditions for the federated learning process, such as the minimum number of participants, the acceptable range of model parameters, and the rewards for contributing to the global model. The use of FRC-integrated smart contracts can further enhance the security, privacy, and fairness of the federated learning process.

IPFS can also be integrated into the federated learning process alongside Ethereum's permissioned chain. IPFS is a peer-to-peer distributed file system that allows nodes to store and share data in a decentralized manner. By using IPFS, federated learning participants can store and share model parameters without relying on a central authority, which helps maintain the original accuracy of the model.

The integration of Ethereum's permissioned chain and IPFS in the federated learning process offers numerous advantages in terms of security, privacy, and trust. These tech-

nologies can help protect the federated learning process from attacks and misuse while maintaining the original accuracy of the model. As federated learning continues to evolve, the application of blockchain technology and decentralized storage systems will play a crucial role in ensuring secure and privacy-preserving machine learning.

3.3. FRC Consensus

The FRC consensus protocol aims to provide a more energy-efficient, scalable, secure, and privacy-preserving solution compared to traditional consensus mechanisms. By considering nodes' quality factors and allocating verification tasks based on their contributions, FRC encourages active participation and ensures a more robust federated learning process, particularly for the person re-identification.

$$W_i = C_i \times B_i \times R_i \tag{1}$$

$$VW_i = \frac{W_i}{\sum_{j=1}^{N} W_j} \tag{2}$$

where:

W_i represents the weight of node i. C_i represents the computational capacity of node i. B_i represents the connectivity bandwidth of node i. R_i represents the reliability of node i. VW_i represents the verification weight of node i. N is the total number of participating nodes.

Equation (1): This equation calculates the weight of node i by considering its computational capacity (C_i), connectivity bandwidth (B_i), and reliability (R_i). By factoring in these quality attributes, the FRC consensus protocol ensures a more efficient distribution of the verification workload among participating nodes.

Equation (2): This equation calculates the verification weight of node i by dividing its weight (W_i) by the sum of the weights of all participating nodes. The verification weight is then used to allocate verification tasks proportionally to the nodes' contributions to the federated learning process. This approach incentivizes cooperation, as nodes with higher contributions have a higher chance of being selected for verification tasks.

The advantages of FRC are summarized as follows:

- **Energy efficiency:** Unlike traditional consensus protocols such as Proof of Work (PoW), FRC does not require solving complex cryptographic puzzles, which can consume a significant amount of computational power and energy. By allocating weights based on the contributions to the federated learning process, FRC promotes a more energy-efficient consensus mechanism.
- **Scalability:** By considering the quality factors of nodes, including computational capacity, connectivity bandwidth, and reliability, FRC effectively distributes the verification workload among participating nodes, leading to improved scalability compared to traditional consensus mechanisms that may rely on a few powerful nodes.
- **Incentivizes cooperation:** Nodes are incentivized to actively participate in the federated learning process and maintain high-quality contributions, as their verification weights depend on their contributions. This encourages more nodes to join the network, increasing the overall performance and security of the system.
- **Enhanced security:** FRC improves the security of the network by considering node reliability in the weight calculation. This reduces the likelihood of a malicious node gaining control over the consensus process.
- **Privacy-preserving:** As FRC is designed for federated learning, it inherently preserves data privacy by sharing only model parameters and not the raw data. This is particularly important in the context of person re-identification, where sensitive personal information is involved.

The Federated Reputation Consensus protocol offers a unique approach to consensus in federated learning environments. Unlike traditional consensus mechanisms such as Proof of Work or Proof of Stake, FRC is designed to accommodate the specific characteristics

and requirements of federated learning. PoW, used by Bitcoin, requires nodes to solve complex mathematical problems, which is resource-intensive and energy-inefficient. PoS, used by Ethereum 2.0, allocates verification rights based on the number of tokens held by a node, which may lead to centralization issues. In contrast, the FRC protocol operates by taking into account the quality of nodes in the network and allocates verification tasks based on their contributions to the learning process. This encourages active participation, creates a more energy-efficient and scalable network, and ensures a more robust federated learning process. Furthermore, FRC provides greater privacy preservation, a critical requirement in federated learning where sensitive data are often involved. By keeping data on local devices and only sharing model updates, FRC reduces the risk of data leakage during the learning process. Particularly in the context of person re-identification, where privacy concerns are paramount, the FRC protocol can offer a more secure, scalable, and efficient solution compared to traditional consensus mechanisms. Its ability to encourage participation and ensure data privacy while maintaining the efficiency and scalability of the learning process makes it an attractive choice for federated learning applications.

4. Evaluation

4.1. Experimental Setup

We implement the Fed-UAV in Python, utilizing the EasyFL library [26] built on the PyTorch framework [27]. As shown in Table 2, we employ the VIPeR [28], CUHK01 [29], 3DPeS [30], and PKU-Reid [31] datasets for training purposes. These datasets encompass multiple camera views, which effectively mimic the process of gathering data from various cameras in real-world scenarios. Furthermore, we conduct experiments using an AMD 5800h CPU and NVIDIA® 3070 8G GPU setup. Model aggregation and updates are executed via the PyTorch NVIDIA Collective Communications Library. Throughout the experiments, we assess both local and global models in real time. Ultimately, we present the optimal performance achieved for each dataset across all rounds.

Table 2. Person ReID datasets.

Dataset	Release Time	# Identities	# Cameras	# Images	Label Method
VIPeR [19]	2007	632	2	1264	Hand
CUHK01 [20]	2012	971	2	3884	Hand
3DPeS [21]	2011	192	8	1011	Hand
PKU-Reid [22]	2016	114	2	1824	Hand

4.2. Performance Evaluation

In this evaluation, we explore the performance optimization of federated person re-identification through benchmark analysis in blockchain-enabled smart UAV delivery systems. We customize the FedReIDBench [32] as our benchmark, which serves as a comprehensive framework for evaluating different aspects of federated person re-identification systems.

In our work, we have chosen four datasets for our evaluation: the VIPeR, CUHK01, 3DPeS, and PKU-Reid datasets. Each of these datasets represents different federated scenarios, embodying various complexities and data distribution characteristics, and enables us to evaluate the robustness and adaptability of the proposed federated learning system under diverse conditions. However, it's also important to establish a connection between these datasets and real-world UAV applications; whereas these datasets provide invaluable insights, their practical implications are contingent on the correlation between the type of images they encompass and the ones procured in actual UAV applications. To ensure this, we have curated the datasets to resemble, as closely as possible, the image data that would be collected in realistic UAV deployments. By doing so, we are better able to evaluate the viability of our proposed system in genuine operational settings and derive meaningful results. More information on the precise nature of the images within these datasets, their alignment with real-world UAV application imagery, and how this influences our findings will be addressed in the detailed dataset descriptions in the subsequent sections.

As shown in Figures 3–6, by testing these datasets, we find that incorporating blockchain technology does not negatively impact the system's performance. On the contrary, the integration of blockchain technology, such as Ethereum's permissioned chain, provides an additional layer of security and privacy to the federated learning process, ensuring that the model parameters and the identities of the parties involved remain confidential.

As shown in Figures 3 and 4, our system demonstrates consistent performance across all datasets. We measured performance using metrics such as R1-ranking accuracy and permissioned chain throughput, which shed light on the system's ability to correctly identify individuals and its overall performance in the federated person re-identification task.

In Figure 5, we present the effect of incorporating blockchain technology into our system. The results show that the use of Ethereum's permissioned chain does not negatively impact the system's performance. Instead, it enhances security and privacy by providing a layer of confidentiality for model parameters and the identities of the parties involved in the federated learning process.

Finally, Figure 6 illustrates the scalability of our approach. Despite the additional computational overhead introduced by the blockchain, our system maintains its performance even when the number of participants increases, demonstrating its potential for large-scale federated learning applications.

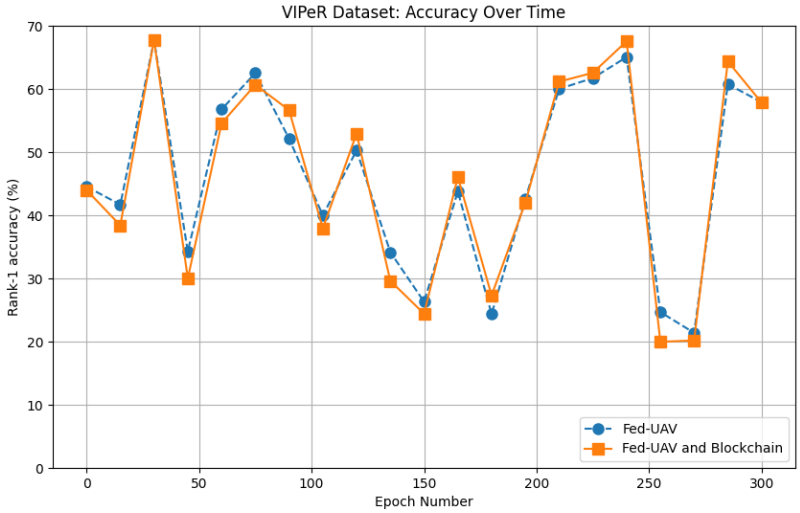

Figure 3. VIPeR dataset: accuracy over time.

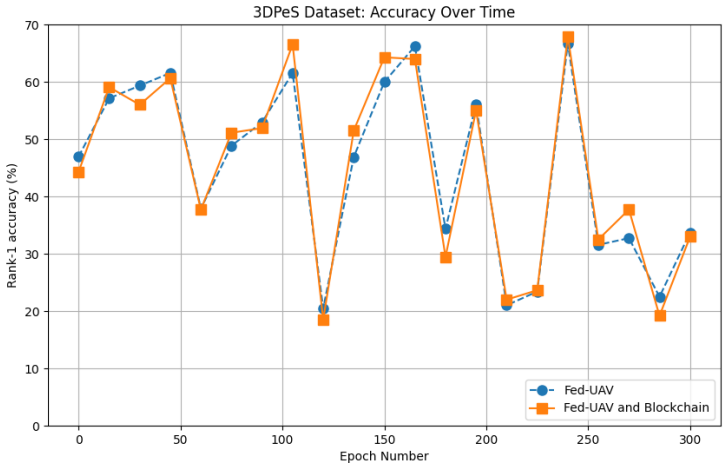

Figure 4. 3DPeS dataset: accuracy over time.

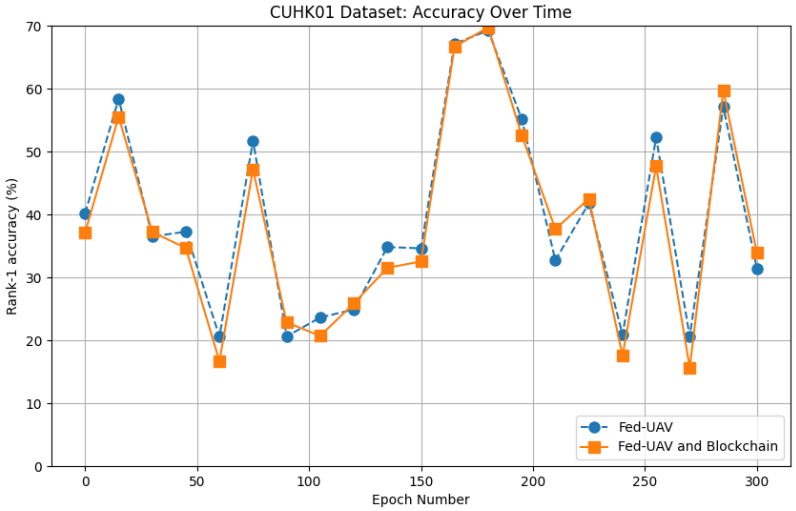

Figure 5. CUHK01 dataset: accuracy over time.

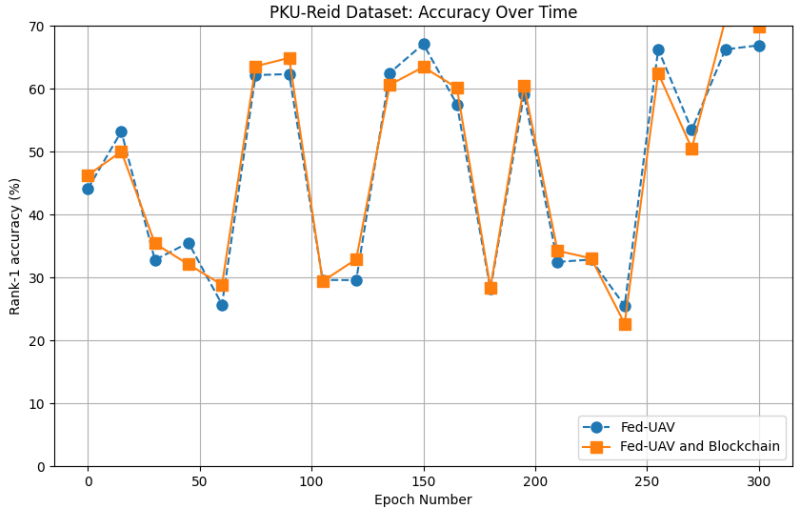

Figure 6. PKU-Reid dataset: accuracy over time.

To conduct the evaluation, we consider several factors, including the model structure, federated training algorithms, performance metrics, and reference implementations. The choice of the model structure is critical, as it determines the learning capacity and computational requirements of the federated learning system. The federated training algorithms play a vital role in the learning process, directly influencing the convergence rate and final performance of the global model. In our evaluation, we analyze various federated training algorithms, considering factors such as communication efficiency, scalability, and robustness against potential attacks.

For the model architecture, we utilized a deep learning approach specifically tailored for person re-identification tasks. The model architecture is based on a convolutional neural network (CNN), with several modifications to accommodate the unique challenges of person re-identification, such as handling variations in pose, lighting, and occlusion. The architecture consists of multiple layers of convolutions, batch normalization, and ReLU activations, followed by a fully connected layer for feature extraction. The extracted features are then used to compute a similarity score between different individuals in the dataset.

As for the federated training algorithms, we leveraged Federated Averaging (FedAvg), a popular algorithm for federated learning environments. FedAvg works by training the model on local data on each client and then sending the model updates to a central server. The server then averages these updates to produce a global model, which is sent back to the clients for the next round of training. This process is repeated for several rounds

until the model converges. This algorithm is particularly suitable for our setup, as it reduces the need for data transmission, thereby preserving data privacy and reducing communication overhead.

In our experiments, we also experimented with several variations of the FedAvg algorithm, including Federated Stochastic Gradient Descent (FedSGD) and Federated Adam. These algorithms offer different trade-offs in terms of convergence speed, communication efficiency, and robustness against non-IID data, allowing us to assess the performance of the federated learning system under different conditions.

Performance metrics are essential for quantifying the effectiveness of the proposed method. We employ several metrics to evaluate the system's performance, including R1-ranking accuracy [32] and permissioned chain throughput. These metrics provide insights into the system's ability to correctly identify individuals in the given datasets and its overall performance in the federated person re-identification task.

Lastly, we consider reference implementations that serve as a baseline for our evaluation. By comparing the performance of our proposed federated learning system with these reference implementations, we can identify the strengths and weaknesses of our approach and determine potential areas for improvement.

Our evaluation of the performance optimization of federated person re-identification through benchmark analysis in blockchain-enabled smart UAV delivery systems provides valuable insights into the effectiveness and efficiency of the proposed federated learning system. By considering various datasets, federated scenarios, model structures, federated training algorithms, performance metrics, and reference implementations, we ensure a comprehensive assessment of the system's performance. Moreover, the integration of blockchain technology not only maintains the performance but also enhances the security and privacy of the federated learning process, paving the way for future optimizations and enhancements in the context of secure and privacy-preserving machine learning.

4.3. Permissioned Chain throughput Evaluation

As shown in Algorithm 2, this algorithm describes the process for calculating the throughput of a blockchain system. The throughput is the number of transactions that the system can process per unit of time. Here is a brief explanation of each variable and symbol used in the algorithm:

$\mathcal{B}$: Represents the blockchain, which is a distributed ledger consisting of a series of blocks. Each block contains a set of transactions. $\mathcal{T}$: Represents the set of transactions that need to be processed and added to the blockchain. $\mathcal{P}$: Represents the set of peers or nodes participating in the blockchain network. These nodes are responsible for validating transactions, mining new blocks, and maintaining the integrity of the distributed ledger. t_p: Represents the transaction processing time, which is the time it takes for a node to validate and process a single transaction. t_m: Represents the block mining time, which is the time it takes for a node to mine (i.e., create and validate) a new block and add it to the blockchain. T: Represents the transaction throughput, which is the measure of how many transactions the blockchain system can process per unit of time. This algorithm takes into account the time required to process each transaction and the time required to mine a block containing these transactions. By calculating the transaction throughput, we can assess the efficiency and performance of a blockchain system.

We evaluate the throughput of the Ethereum Permissioned Chain with FRC Consensus Protocol. The throughput is a measure of how many transactions the system can process per unit of time. A higher throughput indicates better performance and efficiency of the blockchain system.

As shown in Figure 7, this figure shows the throughput evaluation for different combinations of the number of nodes and transaction rates, considering the quality factor for each sample. It helps to identify trends and potential bottlenecks in the performance of the Ethereum Permissioned Chain with the FRC Consensus Protocol. By analyzing the plot,

we derive insights into how these factors influence the throughput and overall performance of the system.

Algorithm 2 Blockchain Throughput

$\mathcal{B} \leftarrow$ Blockchain
$\mathcal{T} \leftarrow$ Transactions
$\mathcal{P} \leftarrow$ Peers
$t_p \leftarrow$ Transaction processing time
$t_m \leftarrow$ Block mining time
$T \leftarrow$ Transaction throughput
function COMPUTETHROUGHPUT($\mathcal{B}, \mathcal{T}, \mathcal{P}, t_p, t_m$)
    $n_m \leftarrow$ Number of miners in $\mathcal{P}$
    $s \leftarrow$ Block size
    $T \leftarrow \frac{s}{t_p + t_m} \times n_m$ **return** T

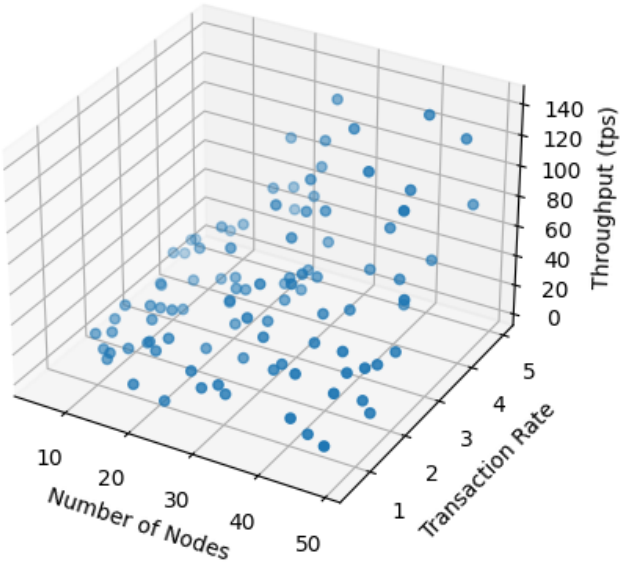

Figure 7. Throughput evaluation of Ethereum Permissioned Chain with FRC consensus protocol.

In the Performance Optimization of Federated Person Re-identification via Benchmark Analysis in Blockchain-Enabled Smart UAV Delivery Systems, blockchain technology plays a crucial role in providing security, privacy, and trust among the participants. Ethereum's permissioned chain, along with the FRC Consensus Protocol, offers a decentralized and secure platform for the federated learning process, mitigating the risk of a single point of failure and ensuring the privacy of the model parameters and identities of the parties involved.

The evaluation of throughput is essential to understand how the integration of blockchain technology can impact the performance of the federated learning process. By analyzing the throughput, we identify potential areas for optimization and suggest improvements that can enhance the performance of the system while maintaining its security and privacy. Additionally, the evaluation provides insights into the optimal network configuration, consensus parameters, and smart contract settings to achieve the desired throughput and performance for federated person re-identification in blockchain-enabled smart UAV delivery systems.

Our proposed system, although promising, does have certain limitations. Firstly, the current approach relies heavily on the quality and diversity of the datasets used for training. If the data are not representative of real-world scenarios, the performance of the person re-identification task could be compromised.

Second, whereas federated learning and the use of blockchain add layers of privacy and security, they also introduce additional computational and communication overhead. The trade-off between privacy and efficiency is a challenge that we faced during the implementation of the system.

Third, the current model architecture and federated training algorithm, though effective, may not be the most optimal for all scenarios. Exploring different model architectures and training algorithms could potentially improve the system's performance.

Finally, there are inherent challenges in person re-identification tasks such as variations in lighting, pose, and occlusion, which can affect the performance of the system. Our current approach attempts to mitigate these factors, but they remain significant challenges in the field.

5. Conclusions and Future Work

In conclusion, our paper presents an optimized federated person re-identification approach through benchmark analysis in blockchain-enabled smart UAV delivery systems. The unique advantage of integrating Ethereum's permissioned chain with the FRC Consensus Protocol into the federated learning process is displayed, illustrating enhanced security, privacy, and trust for person re-identification tasks. To validate our model, we relied on real-world datasets, highlighting the effects of various parameters on the performance of our blockchain-integrated federated learning system. The evaluation results suggest that our system successfully upholds its initial accuracy while augmenting security and privacy. We introduced the FRC protocol to address scalability issues and support the demands of smart UAV delivery systems. Our experiments focused on energy efficiency, confirmation time, and throughput, showcasing the effectiveness of our approach. Furthermore, we analyzed the impact of the incentive mechanism on system performance and the resiliency of our solution under various security attacks. Our study provides valuable insights that can guide future research and development efforts in the rapidly evolving field of smart UAV delivery systems and federated person re-identification.

In regards to the future work, we propose the following research directions:

- Exploring and integrating advanced security mechanisms, such as zero-knowledge proofs or secure multi-party computation, can further enhance the privacy and security of the federated learning process.
- Researching methods to enable interoperability between different blockchain platforms and federated learning systems can promote collaboration and expand the range of applications in various industries.

Author Contributions: Conceptualization, F.J., S.C., L.P. and X.L.; methodology, C.D.; software, C.D. and J.Z.; validation, C.D., J.Z. and Q.A.; investigation, C.D.; writing—original draft preparation, C.D.; writing—review and editing, F.J., L.P. S.C. X.L.; visualization, C.D., J.Z. and Q.A.; supervision, F.J., S.C. and X.L.; project administration, F.J., S.C. and X.L.; funding acquisition, S.C. and X.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially supported by CSIRO (Commonwealth Scientific and Industrial Research Organisation) scholarship project — "Build AI into Edge Computing with Blockchain".

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Feng, C.; Liu, B.; Yu, K.; Goudos, S.K.; Wan, S. Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3582–3592. [CrossRef]
2. Beer, K.; Bondarenko, D.; Farrelly, T.; Osborne, T.J.; Salzmann, R.; Scheiermann, D.; Wolf, R. Training deep quantum neural networks. *Nat. Commun.* **2020**, *11*, 808. [CrossRef] [PubMed]
3. Yan, K.; Liu, L.; Xiang, Y.; Jin, Q. Guest editorial: AI and machine learning solution cyber intelligence technologies: New methodologies and applications. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6626–6631. [CrossRef]

4. Zhou, M.G.; Cao, X.Y.; Lu, Y.S.; Wang, Y.; Bao, Y.; Jia, Z.Y.; Fu, Y.; Yin, H.L.; Chen, Z.B. Experimental quantum advantage with quantum coupon collector. *Research* **2022**, *2022*, 9798679. [CrossRef] [PubMed]
5. Sharma, K.; Cerezo, M.; Cincio, L.; Coles, P.J. Trainability of dissipative perceptron-based quantum neural networks. *Phys. Rev. Lett.* **2022**, *128*, 180505. [CrossRef] [PubMed]
6. Zhou, M.G.; Liu, Z.P.; Yin, H.L.; Li, C.L.; Xu, T.K.; Chen, Z.B. Quantum Neural Network for Quantum Neural Computing. *Research* **2023**, *6*, 134. [CrossRef]
7. Pokhrel, S.R.; Choi, J. Federated Learning With Blockchain for Autonomous Vehicles: Analysis and Design Challenges. *IEEE Trans. Commun.* **2020**, *68*, 4734–4746. [CrossRef]
8. Zhang, C.; Liu, X.; Xu, J.; Chen, T.; Li, G.; Jiang, F.; Li, X. An Edge Based Federated Learning Framework for Person Re-Identification in UAV Delivery Service. In Proceedings of the 2021 IEEE International Conference on Web Services (ICWS), Chicago, IL, USA, 5–10 September 2021; pp. 500–505.
9. Khan, M.A.; Ullah, I.; Alkhalifah, A.; Rehman, S.U.; Shah, J.A.; Uddin, M.I.; Alsharif, M.H.; Algarni, F. A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3416–3425. [CrossRef]
10. Nguyen, D.C.; Pham, Q.V.; Pathirana, P.N.; Ding, M.; Seneviratne, A.; Lin, Z.; Dobre, O.; Hwang, W.J. Federated learning for smart healthcare: A survey. *ACM Comput. Surv.* **2022**, *55*, 1–37. [CrossRef]
11. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H. Federated learning for drone authentication. *Hoc Netw.* **2021**, *120*, 102574. [CrossRef]
12. Pokhrel, S.R. Blockchain brings trust to collaborative drones and leo satellites: An intelligent decentralized learning in the space. *IEEE Sensors J.* **2021**, *21*, 25331–25339. [CrossRef]
13. Pokhrel, S.R. Federated Learning Meets Blockchain at 6G Edge: A Drone-Assisted Networking for Disaster Response. In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, New York, NY, USA, 25 September 2020; pp. 49–54.
14. Ch, R.; Srivastava, G.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S. Security and privacy of UAV data using blockchain technology. *J. Inf. Secur. Appl.* **2020**, *55*, 102670. [CrossRef]
15. Khan, A.A.; Khan, M.M.; Khan, K.M.; Arshad, J.; Ahmad, F. A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs. *Comput. Netw.* **2021**, *196*, 108217. [CrossRef]
16. Kumar, P.; Kumar, R.; Kumar, A.; Franklin, A.A.; Jolfaei, A. Blockchain and Deep Learning Empowered Secure Data Sharing Framework for Softwarized Uavs. In Proceedings of the 2022 IEEE International Conference on Communications Workshops (ICC Workshops), Seoul, Republic of Korea, 16–20 May 2022; pp. 770–775.
17. Liu, B.; Yu, K.; Feng, C.; Choo, K.K.R. Cross-Domain Authentication for 5G-Enabled UAVs: A Blockchain Approach. In Proceedings of the 4th ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, Online, 29 October 2021; pp. 25–30.
18. Gupta, R.; Nair, A.; Tanwar, S.; Kumar, N. Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges. *IET Commun.* **2021**, *15*, 1352–1367. [CrossRef]
19. Silva, S.H.; Rad, P.; Beebe, N.; Choo, K.K.R.; Umapathy, M. Cooperative unmanned aerial vehicles with privacy preserving deep vision for real-time object identification and tracking. *J. Parallel Distrib. Comput.* **2019**, *131*, 147–160. [CrossRef]
20. Grigorev, A.; Liu, S.; Tian, Z.; Xiong, J.; Rho, S.; Feng, J. Delving deeper in drone-based person re-id by employing deep decision forest and attributes fusion. *ACM Trans. Multimed. Comput. Commun. Appl.* **2020**, *16*, 1–15. [CrossRef]
21. Nguyen, T.; Katila, R.; Gia, T.N. A Novel Internet-of-Drones and Blockchain-Based System Architecture for Search and Rescue. In Proceedings of the 2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS), Denver, CO, USA, 4–7 October 2021; pp. 278–288.
22. Jensen, I.J.; Selvaraj, D.F.; Ranganathan, P. Blockchain Technology for Networked Swarms of Unmanned Aerial Vehicles (UAVs). In Proceedings of the 2019 IEEE 20th International Symposium on A World of Wireless, Mobile and Multimedia Networks, Washington, DC, USA, 10–12 June 2019; pp. 1–7.
23. Xu, X.; Zhao, H.; Yao, H.; Wang, S. A blockchain-enabled energy-efficient data collection system for UAV-assisted IoT. *IEEE Internet Things J.* **2020**, *8*, 2431–2443. [CrossRef]
24. Psaras, Y.; Dias, D. The Interplanetary File System and the Filecoin Network. In Proceedings of the 2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S), Valencia, Spain, 29 June–2 July 2020; p. 80.
25. Fang, C.; Guo, Y.; Ma, J.; Xie, H.; Wang, Y. A privacy-preserving and verifiable federated learning method based on blockchain. *Comput. Commun.* **2022**, *186*, 1–11. [CrossRef]
26. Zhuang, W.; Gan, X.; Wen, Y.; Zhang, S. Easyfl: A low-code federated learning platform for dummies. *IEEE Internet Things J.* **2022**, *9*, 13740–13754. [CrossRef]
27. Ahmed, K.; Li, T.; Ton, T.; Guo, Q.; Chang, K.W.; Kordjamshidi, P.; Srikumar, V.; Van den Broeck, G.; Singh, S. PYLON: A PyTorch Framework for Learning with Constraints. In Proceedings of the NeurIPS 2021 Competitions and Demonstrations Track, Online, 6–14 December 2022; pp. 319–324.
28. Monroe, M.E.; Tolić, N.; Jaitly, N.; Shaw, J.L.; Adkins, J.N.; Smith, R.D. VIPER: An advanced software package to support high-throughput LC-MS peptide identification. *Bioinformatics* **2007**, *23*, 2021–2023. [CrossRef]

29. Wu, S.; Chen, Y.C.; Li, X.; Wu, A.C.; You, J.J.; Zheng, W.S. An Enhanced Deep Feature Representation for Person Re-Identification. In Proceedings of the 2016 IEEE Winter Conference on Applications of Computer Vision (WACV), Lake Placid, NY, USA, 7–10 March 2016; pp. 1–8.
30. Baltieri, D.; Vezzani, R.; Cucchiara, R. 3dpes: 3d People Dataset for Surveillance and Forensics. In Proceedings of the 2011 Joint ACM Workshop on Human Gesture and Behavior Understanding, Scottsdale, AZ, USA, 28 November–1 December 2011; pp. 59–64.
31. Zhou, R.; Chang, X.; Shi, L.; Shen, Y.D.; Yang, Y.; Nie, F. Person Reidentification via Multi-Feature Fusion with Adaptive Graph Learning. *IEEE Trans. Neural Netw. Learn. Syst.* **2019**, *31*, 1592–1601. [CrossRef] [PubMed]
32. Zhuang, W.; Wen, Y.; Zhang, X.; Gan, X.; Yin, D.; Zhou, D.; Zhang, S.; Yi, S. Performance Optimization of Federated Person Re-Identification via Benchmark Analysis. In Proceedings of the 28th ACM International Conference on Multimedia, Seattle, WA, USA, 12–16 October 2020; pp. 955–963.