applied sciences

MDPI

Article

Identity Management and Authentication of a UAV Swarm Based on a Blockchain

Pengbin Han [1], Aina Sui [1] and Jiang Wu [2,*]

[1] School of Computer and Cyber Sciences, Communication University of China, Beijing 100024, China
[2] School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, China
* Correspondence: blockchaincyber@163.com

Abstract: In recent years, with the continuous development of UAV technology, the application of the UAV swarm in the military has been a global focus of research. Although it can bring a series of benefits in autonomous cooperation, the traditional UAV management technology is prone to hacker attacks due to many security issues, such as a single point of failure brought by centralized management and the lack of reliable identity authentication. This paper studies the advantages and the recent advances of the blockchain in UAV swarm, proposes a blockchain-based UAV swarm identity management model (B-UIM-M), and establishes a distributed identity authentication scheme based on the distributed identity identifier (DID) under this model. Moreover, to ensure the safe transmission of UAV communication data, a secure communication architecture based on blockchain and a set of secure transmission protocols were designed, combined with cryptography. In the current military field, there is no similar application case of the UAV swarm identity management model and distributed identity authentication. The feasibility and security of the proposed scheme are proved through experiments and security analyses.

Keywords: blockchain; UAV swarm; identity management; secure communication; distributed identity authentication

check for updates

Citation: Han, P.; Sui, A.; Wu, J. Identity Management and Authentication of a UAV Swarm Based on a Blockchain. *Appl. Sci.* **2022**, *12*, 10524. https://doi.org/10.3390/app122010524

Academic Editors: Nadejda Komendantova and Hossein Hassani

Received: 17 September 2022
Accepted: 17 October 2022
Published: 18 October 2022

1. Introduction

UAV swarm means that multiple UAVs with limited autonomous abilities can achieve a higher degree of autonomous cooperation through information communication without centralized command and control. Drones, also known as unmanned aerial vehicles (UAVs) or flying robots (FRs), are aerial devices that are equipped with sensors, processors, and wireless connectivity [1]. Due to their advantages of high mobility, low costs, and on-demand deployment, they are widely used in many fields, such as civil, military, logistics, industrial, commercial, agricultural surveillance, smart city, and rescue [2–5]. The versatility of UAVs also shows that the robustness and security of their system are critical [6,7].

1.1. Security Issues Faced by UAV Swarm

Drones were originally used in the commercial field and have already achieved many good results, for example, Amazon has announced the benefits of integrating drones and related technologies into their existing delivery system, which has enhanced its rate of delivery [8,9]. In recent years, the application of UAVs in the military has become an important research topic. Many UAV research projects were launched by American technology institutes, such as the Defense Advanced Research Projects Agency's "Gremlins" UAV Swarm Project and the US Naval Research Office's "Low-Cost UAV Swarm" project. Moreover, the European Defense Agency launched the European Swarm project in November 2016 to develop key technologies, such as autonomous mission decision-making and collaborative navigation for UAV swarms [10]. While drones have excellent combat capabilities, they also attract hackers attempting to break into them. In UAV swarm warfare, communication between UAVs is the main target of attack [11,12]. A study by [13] indicates that many IoT (Internet of Things) devices lack basic security considerations, and the UAV swarm is no exception. In general, the risks faced by a UAV swarm mainly include the following.

- Single point of risk brought by centralized management. At present, numerous UAV systems mainly adopt aerial- or ground-layered methods to control UAVs, which are highly centralized. When the management node is destroyed or taken over by the enemy, the control of the entire UAV network will become invalid, affecting the flight and operation of UAVs [14–16];
- The lack of reliable authentication mechanisms. Some software bugs or insecure settings may be exploited by enemy drones to invade [17,18]. However, the current drone systems lack reliable identity authentication, which makes it difficult to ensure the authentication and data reliability between UAV nodes;
- Communication link interference and data tampering risk. UAV swarm generally transmits data through wireless channels. The unreliability of the wireless communication environment will seriously affect the interaction between nodes [19–21]. At the same time, the UAV terminal capacity is insufficient, and traditional encryption technology and data storage are difficult to use on drone equipment. So, UAVs are particularly vulnerable and tamper-proof, and there is a risk of wireless link monitoring and data theft;
- Difficulty managing drones belonging to different agencies. In typical military applications, it is sometimes necessary for multiple agencies to jointly execute a combat mission. Due to the different management methods, management platforms, and identity authentication methods of different parts, the management of UAVs belonging to different agencies is difficult.

In summary, it is crucial to maintain the communication security between UAVs, realize the reliable identity management of UAVs, and the identity authentication of UAVs between different agencies. The emergence of blockchain technology provides a possible solution to the above problems [22–26]. Blockchain was first applied in decentralized virtual currency [27]. After several years of development, it plays an essential role in many fields, for example, finance, trade, the Internet of Things, medical care, renewable energy, smart cities, social media, copyright protection, etc. [28–34].

1.2. Blockchain and Related Work

The security of the blockchain relies on a consensus mechanism rather than a trusted third party [35]. For the Bitcoin system, as long as more than 25% of the miners are honest, its security and trust can be guaranteed [36]. Each block is linked by a hash value, and the content of previous blocks can be traced from the last block. All stored information is managed by all participating nodes or several authoritative nodes. More importantly, any change in block data will affect all subsequent blocks [37]. Due to the tamper-proof, distributed, and trusted advantages of the blockchain, it is combined with UAV in the military, aiming to solve some risks faced by UAV systems [38,39].

So far, the application of the blockchain in UAV systems was extensively explored by researchers. To improve the privacy and security of UAV equipment, Ch et al. [8] proposed a blockchain-based solution that stores some data on Ethereum, but there is no mention of how to manage the drone's identity and how to transmit data securely. Blockchain-based federated learning in UAVs beyond 5G networks was studied by Saraswat et al. [14], who focused on the privacy and security of UAVs in open channels. However, the identity management and authentication of UAVs were not studied in depth. For secure communication and network management, Kumari et al. [40] proposed a software architecture of UAV supporting blockchain, which makes use of the distributed and tamper-proof advantages of blockchain to store data. A method to realize the privacy and security of drones using blockchain is proposed by Rana et al. [41], in which interactions between UAVs and other entities are secured only by encryption. To solve the security and privacy issues of UAV data, Lv et al. [42] studied a privacy protection method for UAV big data based on blockchain technology, but ignored how to ensure that the identities between UAVs are trustworthy to each other. Jensen et al. [43] studied a method for UAV identity authentication, issuing a set of x.509 certificates to each drone and storing these certificates on the blockchain. Liang et al. [44] explored the combination of drones, blockchain, and cloud services, where complex computations are performed by cloud services, and the blockchain stores some key information. However, there is no mention of how to ensure that cloud services, drones, and blockchain can be trusted with each other. Rodríguez-Molina et al. [45] proposed a method of secure data transmission based on a blockchain but did not study how to implement UAV identity management and authentication. A blockchain-based secure system architecture was studied by Kuzmin and Znak [46], in which drones act as nodes in a blockchain network. Ge et al. [47] designed a distributed scheme of UAVs based on blockchain technology, but it was only limited to the design of a lightweight structure of blockchain and the secure storage of data.

Although the above studies proposed some constructive methods, some problems are still ignored. The nodes in the blockchain network need to frequently synchronize transaction data while using UAV with the limited computing power as a node is currently impractical. In addition, most of the above studies only focused on the security of UAV data storage, and rarely studied the security of data transmission. More importantly, there is a lack of a safe identity management model and reliable identity authentication for drone swarms belonging to different institutions. It was also proposed by Mehta et al. [48] that identity authentication will play an important role in future 5G communication. Although Jensen et al. [43]. proposed an identity authentication method, it is still limited to the public key infrastructure (PKI) system and lacks a set of secure and reliable communication protocols. The following Table 1 provides a summary of recent studies conducted using blockchain technologies.

Table 1. Summary of literature survey.

Author	Secure Data Transmission	Distributed Identity Authentication	Type	Identity Information Management	Designed/ Implemented
[8]	No	No	Public blockchain	No	Designed and implemented
[14]	Yes	No	Consortium blockchain	No	Designed and implemented
[40]	No	No	Public blockchain	No	Designed and implemented
[41]	No	No	Public blockchain	No	Only designed
[42]	No	No	Not specified	No	Only designed
[43]	No	No	Not specified	No	Designed and implemented
[44]	No	No	Consortium blockchain	No	Only designed
[45]	Yes	No	Consortium blockchain	No	Designed and implemented
[46]	No	No	Not specified	No	Designed and implemented
[47]	Yes	No	Not specified	No	Only designed
Proposed	Yes	Yes	Consortium blockchain	Yes	Designed and implemented

As can be seen from Table 1, the research on the integration of blockchain in UAV identity management and authentication is still very limited. To solve the problems faced by drone swarms, this paper proposes a new drone identity management model B-UIM-M; we designed a blockchain-based distributed identity authentication scheme based on this model. In addition, to ensure the secure transmission of data, a secure communication architecture based on blockchain and a set of secure transmission protocols were designed.

The rest of the paper is organized as follows. Section 2 introduces the blockchain-based UAV identity management model in detail, the specific details of the distributed identity authentication method and secure communication are discussed in Section 3, and Section 4 presents the performance evaluation of the proposed scheme. The security of the study is analyzed in Section 5, while Section 6 concludes the paper.

2. Blockchain-Based UAV Swarm Identity Management Model

At present, the management of drones is centralized by the owner of the drones. This centralized management often brings some problems, such as a single point of failure. Once the management node fails, all UAVs belonging to it may be invaded. Moreover, each agency has its own management scheme, which leads to great differences in the management systems. As the swarms of drones that perform tasks collaboratively by multiple agencies continue to expand, which greatly increases the difficulty of drone management and the authentication of drones from different agencies to each other. The identity authentications of almost all systems adopt PKI systems. A centralized third-party organization issues digital certificates for participating nodes, which contain the entity's public key and related identity information. These certificates establish the association between entity identity information and its public key and are transmitted publicly in the network. Although the PKI system can complete identity authentication, the following problems still exist.

- The authentication process of the digital certificate is cumbersome. The OCSP (online certificate status protocol) must be asked for each verification of digital certificates, and it needs to update the CRL (certificate revocation list) signed by the CA (certificate authority);
- The identity of the UAV is centrally managed by the owners of the drones or some trusted third parties, which often has a single point of failure and leads to the disclosure of UAV identity information.

Therefore, a blockchain-based UAV identity management model (B-UIM-M) is proposed. Using blockchain to manage UAV identity information avoids the single point of failure caused by centralized management and provides distributed identity authentication for UAVs of different agencies so that their identity authentications are no longer dependent on trusted third parties. This model is mainly divided into two layers. The first layer manages the UAV-owning organizations to ensure mutual trust between them, and the second layer manages UAVs to ensure that UAVs belonging to different organizations can verify each other's identities. The details are shown in Figure 1.

In Figure 1, DID_O and DID_U are the DIDs of the UAV owners and the UAVs, respectively. Moreover, SK_O and SK_U separately represent the private keys of UAV owners and UAVs, $O = 1, 2, \ldots\ldots, n$, $U = 1, 2, \ldots\ldots, k$. The DID document is mainly used to store the identity information of UAV owners and UAVs. Identity information distributed to them can be transmitted through physical media, and identity information stored on the blockchain can be transmitted through secure protocols.

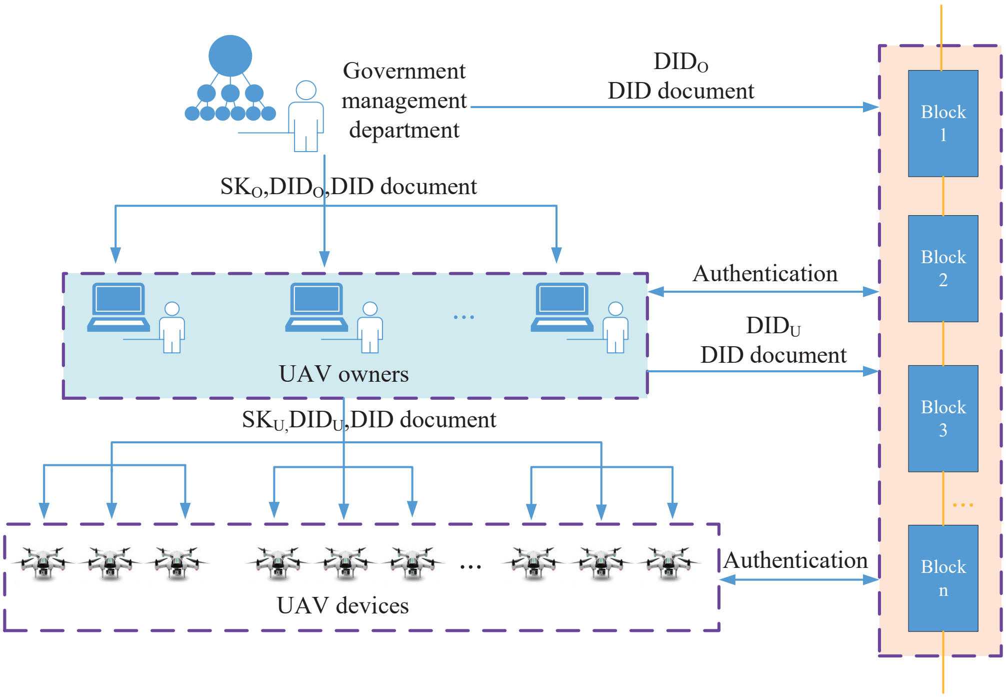


Figure 1. Blockchain-based UAV identity management model.

In B-UIM-M, a blockchain-based identity information distribution process is proposed. First, the government management department generates identity information for the UAV owners uniformly, and this identity information is distributed to the corresponding UAV owners after tamper-proof storage by blockchain. The identity information of government management departments must be authenticated and stored by blockchain. The drone owner generates identity information for the drone when it is registered. Similarly, the identity information is distributed to the corresponding drone after tamper-proof storage by the blockchain. The specific process of identity information distribution is shown in Figure 2.

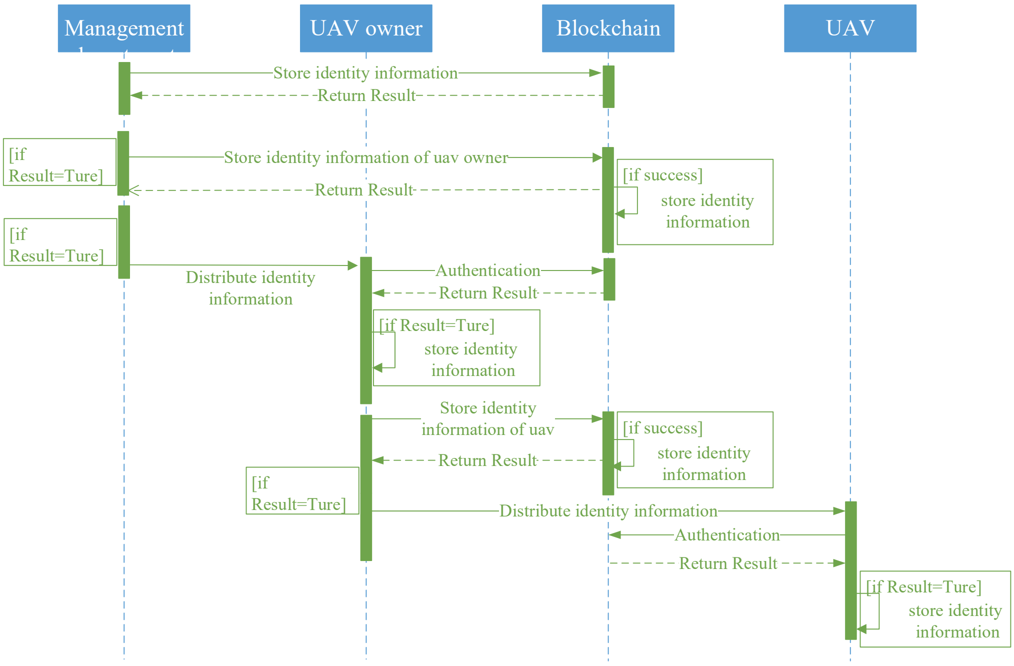

Management
UAV owner
Blockchain
UAV
Store identity information
Return Result
[if Result=Ture]
Store identity information of uav owner
Return Result
[if success]
store identity information
[if Result=Ture]
Distribute identity information
Authentication
Return Result
[if Result=Ture]
store identity information
Store identity information of uav
Return Result
[if success]
store identity information
[if Result=Ture]
Distribute identity information
Authentication
Return Result
[if Result=Ture]
store identity information

Figure 2. Blockchain-based identity information distribution processing.

To ensure the authenticity and credibility of the identity information, after the drone owner and the drone respectively obtain the identity information, they will request the blockchain for the following verification.

- Whether the identity information has been successfully stored in the blockchain;
- Whether the identity information distribution agency is credible, i.e., whether its identity information has been tamper-proof–stored by the blockchain.

To ensure the authenticity and credibility of the stored information send by sending agency (including government management department and UAV owners), the blockchain will perform the following verifications after receiving it.

- Whether the identity information of the sending agency is credible;
- Whether the information is modified during transmission;
- Whether the identity information is distributed by sending agency.

When the UAV owners perform tasks collaboratively, they first authenticate each other's identities through the blockchain, and if the identity authentication is passed, the tasks are performed collaboratively.

In B-UIM-B, a number of security technologies, such as identity distribution, identity verification, data secure transmission, and asymmetric cryptographic algorithm are integrated with blockchain technology for the first time to explore its application in UAV identity management. A blockchain-based identity information distribution process, using a secure transmission protocol to store the identity authentication credentials of the drone owner and the drone on the blockchain to ensure the safety and reliability of drone identity management is proposed. Moreover, a distributed identity authentication scheme is established based on DID and DID documents, which not only avoids the single point of failure and centralized bottleneck problem of CA authentication center in traditional PKI system, but also simplifies the identity authentication process of the UAV by no longer asking OCSP for each identity authentication, and provides a solution for identity authentication between UAVs of different agencies in typical combat scenarios. In the current military field, there is no similar application case of the UAV identity management model and distributed identity authentication.

3. Identity Authentication and Secure Transmission Based on Blockchain

The management model proposed needs to transmit data between blockchain and UAV, and between UAV and UAV. Although blockchain can guarantee the tamper-proof of on-chain data, it cannot guarantee the security of data transmission. Therefore, it is necessary to combine cryptography to realize the secure transmission of data.

3.1. Secure Transmission of UAV Data Based on Blockchain

To solve the security of data transmission, a secure communication architecture based on blockchain is proposed. This architecture is mainly composed of three parts, including the data sender, the data receiver, and the blockchain. In this paper, UAVs are abstracted as data senders, and any devices that communicate with UAVs are abstracted as data receivers, such as ground stations, tactical clouds, and other UAVs in the swarm. Blockchain provides tamper-proof storage of key information, identity management of both communication parties, and distributed identity authentication.

In Figure 3, PK_R indicates the private key of the sender. $AuResult$ represents the result of identity authentication, and $Information_S$ is the communication data. If $AuResult$ = True, the identity authentication is passed, otherwise it fails. When two UAVs want to communicate with each other, the sender requests the public key of the receiver from the blockchain. After receiving the information sent by the sender, the receiver requests the blockchain to authenticate the identity of the sender. Compared with the traditional communication architecture, the innovation of the architecture proposed is that the identity information of communication parties no longer depends on a trusted third party, but is stored by blockchain tamper-proof and their distribution identity authentication is completed by the blockchain.

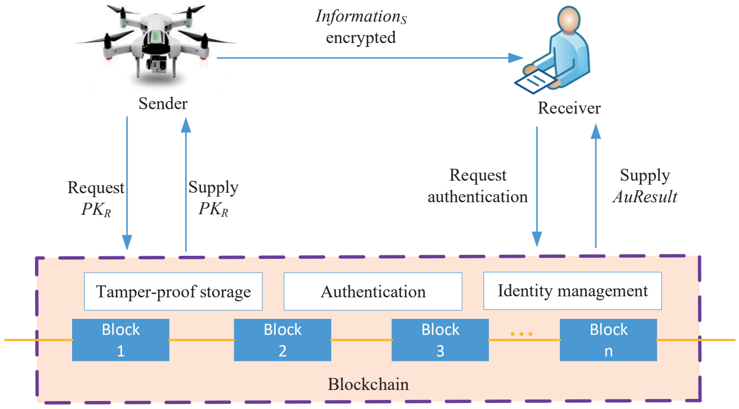


Figure 3. Secure communication architecture based on blockchain.

A reliable and secure communication protocol is proposed based on the above architecture. to prevent attackers from forging and tampering with communication information, this paper also adds the identifier of the drone on the basis of signature encryption to mark the receiver and the sender. In addition, considering the replay attack, all entities will obtain the current time *Timestamp* after receiving the message, and compare it with the time when the message was sent. If the time difference between the two is less than d (the threshold of the time interval from sending the message to receiving the message), the next processing will be executed. Protocol details are as follows.

- The sender sends message;

$$S \rightarrow R/B : C_S = \{E_{PK_R/PK_B}(DID_S, DID_R, E_{SK_S}(Hash(DID_S, DID_R, Timestamp_1, Informations_S/PkRequest)), Timestamp_1, Informations_S/PkRequest)\}$$

where S is sender, B is blockchain, C_S means ciphertext sent by the sender, E_{PK_R} is used to indicate encryption with PK_R, PK_B indicates the public key of the blockchain, SK_S is the private key of the sender, DID_S and DID_R represent the DID of sender and receiver, respectively, $Hash$ represents the function that generates a hash value, $Timestamp_1$ indicates the time when the sender sends the current information, and $PkRequest$ represents the public key request information.

- The receiver requests blockchain for identity authentication;

$$R \rightarrow B : C_R = \{E_{PK_B}(DID_R, DID_S, E_{SK_R}(Hash(DID_R, DID_S, Sign_S, Timestamp_2, AuRequest, M_S)), Sign_S, Timestamp_2, AuRequest, M_S)\}$$

where C_R means ciphertext sent by the receiver, $Sign_S$ indicates the sender's signature, $Timestamp_2$ indicates the time when the request message was sent, $AuRequest$ is the request information of identity authentication, and $M_S = Hash(DID_S, DID_R, Timestamp_1, Informations_S)$ is the hash value of the information sent by the sender.

The receiver will mainly receive two types of information, one is the communication information sent by the sender, and the other is the response information of the blockchain to the identity authentication request. If the received message is C_S, the receiver decrypts it and makes a timestamp comparison. After meeting the conditions, it sends an identity authentication request C_R to the blockchain. In the case of C_B, the receiver decrypts and authenticates the blockchain signature. The detailed processing of the received information is shown in Algorithm 1.

Algorithm 1 Receiver processing information.

```
if information = $C_S$ then then
    $P_S$ = decrypt ($C_S$)
    compare $Timestamp$ and $Timestamp_1$
    send $C_R$
else if information = $C_B$ then then
    $P_B$ = decrypt($C_B$)
    compare $Timestamp$ and $Timestamp_3$
    receive $C_B$
else
    discard data
end if
```

- The blockchain responds to request;

$$B \rightarrow R/S : C_B = \{E_{PK_R/PK_S}(DID_R, DID_S, E_{SK_B}(Hash(DID_R, DID_S, Timestamp_3, AuResult/PK_R)), Timestamp_3, AuResult/PK_R)\}$$

where C_B represents ciphertext sent by the blockchain, PK_S indicates the public key of the sender, SK_B is the private key of the blockchain, $Timestamp_3$ represents the time when the response message was sent.

The blockchain mainly responds to two types of request information, one is the public key request of the sender, and the other is the identity authentication request of the receiver. If the request information is C_S, the blockchain finds the PKR requested public key on the chain and returns the C_B. If it is C_R, the blockchain performs the UAV identity authentication and returns the C_B. The detailed processing of the request information is shown in Algorithm 2.

Algorithm 2 Blockchain processing information.

```
if information = $C_S$ then then
    $P_S$ = decrypt ($C_S$)
    compare $Timestamp$ and $Timestamp_1$
    check $P_S$'s authenticity and authenticate sender's identity
    find $PK_R$ on block
    send $C_B$
else if information = $C_R$ then then
    $P_R$ = decrypt($C_R$)
    compare $Timestamp$ and $Timestamp_2$
    check $P_R$'s authenticity and authenticate receiver's identity
    authenticate sender's identity requested by receiver
    send $C_B$
else
    discard data
end if
```

3.2. UAV Distributed Identity Authentication Scheme Based on Blockchain

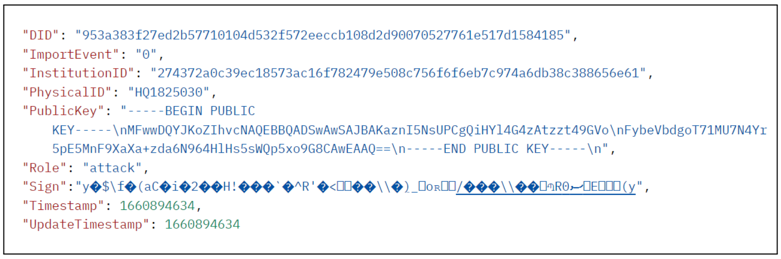
In this paper, the distributed identity authentication based on DID information is established, and the DID document is used to store the identity information of the drone and its owner. The distributed identity authentication of UAVs is uniformly completed by blockchain. The owner of the UAV only generates the identity information for the UAV when it is registered. The identity information received by the blockchain is securely stored on the block after consensus of other nodes in the network. The drone to be authenticated communicates securely with the blockchain to complete distributed identity authentication.

In B-UIM-M, the blockchain stores the DID and DID documents of the drone owner and the drone. For different application scenarios, the content of the DID document may be different. In this paper, the content design of the DID document is shown in Table 2.

Table 2. DID document content.

UAV Owner	UAV
UAV owner DID that identifies the body of DID document	UAV DID that identifies the body of DID document
public key information required for authentication, communication establishment and authorization	public key information required for authentication, communication establishment and authorization
The timestamp of the creation of the DID document	The timestamp of the creation of the DID document
The timestamp when the DID document was last updated	The timestamp when the DID document was last updated
DID of the distribution agency	DID of the distribution agency
Agency name	Physical ID
Records of important events	Role
Integrity proof of the DID document, i.e., the signature of its distribution agency	records of important events
	Integrity proof of the DID document, i.e., the signature of its distribution agency

The DID and DID document are stored on the blockchain in the form of key-value pairs, where DID is the key and DID document is the value.The detailed content is shown in Figure 4.



```
"DID": "953a383f27ed2b57710104d532f572eeccb108d2d90070527761e517d1584185",
"ImportEvent": "0",
"InstitutionID": "274372a0c39ec18573ac16f782479e508c756f6f6eb7c974a6db38c388656e61",
"PhysicalID": "HQ1825030",
"PublicKey": "-----BEGIN PUBLIC
    KEY-----\nMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKaznI5NsUPCgQiHYl4G4zAtzzt49GVo\nFybeVbdgoT71MU7N4Yr
    5pE5MnF9XaXa+zda6N964HlHs5sWQp5xo9G8CAwEAAQ==\n-----END PUBLIC KEY-----\n",
"Role": "attack",
"Sign":"y�$\f�(aC�i�2��H!���`�^R'�<□□��\\�)_□oR□□/���\\��□ᥲR0,⤻□E□□□(y",
"Timestamp": 1660894634,
"UpdateTimestamp": 1660894634
```

Figure 4. DID document stored on the blockchain.

When a drone requests identity authentication, it must provide the blockchain with the DID of the drone to be authenticated, the digital signature, and the hash of the message sent by the drone. The blockchain first finds the DID document from the chain, and returns the identity authentication result after decrypting and verifying the signature. The detailed processing of the identity authentication is shown in Algorithm 3.

Algorithm 3 Identity authentication processing.

Input: identity identifier DID, signature M, and hash value H of sending information
Output: identity authentication result $AuResult$

```
for i = block “1” to block = “n” do
    find DID according to DID document
end for
read public key form DID document
$H \leftarrow$ decrypt($M$)
compare $H$ and $M$
return $AuResult$
```

4. Performance Evaluation

This section mainly evaluates the performance of the proposed scheme. We begin with an introduction of the experimental method and environment, followed by a discussion of the experimental results.

4.1. Experimental Method and Environment

This paper mainly evaluates the influence of the number of drones and the number of blockchain nodes on the public key request time and identity authentication time. In this experiment, the RSA algorithm is used to generate public and private keys for the drone, blockchain, and government management departments. Four Alibaba Cloud servers are used to build the blockchain system. A notebook is used to simulate the UAV owners. The quadrotor UAV model is used in MATLAB for digital UAV simulations. The blockchain system run in Ubuntu 16.0 with 2 GB RAM, and the UAV owners and digital drones run on Windows 10 with a 1.8 GHz AMD Ryzen 7 4800U CPU and 16.0 GB RAM. In the experiment, the Hyperledger Fabric platform developed by IBM is adopted as the underlying development platform of the blockchain system, and the go language is used to develop smart contracts.

4.2. Experimental Settings and Results

In this section, two experiments were set up to complete the performance evaluation described in the previous section. One is the effect of the number of drones on the public key request time and identity authentication time (Exp.1). Another is the influence of the number of blockchain nodes on the public key request time and identity authentication time (Exp.2). The number of drones in this experiment refers to the number of drones that simultaneously initiate public key requests or identity authentication requests. In the following, they are introduced in detail.

In Exp.1, we conducted experiments respectively in the environment where there were no malicious nodes and where there were less than 1/3 malicious nodes in the blockchain system. In an environment without malicious nodes, the number of normal nodes is equal to 20. In another environment, the number of normal nodes is equal to 15. The variation trends of the public key request processing time and the identity authentication processing time with the increase in the number of drones in these two environments are shown in Figures 5 and 6, respectively.

It can be seen from Figures 5 and 6 that the processing time of the public key request and identity authentication increases linearly with the increase in the number of UAVs. Moreover, in an environment with less than 1/3 of malicious nodes, the two processing times are not affected, which also shows that blockchain can tolerate the existence of a certain number of malicious nodes and the normal operation of the system is not affected by these malicious nodes.

In Exp.2, to study the influence of the number of blockchain nodes on the processing time of the public key request and identity authentication, we conducted experiments under different numbers of UAVs (i.e., 50, 100, and 150). The variation trends of the public key request processing time and the identity authentication processing time with the increase in the number of blockchain nodes are shown in Figures 7 and 8, respectively.

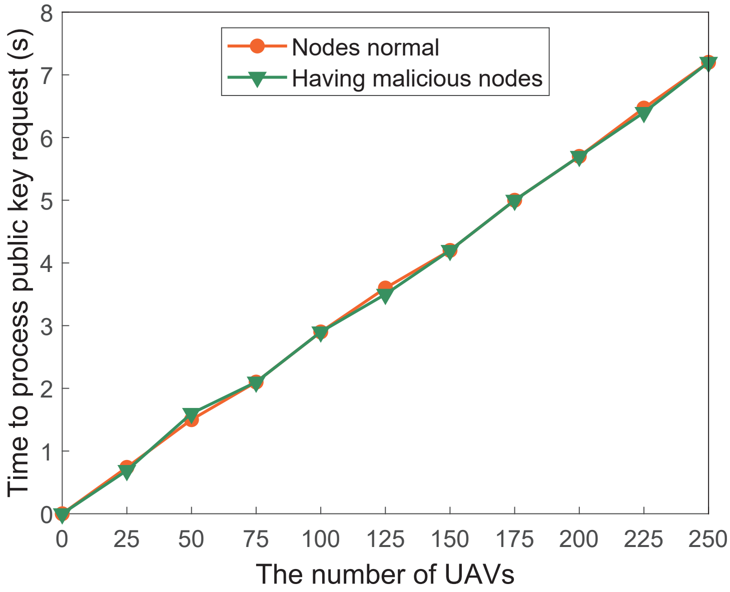


Figure 5. Public key request time according to the number of drones.

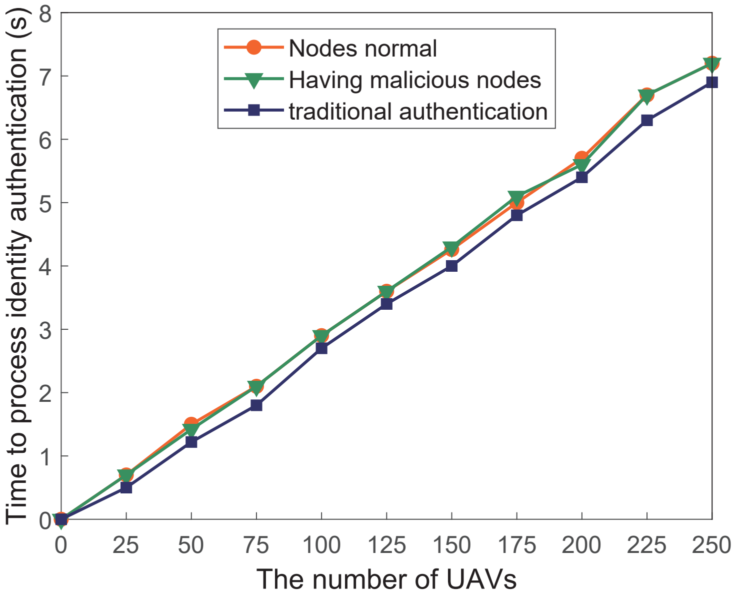


Figure 6. Identity authentication time according to the number of drones.

It can be seen from Figures 7 and 8 that the processing time of the public key request and identity authentication does not increase with the increase in the number of blockchain nodes. When the number of drones is constant, the two processing times tend to a certain value. For instance, When the number of drones requesting the public key at the same time is 50, the processing time of the public key request is about 1.4 s, and the processing time of identity authentication is about 1.5 s.

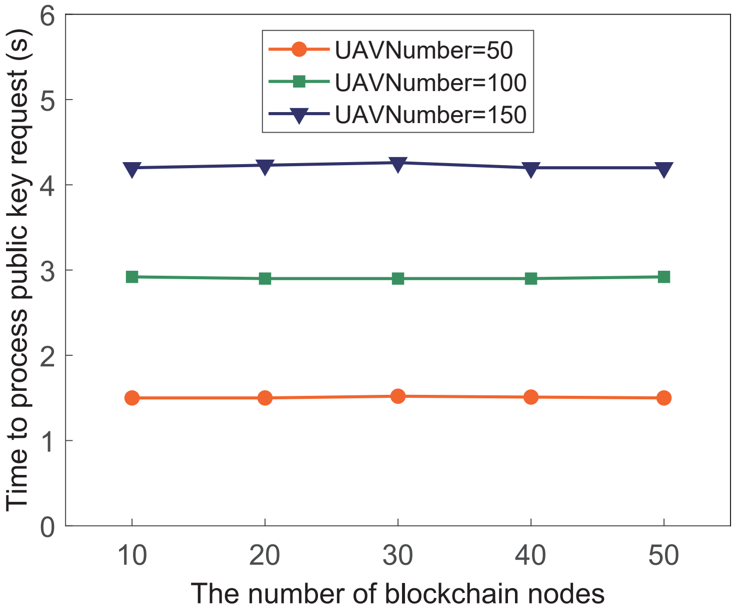


Figure 7. Public key request time according to the number of blockchain nodes.

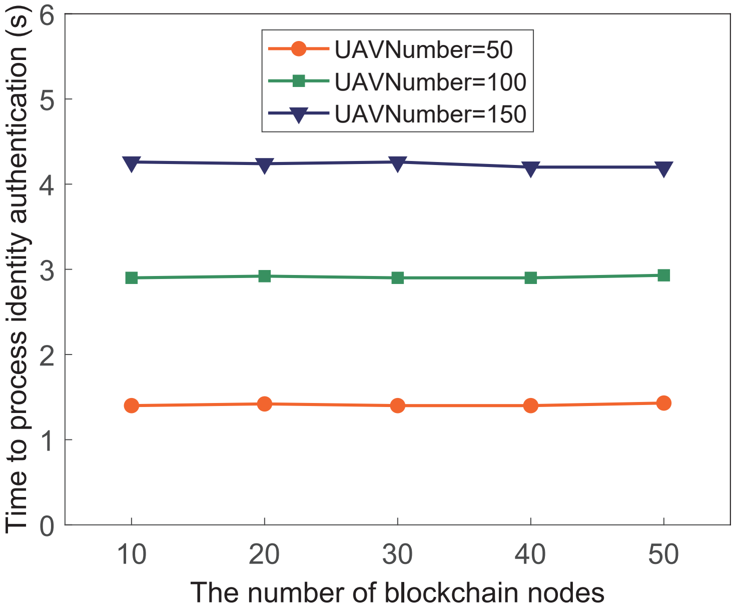


Figure 8. Identity authentication time according to the number of blockchain nodes.

4.3. Discussion and Limitations

The above experimental results show that the secure communication method and distributed identity authentication proposed not only solve the single point of failure caused by centralized management, but also have good scalability, and the identity authentication time will not increase with the increase of blockchain nodes. As can be seen from Figure 6, compared with the existing PKI system, the identity authentication time of the proposed scheme is slightly higher. However, it has better fault tolerance and security, and the normal operation of the system can still be ensured in the presence of malicious nodes. More importantly, the scheme proposed in this paper has a wide range of application scenarios and it can also be applied to some Internet of Things devices. The research of Ahmed et al. [49] indicates that the vehicular ad hoc networks also face some security problems, including malicious vehicle attacks. The identity authentication, and secure communication scheme proposed can also be applied to vehicular ad hoc networks to resist attacks from malicious vehicles and ensure secure communication between vehicles. To complete the secure communication between UAVs, this paper uses smart contracts to realize the functions of identity registration, identity authentication and public key request. By referring to the k + 1 Symmetric Test Pattern proposed by Górski [50], the functional test is carried out, which reduces the number of test cases on the premise of ensuring the accuracy of the test. Although the scheme proposed has better security, applicability, and scalability, the practical Byzantine fault tolerance (PBFT) algorithm adopted by the blockchain will cause communication bottlenecks when the number of consensus nodes increases, which is a major factor limiting the performance of the scheme. Therefore, the lightweightness of the blockchain consensus algorithm will be the next research content.

5. Security Analysis

According to the Dolev-Yao model, the attacker can control the whole network and generate different kinds of output messages [51]. The security of the proposed protocol is analyzed under the Dolev-Yao model.

5.1. Confidentiality

It is assumed that the sender is UAV_1 and the receiver is UAV_2. Taking the UAV_2 public key requested by UAV_1 to the blockchain as an example, Dolev and Yao's methods are used to prove the confidentiality of the proposed protocol. The protocol interaction process is as follows.

(1) $UAV_1 \rightarrow B:$

$$C = \{E_{PK_B}(DID_1, DID_2, E_{SK_1}(Hash(DID_1, DID_2, Timestamp_1, PkRequest)),\\ Timestamp_1, PkRequest)\}$$

(2) $B \rightarrow UAV_1:$

$$C = \{E_{PK_1}(DID_1, DID_2, E_{SK_B}(Hash(DID_1, DID_2, Timestamp_2, PK_2)),\\ Timestamp_2, PK_2)\}$$

The above protocol is formally described as follows.

$$\begin{aligned} N_1(UAV_1, B)P_1 &= \overline{\alpha_1(UAV_1, B)}P_1 \\ &= E_{PK_B}(E_{SK_1}(Hash(P_1))P_1). \end{aligned}$$

where $\alpha_1(UAV_1, B) = E_{PK_B}E_{SK_1}$, and $P_1 = (DID_1, DID_2, Timestamp_1, PkRequest)$.

$$\begin{aligned} N_2(UAV_1, B)P_2 &= \overline{\beta_1(UAV_1, B)N_1(UAV_1, B)}P_2 \\ &= \overline{\beta_1(UAV_1, B)\alpha_1(UAV_1, B)}P_2 \\ &= \overline{E_{PK_1}E_{SK_B}D_{PK_1}D_{SK_B}E_{PK_B}E_{SK_1}}P_2 \\ &= E_{PK_1}(E_{SK_B}(Hash(P_2))P_2). \end{aligned}$$

where $\beta_1(UAV_1, B) = E_{PK_1}E_{SK_B}D_{PK_1}D_{SK_B}$, $P_2 = (DID_1, DID_2, Timestamp_2, PK_2)$, and $E_{PK_1}D_{SK_1} = 1$.

In Dolev-Yao models, there is $\gamma = D_{SK_Z}\beta_1(UAV_Z\ , B)$ that makes:

$$\begin{aligned} \overline{\gamma N_1(UAV_1, B)} &= \overline{D_{SK_Z}\beta_1(UAV_Z, B)N_1(UAV_1, B)} \\ &= \overline{D_{SK_Z}E_{PK_Z}E_{SK_B}E_{PK_Z}D_{SK_B}E_{PK_B}E_{SK_1}} \\ &= \overline{E_{SK_B}D_{PK_Z}E_{SK_1}} \neq \lambda. \end{aligned}$$

where SK_Z is the private key of any UAV in the system, and λ is an empty set.

According to the method of Dolev and Yao, the proposed secure communication protocol satisfies the requirement of confidentiality.

5.2. Tamper-Proofing

All nodes in the blockchain network jointly maintain a ledger, and the consistency of the ledger is guaranteed through a consensus algorithm. To ensure the security and reliability of the data, identity information such as public and private keys are physically transmitted through secure channels. Blockchain verifies the integrity of the received information and stores it only after passing the verification, which can solve the risk of tampering before the data are uploaded to the chain. In Hyperledger fabric, if the total number of nodes is N and the number of malicious nodes is less than 1/3 N, the consensus algorithm PBFT (practical Byzantine fault tolerance) can still ensure the tamper-proof storage of data and the normal operation of the system [52,53].

5.3. Other Securities

In addition to information confidentiality and tamper-proofing, a security protocol should also meet the requirements of integrity, unforgeability, and replay attack resistance. The rest of this section will use Petri Net [54] to analyze the security of the proposed protocol. The ultimate goal of the secure communication protocol proposed is that the sender can correctly receive the receiver's public key, and the receiver can correctly authenticate the sender's identity. Therefore, the security criteria of the protocol are defined as follows.

- The public key endorsed by the sender must be the genuine one belonging to the receiver whose public key is requested by this sender;
- The identity authentication endorsed by the receiver must be the genuine one belonging to the sender whose identity authentication is requested by this receiver.

For security criterion 1, it is assumed that the sender is UAV_1 and the receiver is UAV_2, and UAV_1 requests the public key of UAV_2 from the blockchain. Under the Dolev-Yao model, the public key request protocol model with the attacker and the reachable tree of the model are constructed. The "token/place" pair is used to describe the state of the system in the reachable tree; the detailed information is shown in Figures 9 and 10.

In the figure, $E\{(DID_1, DID_2); SK_1\}$ indicates that DID_1 and DID_2 are encrypted using SK_1. As can be seen from Figure 10, attacks mainly occur in M1 -> M2 and M4 -> M5 processes. In Figure 9, the main purpose of the attacker is to make the public key received by the sender (not the genuine requested one). Therefore, forgery, tampering, and replay are the most likely attacks by attackers.

In many systems, cryptographic techniques, such as encryption, signatures, and timestamps, are also used, but the lack of significant identifiers in the protocol often allows attackers to exploit this vulnerability. If the communication protocol is in the following format, it is insecure.

$$C = \{E_{PK_B}(DID_S, E_{SK_S}(Hash(DID_S, Timestamp_1, PkRequest)), Timestamp_1, PkRequest)\}$$

Supposing UAV_1 requests the public keys of UAV_2 and UAV_3 from the blockchain, and the blockchain returns the requested public keys to UAV_1 according to the above protocol. Since there is no receiver's identity in the protocol, UAV_1 can only judge which UAV's public key is received by the sequence. If the attacker intercepts the information and sends it to UAV_1 in reverse order. At this point, UAV_1 thinks that it has received the requested public key, which is not what it actually requested.

The proposed protocol combines encryption, signature, and identity authentication to prevent attackers from tampering with the transmitted information. Moreover, DID identifiers are added to the protocol to identify senders and receivers, and a timestamp is added to resist replay attacks, which avoids the shortcomings of the above protocols. So, the proposed protocol satisfies the requirements of security criterion 1.

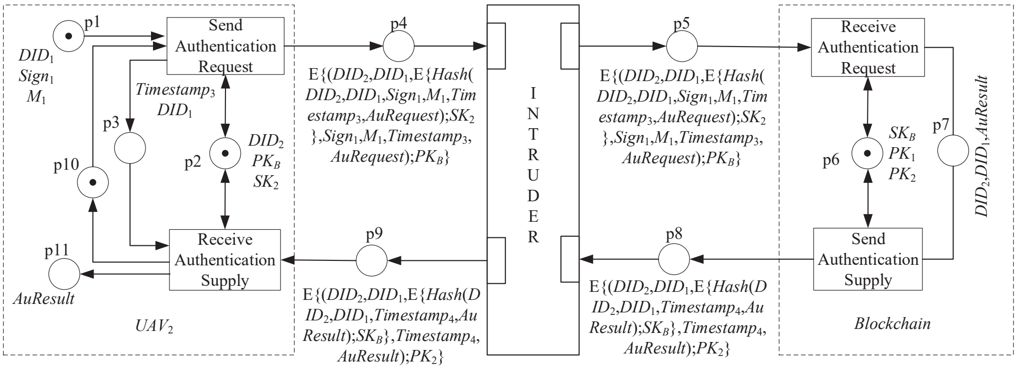

p1
Send Authentication Request
DID1 Sign1 M1
Timestamp3 DID1
p3
p10
p2
DID2 PKB SK2
Receive Authentication Supply
p11
AuResult
UAV2
p4
E{(DID2,DID1,E{Hash(DID2,DID1,Sign1,M1,Timestamp3,AuRequest);SK2},Sign1,M1,Timestamp3,AuRequest);PKB}
p9
E{(DID2,DID1,E{Hash(DID2,DID1,Timestamp4,AuResult);SKB},Timestamp4,AuResult);PK2}
INTRUDER
p5
E{(DID2,DID1,E{Hash(DID2,DID1,Sign1,M1,Timestamp3,AuRequest);SK2},Sign1,M1,Timestamp3,AuRequest);PKB}
p8
E{(DID2,DID1,E{Hash(DID2,DID1,Timestamp4,AuResult);SKB},Timestamp4,AuResult);PK2}
Receive Authentication Request
p6
SKB PK1 PK2
p7
DID2,DID1,AuResult
Send Authentication Supply
Blockchain

Figure 9. The public key request protocol model with the attacker.

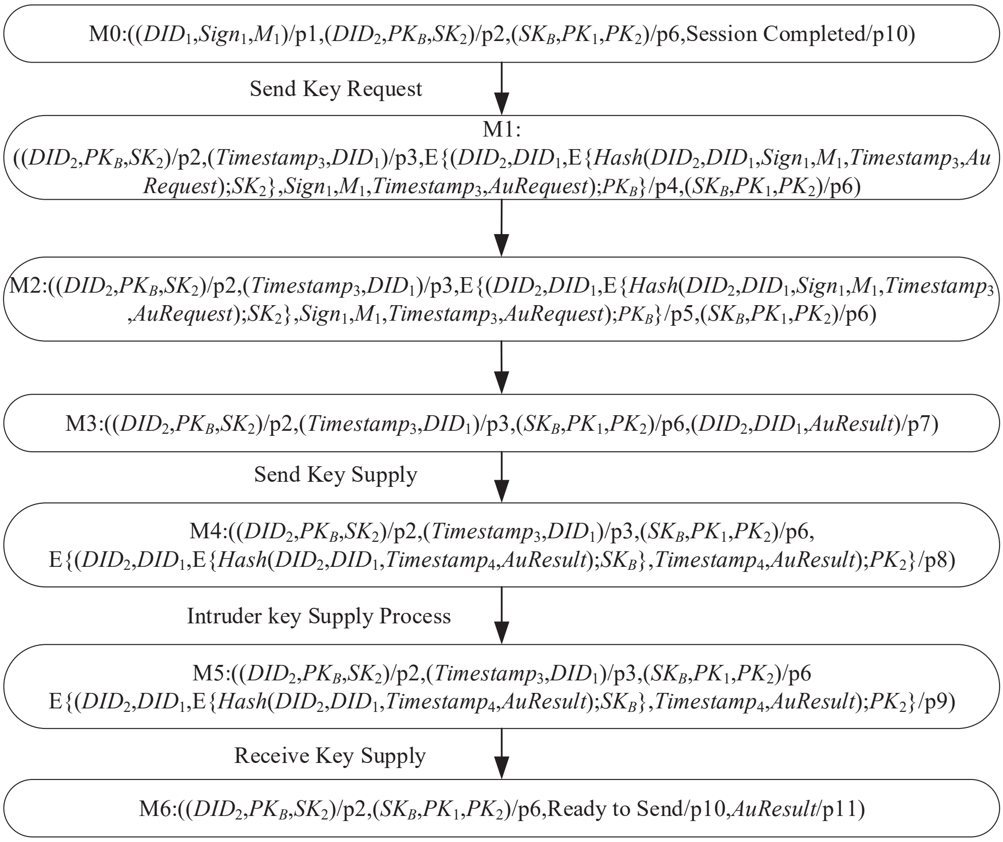

M0:((DID1,Sign1,M1)/p1,(DID2,PKB,SK2)/p2,(SKB,PK1,PK2)/p6,Session Completed/p10)
Send Key Request
M1: ((DID2,PKB,SK2)/p2,(Timestamp3,DID1)/p3,E{(DID2,DID1,E{Hash(DID2,DID1,Sign1,M1,Timestamp3,AuRequest);SK2},Sign1,M1,Timestamp3,AuRequest);PKB}/p4,(SKB,PK1,PK2)/p6)
M2:((DID2,PKB,SK2)/p2,(Timestamp3,DID1)/p3,E{(DID2,DID1,E{Hash(DID2,DID1,Sign1,M1,Timestamp3,AuRequest);SK2},Sign1,M1,Timestamp3,AuRequest);PKB}/p5,(SKB,PK1,PK2)/p6)
M3:((DID2,PKB,SK2)/p2,(Timestamp3,DID1)/p3,(SKB,PK1,PK2)/p6,(DID2,DID1,AuResult)/p7)
Send Key Supply
M4:((DID2,PKB,SK2)/p2,(Timestamp3,DID1)/p3,(SKB,PK1,PK2)/p6, E{(DID2,DID1,E{Hash(DID2,DID1,Timestamp4,AuResult);SKB},Timestamp4,AuResult);PK2}/p8)
Intruder key Supply Process
M5:((DID2,PKB,SK2)/p2,(Timestamp3,DID1)/p3,(SKB,PK1,PK2)/p6 E{(DID2,DID1,E{Hash(DID2,DID1,Timestamp4,AuResult);SKB},Timestamp4,AuResult);PK2}/p9)
Receive Key Supply
M6:((DID2,PKB,SK2)/p2,(SKB,PK1,PK2)/p6,Ready to Send/p10,AuResult/p11)

Figure 10. The reachable tree.

For security criterion 2, the main purpose of the attacker is to make the identity authentication result obtained by the receiver (not the one it really requested). As with security criterion 1, forgery, tampering, and replay are the most likely attacks by an attacker.

In numerous authentication systems, only timestamps and authentication results are returned to simplify communication, which will become the main target of attackers. Assuming that the communication protocol is in the following form, it is insecure.

$$E_{PK_R}\{(E_{SK_B}\{Hash(Timestamp, AuResult)\}, Timestamp, AuResult)\}$$

In the above protocol, it is assumed that UAV_1 requests the blockchain to verify the identity of UAV_2, and at the same time, UAV_3 requests the blockchain to verify the identity of UAV_4. If the attacker intercepts the returned information and exchanges the authentication result, UAV_2 and UAV_3 think that it has received the correct authentication result, but it does not. Further, if the UAV_4 is an illegal drone, it will cause security problems. According to the analysis of security criterion 1, this proposed protocol also meets the requirements of security criterion 2. Therefore, the proposed secure communication protocol is secure.

6. Conclusions

For the security problems, such as single point of failure and lack of reliable authentication mechanism faced by UAV swarm, a blockchain-based UAV identity management model is proposed, and a distributed identity authentication scheme based on DID information is established under this model. Moreover, to ensure the safe transmission of UAV communication data, a secure communication architecture based on blockchain and a set of secure transmission protocols are designed combined with cryptography. Compared with the traditional UAV management scheme, the proposed scheme has obvious advantages in UAV identity management, UAV identity authentication, scalability, and secure transmission of communication data. When the number of drones requesting the public key at the same time is 50, the processing time of identity authentication is about 1.5 s, which also shows that when the number of drones is within a certain range, the time required to process identity authentication is acceptable. Moreover, through various security analyses, it is proved that the proposed scheme is secure and reliable. Therefore, the proposed scheme is feasible in practical applications and has broad application prospects. However, as the number of consensus nodes increases, the PBFT algorithm adopted by the blockchain will cause communication bottlenecks, so in future research, the lightweight consensus algorithm will be the focus of the research.

Author Contributions: Conceptualization, P.H. and A.S.; methodology, P.H. and J.W.; investigation, P.H.; writing—original draft preparation, P.H.; writing—review and editing, A.S. and J.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: "Not applicable" for studies not involving humans or animals.

Informed Consent Statement: ″Not applicable" for studies not involving humans.

Data Availability Statement: Not applicable.

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

References

1. Gharibi, M.; Boutaba, R.; Waslander, S.L. Internet of drones. *IEEE Access* **2016**, *10*, 142–149. https://doi.org/10.1109/ACCESS.2016.2537208.
2. Lukić, I.; Miličević, K.; Köhler, M.; Vinko, D. Possible Blockchain Solutions According to a Smart City Digitalization Strategy. *Appl. Sci.* **2022**, *12*, 5552. https://doi.org/10.3390/app12115552.
3. Kainz, O.; Dopiriak, M.; Michalko, M.; Jakab, F.; Nováková, I. Traffic Monitoring from the Perspective of an Unmanned Aerial Vehicle. *Appl. Sci.* **2022**, *12*, 7966. https://doi.org/10.3390/app12167966.
4. Alhelaly, S.; Muthanna, A.; Elgendy, I.A. Optimizing Task Offloading Energy in Multi-User Multi-UAV-Enabled Mobile Edge-Cloud Computing Systems. *Appl. Sci.* **2022**, *12*, 6566. https://doi.org/110.3390/app12136566.
5. Arafat, M.Y.; Habib, M.A.; Moh, S. Routing Protocols for UAV-Aided Wireless Sensor Networks. *Appl. Sci.* **2020**, *10*, 4077. https://doi.org/10.3390/app10124077.
6. Zhi, Y.; Fu, Z.; Sun, X.; Yu, J. Security and Privacy Issues of UAV: A Survey. *Mob. Netw. Appl.* **2022**, *25*, 95–101. https://doi.org/10.1007/s11036-018-1193-x.
7. Tang, J.; Chen, G.; Coon J.P. Secrecy Performance Analysis of Wireless Communications in the Presence of UAV Jammer and Randomly Located UAV Eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 3026–3041. https://doi.org/10.1109/TIFS.2019.2912074.
8. 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. https://doi.org/10.1016/j.jisa.2020.102670.
9. Zhou, L.; Yang, Z.; Zhou, S.; Zhang, W. Coverage probability analysis of UAV cellular networks in urban environments. In Proceedings of the 2018 IEEE international conference on communications workshops (ICC Workshops), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6. https://doi.org/10.1109/ICCW.2018.8403633.
10. Jiao, S.; Wang, B.; Liu, J.; Liu, R.; Zhou, D. Review of drone swarm research at home and abroad. *Aerosp. Electron. Warf.* **2019**, *35*, 61–64. https://doi.org/10.16328/j.htdz8511.2019.01.014.

11. Manesh, M.R.; Kaabouch, N. Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Comput. Secur.* **2019**, *85*, 386–401. https://doi.org/10.1016/j.cose.2019.05.003.
12. Manesh, M.R.; Kaabouch, N. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. *Int. J. Crit. Infrastruct. Prot.* **2017**, *19*, 16–31. https://doi.org/10.1016/j.ijcip.2017.10.002.
13. Sivaraman,V.; Gharakheili, H.H.; Vishwanath, A.; Boreli, R.; Mehani, O. Network-level security and privacy control for smart-home IoT devices. In Proceedings of the 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, United Arab Emirates, 19–21 October 2015; pp. 163–167. https://doi.org/10.1109/WiMOB.2015.7347956.
14. Saraswat, D.; Verma, A.; Bhattacharya, P.; Tanwar, S.; Sharma, G.; Bokoro, P.N.; Sharma, R. Blockchain-Based Federated Learning in UAVs Beyond 5G Networks: A Solution Taxonomy and Future Directions. *IEEE Access* **2022**, *10*, 33154–33182. https://doi.org/10.1109/ACCESS.2022.3161132.
15. Wang, Z.; Zhang, F.; Yu, Q.; Qin, T. Blockchain-Envisioned Unmanned Aerial Vehicle Communications in Space-Air-Ground Integrated Network: A Review. *Intell. Converg. Netw.* **2021**, *2*, 277–294. https://doi.org/10.23919/ICN.2021.0018.
16. Hassija, V.; Chamola, V.; Krishna, D.N.G.; Guizani, M. A distributed framework for energy trading between UAVs and charging stations for critical applications. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5391–5402. https://doi.org/10.1109/TVT.2020.2977036.
17. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3417–3442. https://doi.org/10.1109/COMST.2019.2906228.
18. Alladi, T.; Chamola, V.; Sahu, N.; Guizani, M. Applications of blockchain in unmanned aerial vehicles: A review. *Veh. Commun.* **2020**, *23*, 100249. https://doi.org/10.3390/app12189203.
19. Sultan, L.; Anjum, M.; Rehman, M.; Murawwat, S.; Kosar, H. Communication Among Heterogeneous Unmanned Aerial Vehicles (UAVs): Classification, Trends, and Analysis. *IEEE Access* **2021**, *9*, 118815–118836. https://doi.org/10.1109/ACCESS.2021.3107479.
20. Duan, Z.; Yang, X.; Xu, Q.; Wang, L. Time-Division Multiarray Beamforming for UAV Communication. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 4089931. https://doi.org/10.1155/2022/4089931.
21. Brito, C.; Silva, L.; Callou, G.; Nguyen, T.A.; Min, D.; Lee, J.-W.; Silva, F.A. Offloading Data through Unmanned Aerial Vehicles: A Dependability Evaluation. *Electronics* **2021**, *10*, 1916. https://doi.org/10.3390/electronics10161916.
22. Soltani, R.; Zaman, M.; Joshi, R.; Sampalli, S. Distributed Ledger Technologies and Their Applications: A Review. *Appl. Sci.* **2022**, *12*, 7898. https://doi.org/10.3390/app12157898.
23. Sharma, P.K.; Kumar, N.; Park, J.H. Blockchain-based distributed framework for automotive industry in a smart city. *IEEE Trans. Ind. Inform.* **2018**, *15*, 4197–4205. https://doi.org/10.1109/TII.2018.2887101.
24. Rasool, S.; Saleem, A.; Iqbal, M.; Dagiuklas, T.; Bashir, A.K.; Mumtaz, S.; Al Otaibi, S. Blockchain-enabled reliable osmotic computing for cloud of things: Applications and challenges. *IEEE Internet Things Mag.* **2020**, *3*, 63–67. https://doi.org/10.1109/IOTM.0001.1900101.
25. Wattana, V.; Tharwon, A.; Danupol, H. When blockchain meets internet of things: Characteristics, challenges, and business opportunities. *J. Ind. Inf. Integr.* **2019**, *15*, 21–28. https://doi.org/10.1016/j.jii.2019.05.002.
26. Kong, L.; Chen, B.; Hu, F. Blockchain-Assisted Adaptive Reconfiguration Method for Trusted UAV Network. *Electronics* **2022**, *11*, 2549. https://doi.org/10.3390/electronics11162549.
27. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, 21260. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 6 October 2022).
28. Han, P.; Sui, A.; Jiang, T.; Gu, C. Copyright certificate storage and trading system based on blockchain. In Proceedings of the 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, 25–27 August 2020; pp. 611–615. https://doi.org/10.1109/AEECA49918.2020.9213631.
29. Barateiro, C.; Faria, A.; Farias Filho, J.; Maggessi, K.; Makarovsky, C. Fiscal Measurement and Oil and Gas Production Market: Increasing Reliability Using Blockchain Technology. *Appl. Sci.* **2022**, *12*, 7874. https://doi.org/10.3390/app12157874.
30. Liu, F.; Feng, Z.; Qi, J. A Blockchain-Based Digital Asset Platform with Multi-Party Certification. *Appl. Sci.* **2022**, *12*, 5342. https://doi.org/10.3390/app12115342.
31. Xi, P.; Zhang, X.; Wang, L.; Liu, W.; Peng, S. A Review of Blockchain-Based Secure Sharing of Healthcare Data. *Appl. Sci.* **2022**, *12*, 7912. https://doi.org/10.3390/app12157912.
32. Nguyen, H.P.D.; Nguyen, D.D. Drone application in smart cities: The general overview of security vulnerabilities and countermeasures for data communication. In *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead. Studies in Systems, Decision and Control*; Krishnamurthi, R., Nayyar, A., Hassanien, A., Eds.; Springer: Cham, Germany, 2021; Volume 332. https://doi.org/10.1007/978-3-030-63339-4_7.
33. Górski, T. Reconfigurable Smart Contracts for Renewable Energy Exchange with Re-Use of Verification Rules. *Appl. Sci.* **2022**, *12*, 5339. https://doi.org/10.3390/app12115339.
34. Hisseine, M.A.; Chen, D.; Yang, X. The Application of Blockchain in Social Media: A Systematic Literature Review. *Appl. Sci.* **2022**, *12*, 6567. https://doi.org/10.3390/app12136567.
35. Feng, W.; Li, Y.; Yang, X.; Yan, Z.; Chen, L. Blockchain-based data transmission control for Tactical Data Link. *Digit. Commun. Netw.* **2021**, *7*, 285–294. https://doi.org/10.1016/j.dcan.2020.05.007.

36. Eyal, I.; Sirer, E.G. Majority is not enough: Bitcoin mining is vulnerable. *Commun. ACM* **2018**, *61*, 95–102. https://doi.org/10.1145/3212998.
37. Sapra, R.; Dhaliwal, P. Blockchain: The perspective future of technology. *Int. J. Healthc. Inf. Syst. Inform.* **2021**, *16*, 1–20. https://doi.org/10.4018/IJHISI.20210401.oa1.
38. 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. https://doi.org/10.1109/JIOT.2020.3030080.
39. Al-Jaroodi, J.; Mohamed, N. Blockchain in industries: A survey. *IEEE Access* **2019**, *7*, 36500–36515. https://doi.org/10.1109/ACCESS.2019.2903554.
40. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. A taxonomy of blockchain-enabled softwarization for secure UAV network. *Comput. Commun.* **2020**, *161*, 304–323. https://doi.org/10.1016/j.comcom.2020.07.042.
41. Rana, T.; Shankar, A.; Sultan, M.K.; Patan, R.; Balusamy, B. An intelligent approach for UAV and drone privacy security using blockchain methodology. In Proceedings of the 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 10–11 January 2019; pp. 162–167. https://doi.org/10.1109/CONFLUENCE.2019.8776613.
42. Lv, Z.; Qiao, L.; Hossain, M.S.; Choi, B.J. Analysis of using blockchain to protect the privacy of drone big data. *IEEE Netw.* **2021**, *35*, 44–49. https://doi.org/10.1109/MNET.011.2000154.
43. 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" (WoWMoM), Washington, DC, USA, 10–12 June 2019; pp. 1–7. https://doi.org/10.1109/WoWMoM.2019.8793027.
44. Liang, X.; Zhao, J.; Shetty, S.; Li, D. Towards data assurance and resilience in IoT using blockchain. In Proceedings of the MILCOM 2017—2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 261–266. https://doi.org/10.1109/MILCOM.2017.8170858.
45. Rodríguez-Molina, J.; Corpas, B.; Hirsch, C.; Castillejo, P. SEDIBLOFRA: A Blockchain-Based, Secure Framework for Remote Data Transfer in Unmanned Aerial Vehicles. *IEEE Access* **2021**, *9*, 121385–121404. https://doi.org/10.1109/ACCESS.2021.3106379.
46. Kuzmin, A.; Znak, E. Blockchain-base structures for a secure and operate network of semi-autonomous unmanned aerial vehicles. In Proceedings of the 2018 IEEE International conference on service operations and logistics, and informatics (SOLI), Singapore, 31 July–2 August 2018; pp. 32–37. https://doi.org/10.1109/SOLI.2018.8476785.
47. Ge, C.; Ma, X.; Liu, Z. A semi-autonomous distributed blockchain-based framework for UAVs system. *J. Syst. Archit.* **2020**, *107*, 101728. https://doi.org/10.1016/j.sysarc.2020.101728.
48. Mehta, P.; Gupta, R.; Tanwar, S. Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. *Comput. Commun.* **2020**, *151*, 518–538. https://doi.org/10.1016/j.comcom.2020.01.023.
49. Ahmed, W.; Di, W.; Mukathe, D. A Blockchain-Enabled Incentive Trust Management with Threshold Ring Signature Scheme for Traffic Event Validation in VANETs. *Sensors* **2022**, *22*, 6715. https://doi.org/10.3390/s22176715.
50. Górski, T. The k + 1 Symmetric Test Pattern for Smart Contracts. *Symmetry* **2022**, *14*, 1686. https://doi.org/10.3390/sym14081686.
51. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. https://doi.org/10.1109/TIT.1983.1056650.
52. Luo, G.; Shi, M.; Zhao, C.; Shi, Z. Hash-Chain-Based Cross-Regional Safety Authentication for Space-Air-Ground Integrated VANETs. *Appl. Sci.* **2020**, *10*, 4206. https://doi.org/10.3390/app10124206.
53. Firdaus, M.; Rhee, K.-H. On Blockchain-Enhanced Secure Data Storage and Sharing in Vehicular Edge Computing Networks. *Appl. Sci.* **2021**, *11*, 414. https://doi.org/10.3390/app11010414.
54. Nieh, B.B.; Tavares, S.E. Modelling and analyzing cryptographic protocols using Petri nets. *Int. Workshop Theory Appl. Cryptogr. Tech.* **1992**, 275–295. https://doi.org/10.1007/3-540-57220-1_69.