Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 1, No. 2, 2022

Blockchain-based Communication Mechanism for Unmanned Aircraft

Peizheng Wang*, Xie Wang

School of Software Engineering, Chengdu University of Information Technology, Chengdu 610225, China
* **Corresponding author**: Peizheng Wang (Email: peizhengwang2022@126.com)

Abstract: With the maturity of unmanned aircraft technology, unmanned aircraft have a wide range of applications in areas such as public safety. However, unmanned aircraft are frequently involved in accidents due to network intrusion, and it is urgent to ensure the safety of unmanned aircraft networks. This paper first introduces the current situation and challenges of unmanned aircraft and blockchain, and proposes a communication mechanism for unmanned aircraft based on blockchain technology to achieve unmanned aircraft data security and privacy protection, multi-party data sharing and data storage security to ensure unmanned aircraft network security.

Keywords: Blockchain; Unmanned aircraft; Security, Privacy.

1. Introduction

Unmanned aircraft technology, refers to UAS, UAV engineering and UAV-related application technology [1]. With the maturity of unmanned aircraft technology, it has become possible to use unmanned aircraft to complete some difficult and dangerous and toxic work that is difficult for humans to complete. Through unmanned aircraft, plant protection, mapping, photography, high-voltage cables and agricultural and forestry patrols can be carried out, and unmanned aircraft also have a broad application space in areas such as public safety. However, unmanned aircraft are frequently involved in accidents due to network intrusions, which can lead to casualties if they are not careful, so it is urgent to ensure their cyber security. In 2012, the S-100 unmanned aircraft test in Incheon, South Korea, was interfered with, resulting in the crash of the unmanned aircraft and causing casualties. In 2018, the Xi'an unmanned aircraft formation shows failed due to malicious interference with some unmanned aircraft signals. A key area of research.

In recent years, the emerging blockchain technology has been developing rapidly and has attracted widespread attention from both academia and industry [2]. Blockchain is a distributed ledger technology with key features such as decentralization, anonymity, difficulty in tampering and auditability, and is able to achieve peer-to-peer value transfer between unfamiliar nodes in an imperfectly trusted environment through the integrated use of technologies such as timestamps, cryptographic hashes, digital signatures, consensus mechanisms and smart contracts.

The application between blockchain and unmanned aircraft has also been actively explored. There are views that unmanned aircraft, as a relatively mature application in the field of Internet of Things and big data, have a wide range of combination scenarios with blockchain. But currently, there are already many companies that have developed blockchain technology in the application of unmanned aircraft.

The US company has partnered with artificial intelligence technology provider Spark Cognition to develop a blockchain technology-based unmanned aircraft tracking system and air traffic management solution. Both parties will use artificial intelligence and blockchain technology to track unmanned aerial vehicles in flight and plan traffic routes to ensure transport safety. There are also plans to provide standardized programming interfaces to support parcel delivery, industrial inspections and other commercial applications. In addition, Boeing is forming a new organization that will provide cargo transportation and urban aviation services in the future mobile ecosystem.

In September 2018, IBM detailed in a patent application how its blockchain can be used to store data related to the flight of unmanned aerial vehicles (UAVs), according to documents published by the United States Patent and Trademark Office [3]. Particularly in the case of high security risks, to ensure effective regulation by airspace controllers and regulators of the increasing number of unmanned aircraft in the sky.

Walmart is also looking to use blockchain technology to secure parcel delivery systems throughout its supply chain of robots and self-driving cars [4]. According to the US Patent and Trademark Office, Walmart filed a patent application for "Blockchain Technology Application for Cloning Unmanned aircraft" in January 2019, which was made public on August 1. According to the disclosure, Walmart intends to apply blockchain technology to the transmission of unmanned aircraft information, including unmanned aircraft identification numbers, flight altitude, flight courier, flight path, battery information or loading capacity, and can share information based on intermediate locations between unmanned aircraft.

Ajman DEEP AERO from the UAE is also developing a blockchain-based artificial intelligence-powered, autonomous and home-grown intelligent Unmanned Aircraft Systems (UAS) traffic management (UTM) platform. The platform can be used to secure unmanned low-altitude civil aviation flights in shared airspace.

2. Blockchain

2.1. Blockchain Basic Concepts

Originally born in 2008 as "Bitcoin: A Peer-to-Peer Electronic Cash System" by an academic going by the pseudonym "Satoshi Nakamoto", blockchain is essentially a decentralized database [5]. Autonomously managed through

a peer-to-peer network and distributed timestamp servers, the blockchain is a data structure used to record the history of bitcoin transaction accounts. Blockchain technology replaces traditional centralized systems based on central trust through software-defined credit, using a distributed node trust mechanism to guarantee that the system records, transmits and stores the activity of value transfer. Blockchain guarantees data consistency through consensus mechanisms, and data confidentiality and security through cryptographic algorithms. The structure of the blockchain is shown in Figure 1.

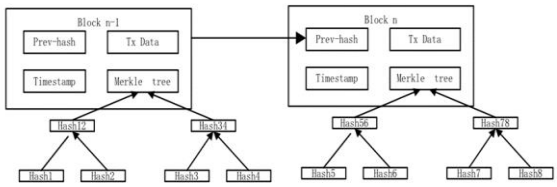

Figure 1. The Structure of the Blockchain

Blockchain technology guarantees decentralization or weak centralization through distributed ledgers, privacy and tamper-evident characteristics of data through cryptographic foundations, and consistency of data in distributed ledgers through consensus mechanisms. Taken together, blockchain has the following characteristics [6].

(1) Decentralization

Compared with the traditional centralized model, blockchain removes or weakens the presence of third parties and uses consensus mechanisms to ensure data consistency in the distributed network.

(2) Non-tamper ability

Once a transaction exists in the blockchain, it is almost impossible to be deleted or have a rollback. In addition, the blockchain can quickly detect blocks containing invalid transactions through validation.

(3) Anonymity

Blockchain technology uses an address linked to the user's public key as the user's representation, and the user only needs to disclose the address without disclosing his or her true identity, so it has a certain degree of anonymity.

(4) Traceability

This feature is based on the UTXO (Unspent Transaction Outputs) transaction model. The Genesis block is the first block, except that all transactions in the block will have several inputs and outputs, and the source of a transaction must be the unused output of another transaction, and the input of this transaction is accompanied by the digital signature of the private key corresponding to the address of the previous output, and every node in the current network maintains the UTXO transaction mode, and the transaction satisfies the UTXO transaction mode and The transaction is considered legitimate only if it satisfies the UTXO transaction pattern and the digital signature is correct. Therefore, it is not necessary to trace the entire history to confirm that the current transaction is legitimate.

2.2. Consensus mechanisms

How to reach consensus among many nodes efficiently is the core technical problem of distributed systems in which nodes are decentralized to handle transactions. Blockchain as a distributed system application, Bitcoin uses PoW proof-of-work algorithm combined with incentive mechanism and cryptography to solve the Byzantine fault tolerance problem. However, blockchains can be divided into blockchains with very different degrees of decentralization depending on the application scenario, which requires different consensus mechanisms to cope with the consensus problem of distributed systems. The development of blockchain has so far produced many new consensus algorithms that can solve the Byzantine fault tolerance problem, and four of the mainstream algorithms are listed below for introduction.

The proof-of-work mechanism was originally designed to allow a certain amount of proof-of-work to be completed before an email could be sent, which resulted in a high cost for sending spam. After this Satoshi Nakamoto introduced the proof-of-work mechanism to Bitcoin. All nodes in Bitcoin are required to "mine", and whenever a new transaction is created in Bitcoin, the pending information is broadcast across the network. When a new transaction needs to be credited to the blockchain, the node generates a block of packets and calculates the Merkle root, which generates a random string of nonce, and only the first node to calculate the nonce has the right to account for it. This shows that the proof-of-work mechanism actually requires a lot of arithmetic resources, which increases the cost of blockchain bookkeeping, but it also makes it more difficult to attack the PoW consensus-based blockchain.

The PoW proof-of-work mechanism is based on arithmetic, which is suspected of reducing efficiency and wasting resources [7]. Researchers have considered the possibility of converting the consumption of arithmetic power into an investment in equity. In general, those with more equity are more willing to maintain the security and stability of the entire chain. Equity in a blockchain involves "coin age", where each coin owned by a node generates one "coin age" per day.

Under the PoS proof-of-interest mechanism, the blockchain decides the bookkeeping node in each round of election based on the equity of the nodes participating in the consensus, and the higher the equity, the higher the probability of being selected [8]. In the next round of election, the nodes are re-elected according to this rule. Compared to the PoW proof-of-work mechanism, the PoS proof-of-stake mechanism is more efficient and arithmetic-efficient, and the confirmation time of new blocks in the blockchain is greatly reduced.

The DPoS proof-of-stake mechanism is an extension of PoS, and also solves the PoW arithmetic problem [9]. The coins owned by each node in DPoS can be seen as individual votes, which can be cast to nodes they trust, thus electing the principals. The principals are the ones who produce the blocks.

PBFT (Practical Byzantine Fault Tolerance) is a practical Byzantine fault tolerance algorithm. This algorithm was proposed by Miguel Castro and Barbara Liskov in 1999 to solve the Byzantine General problem in a trusted channel [10]. In PBFT, nodes are classified according to the consensus role as client nodes, master nodes and backup nodes. All nodes must satisfy the following two properties: first, all correct nodes produce the same output result with the same input message; second, if the input message is successfully verified, all correct nodes must receive the message and compute the corresponding result.

The PBFT mechanism is a Byzantine fault-tolerant system with state machine replication. To maintain a common ledger data state, it is required that all nodes behave uniformly and therefore three protocols need to be implemented: a consistency protocol, a checkpointing protocol and a view switching protocol. The consistency protocol consists of a request phase, a pre-prepare phase, a prepare phase, a commit

phase and a reply phase. Figure 2 shows the flowchart of the PBFT mechanism implementation with five nodes, where client is the client node, primary is the primary node and backup1-3 are the three backup nodes.

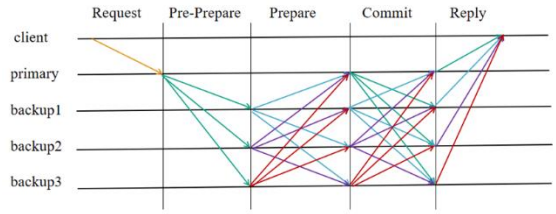

Figure 2. The Consensus Process of PBFT

2.3. Smart Contracts

Smart contracts are a concept developed by cryptographer Nick Szabo, the central idea of which is to embed contractual terms in hardware and software in such a way that breaking the contract is extremely costly or immutable [11]. If the terms of the contract are written in code form, the terms of the contract can be enforced quickly and efficiently and with less intervention from third parties. Prior to the advent of blockchain, the implementation of smart contracts had been plagued by problems of consensus and multi-party trust that prevented their real development. But the advent of blockchain has given smart contracts more scope for development. The addition of smart contracts was a key factor in the development of Blockchain 1.0 into Blockchain 2.0. Blockchain technology serves as the technical basis for smart contracts. It uses smart contracts as scripts, which are initiated with a blockchain address and executed by setting trigger conditions. The transactions executed by smart contracts can be saved on the blockchain. The tamper-evident nature of the blockchain and the consensus mechanism bring a secure and trusted execution environment for smart contracts. Ethernet is currently the most popular platform for smart contract applications.Use American English when writing your paper. The serial comma should be used (“a, b, and c” not “a, b and c”). In American English, periods and commas are within quotation marks, like “this period.” Other punctuation is “outside”! The use of technical jargon, slang, and vague or informal English should be avoided. Generic technical terms should instead be used.

2.4. Hash Algorithm

The Hash algorithm, also known as a hashing algorithm, is able to compress message data of any length into a fixed-length string of binary values, or hashes, in a finite and appropriate amount of time [12]. The hash function ensures the security and integrity of data in a blockchain system. In blockchain, the hash algorithm is used to perform calculations on the digital content to form a digital digest, which can be used to ensure that the content has not been tampered with.

The hash function commonly used in blockchain technology is SHA256, which is collision-resistant and can be used as a data integrity check. If the original message is tampered with during transmission, the hash value has been changed after the hash function calculation, representing that the integrity of the message was broken during transmission. In blockchain, the block header stores the hash value of the previous block, so the integrity of the data in the previous block can be checked by comparing the hash value calculated by the SHA256 function with the already existing hash value.

3. Blockchain-based communication mechanism for Unmanned Aircraft

This paper first introduces the current situation and challenges of unmanned aircraft and blockchain, combines the unmanned aircraft network with blockchain, and under the premise of optimising the unmanned aircraft network as well as safeguarding user privacy, and addresses the problem of multiparty sharing in the unmanned aircraft network, this paper proposes a unmanned aircraft communication mechanism based on blockchain technology to achieve unmanned aircraft data security and privacy protection, multiparty data sharing and data storage security to ensure unmanned aircraft network security. The blockchain-based communication mechanism for unmanned aircraft is shown in Figure 3.

(1) Data security and privacy protection

With the maturity of unmanned aircraft technology, it has become possible to use unmanned aircraft to complete some difficult, dangerous and toxic jobs that are difficult for humans to complete. Unmanned aircraft transmit information through mobile networks to complete efficient collaboration. However, the unmanned aircraft network itself has serious privacy leakage issues and cyber-attacks, which is a big problem that needs to be addressed for the widespread use of unmanned aircraft. The data collected by unmanned aircraft is a highly private record of the user, and a privacy breach could result in damage to the user's privacy and the data falling into the hands of a malicious attacker. Therefore, encryption methods need to be able to cope with malicious attacks by attackers. A blockchain is a network of peer-to-peer components that has a similar network structure to a unmanned aircraft network. Blockchain uses techniques such as hash functions and elliptic curve encryption to secure data. Blockchain guarantees data consistency through consensus mechanisms, and data confidentiality and security through cryptographic algorithms.

(2) Multi-party data sharing

Unmanned aircraft systems are developing rapidly and gradually increasing in scale, requiring multiple UAVs to collaborate with each other in order to complete their tasks. However, the current UAV data collection is localised and home-made, relying mainly on independently operating UAS, and it is difficult to achieve multi-party data sharing. The lack of effective data sharing can lead to information blockage, and the true value of the data cannot be realised without information interaction. By introducing blockchain technology, the UAS network realises multi-party data sharing.

(3) Data storage security

Unmanned aircraft collect data and upload the collected data regularly through neighbouring data collection base stations. This data is stored at a trusted central node, implying a centralised management approach. However, this centralised management requires a high level of data storage security, stability and timeliness, as well as a high risk of single point of attack and malicious tampering. With a centralised management mechanism, it is difficult to recover quickly from an attack, so there is an urgent need to design a decentralised storage mechanism to guarantee the safe storage of unmanned aircraft data.

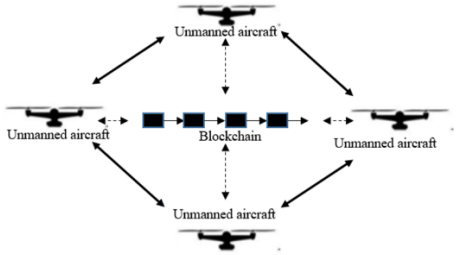

Figure 3. The blockchain-based communication mechanism for unmanned aircraft

4. Conclusion

This paper first introduces the current situation and challenges of UAVs and blockchain, combines UAV networks with blockchain, and addresses the problems of data security and multi-party sharing in UAV networks. This paper proposes a UAV communication mechanism based on blockchain technology to achieve UAV data privacy protection, multi-party data sharing and data storage security.

References

[1] Gupta S G, Ghonge D, Jawandhiya P M. Review of unmanned aircraft system (UAS)[J]. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume, 2013, 2. W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[2] Zheng Z, Xie S, Dai H N, et al. Blockchain challenges and opportunities: A survey[J]. International journal of web and grid services, 2018, 14(4): 352-375.

[3] Alladi T, Chamola V, Sahu N, et al. Applications of blockchain in unmanned aerial vehicles: A review[J]. Vehicular Communications, 2020, 23: 100249.

[4] Sanders N R, Boone T, Ganeshan R, et al. Sustainable supply chains in the age of AI and digitization: research challenges and opportunities[J]. Journal of Business Logistics, 2019, 40(3): 229-240.

[5] Urquhart A. The inefficiency of Bitcoin[J]. Economics Letters, 2016, 148: 80-82.

[6] Nofer M, Gomber P, Hinz O, et al. Blockchain[J]. Business & Information Systems Engineering, 2017, 59(3): 183-187.

[7] Gervais A, Karame G O, Wüst K, et al. On the security and performance of proof of work blockchains[C]//Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016: 3-16.

[8] King S, Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake[J]. self-published paper, August, 2012, 19(1).

[9] Xu G, Liu Y, Khan P W. Improvement of the DPoS consensus mechanism in Blockchain based on vague sets[J]. IEEE Transactions on Industrial Informatics, 2019, 16(6): 4252-4259.

[10] Castro M, Liskov B. Practical byzantine fault tolerance[C]//OsDI. 1999, 99(1999): 173-186.

[11] Zheng Z, Xie S, Dai H N, et al. An overview on smart contracts: Challenges, advances and platforms[J]. Future Generation Computer Systems, 2020, 105: 475-491.

[12] Penard W, van Werkhoven T. On the secure hash algorithm family[J]. Cryptography in context, 2008: 1-18.