International Conference on Astronautics and Space Exploration (iCASE)
Hsinchu, Taiwan, November 03-05, 2022

Exchanges of satellite images by the blockchain encryption system with data security transmission and cloud management platform

[1]Li-Wu Chen, [2]LI-Yu Chang, [3]Henry Horng-Shing Lu

[1]iOne Information Technology Co., Ltd
[2]National Space Organization
[3]National Yang Ming Chiao Tung University

[1]5F-1, 328 ChangChun Rd, Zhongshan Dist. Taipei City, Taiwan (ROC)
[2]8F, 9 Prosperity 1st Road, Hsinchu Science Park, Hsinchu City 300, Taiwan (ROC)
[3]No. 1001, University Rd, East Dist., Hsinchu City, Taiwan (ROC)-

[1]tchen@ioneit.com
[2]davidchang@narlabs.org.tw
[3]henryhslu@nycu.edu.tw

ABSTRACT

The safety delivery of important and confidential files has been a challenge for collaborative units. The main approaches include encrypted email attachment and physical USB. However, these approaches are unsafe and they can be easily hacked. We apply the technology of blockchain encryption technologies via the InterPlanetary File System (IPFS) to solve this issue. That is, we construct the file transmission blockchain platform for fast and secure exchange. This report demonstrates the blockchain platform development for National Space Organization (NSPO) in Taiwan by the techniques of file sharing and asymmetric encryption through IPFS. On the platform, asymmetric encryption technology is used for user authentication and data encryption to enable secure file transmission. The technique of IPFS is also used for file version control. In addition, the cloud management platform can monitor and track the exchange process between transmitters and receivers. Thus, this platform can deploy the security and convenience of file exchanges with the tracking of file transmission records.

***Keywords**: blockchain; InterPlanetary File System; IPFS; asymmetric encryption; cloud management platform*

1. Objective

Recently, there have been many leakage cases of archival materials and government agencies are paying attention to the security of the transmission of important files to each other [1]. The National Space Organization (NSPO) in Taiwan is responsible for managing satellite telemetry data and the related exchanges with various institution units in timely efficiency. Secure transmission is the most important requirement. This development plan is based on blockchain technology to build the data security transmission and cloud management platform instead of the conventional email or USB transmission approach. Hence, the goal is to achieve the data transmission and exchange process with the anti-tampering method and rapid data verification functions. In this development, asymmetric encryption technology is used for user authentication and data encryption transmission. This is used as the basis for data security transmission by the blockchain technique of InterPlanetary File System (IPFS) [2] 、[3] to manage and track every user and the related operation process. It can be utilized to process data transmission of satellite telemetry data exchange to prevent data from being tampered with. Hence, this system can achieve the security and convenience of overall data transmission.

2. System architecture

To design a cloud satellite data blockchain encryption processing platform, in addition to basic management functions such as user management and verification, the main functions provide workflow for file transfer and how to leverage blockchain IPFS technology for satellite telemetry data file transmission management and sharing by using node distribution to achieve safe and fast transmission. The data upload, download and storage process are encrypted by asymmetric encryption technology. The encryption process uses public key encryption, and the private key is decrypted to meet the requirements of data security transmission in order to achieve traceability, immutability, security and tamper proof.

According to the above analysis, the design platform architecture of "Satellite Data Blockchain Encryption Processing System - Data Security Transmission and Cloud Management Platform" is shown in Figure 1.

The data security transmission and cloud management platform includes three main functions: system management, file transmission and query. The data security transmission and cloud management platform architecture is structured in three layers:

- Cloud Platform (Web Layer):
  Handle functions and processes such as NSPO system administration and customer management and also web design.
- API layer:
  Handle the integration of cloud platforms (web layers) with blockchain 、asymmetric encryption and heterogeneous systems [4].
- Blockchain layer:
  Handle smart contract/node management (such as VM-1, VM-2…)/IPFS [5]、[6].

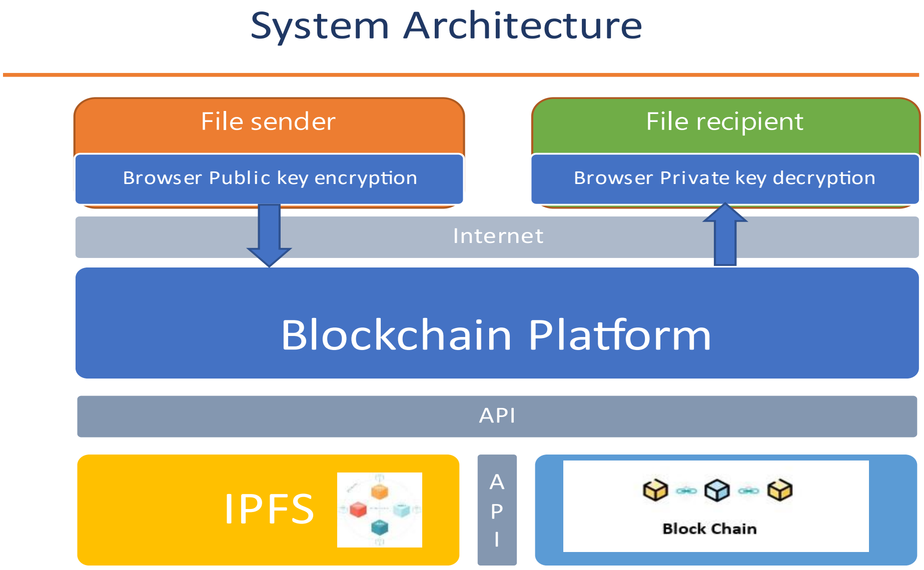
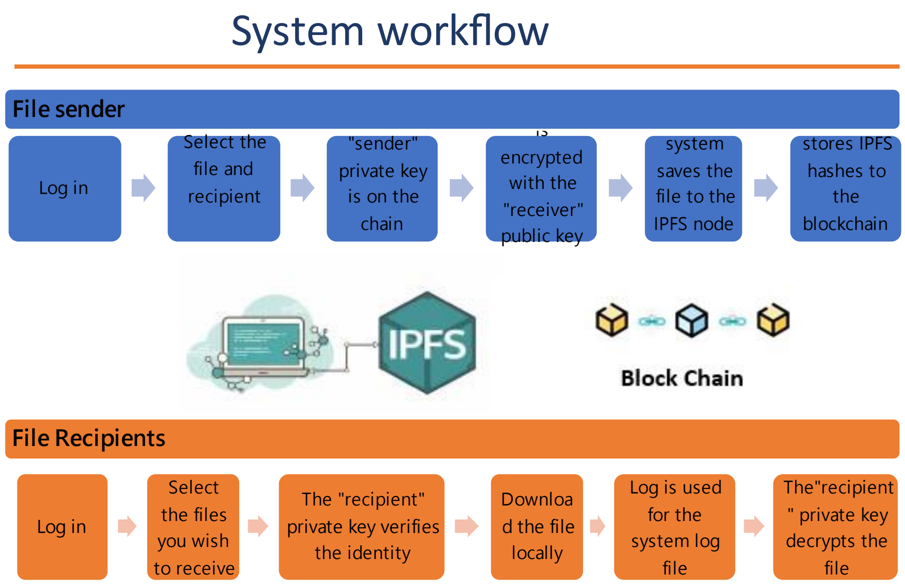


Figure 1. Design platform architecture.

3. Platform major functions

- Cloud platform frond-end operation
  The front end of the platform needs to provide the entire file transfer from the file uploader before uploading private key encryption, filing recipient import its private key to download, and decrypting of all processes [7]. The management mechanism of the entire platform system is shown in Figure 2.



System workflow

File sender

Log in

Select the file and recipient

"sender" private key is on the chain

is encrypted with the "receiver" public key

system saves the file to the IPFS node

stores IPFS hashes to the blockchain

File Recipients

Log in

Select the files you wish to receive

The "recipient" private key verifies the identity

Download the file locally

Log is used for the system log file

The"recipient" private key decrypts the file

Figure 2. The management mechanism of platform system

- Blockchain IPFS data file management process

Blockchain IPFS is a combination of blockchain and IPFS file sharing system mechanism. Blockchain IPFS stores the uploaded satellite files, audio and video files, pictures and other data files hash value in the data block. The data file will not be changed and ensure that the downloaded data file is the same as the original uploader's data file. If the data file is changed, the downloader will still receive an updated version of the data file [8]. The data security transmission and cloud management platform adopt POA (Proof Of Authority) to achieve decentralization and fairness. Each record is encrypted by elliptic curve digital signature algorithm, and a large number of messages are shortened into a hash value through Merkle Tree to ensure that the data is stored in the data block without being tampered with. Use a timestamp server (Timestamp Server) to ensure the sequence of blocks [9]、 [2].

The operation of blockchain IPFS and the sample of blockchain IPFS work are shown in Figure 3 and Figure 4.

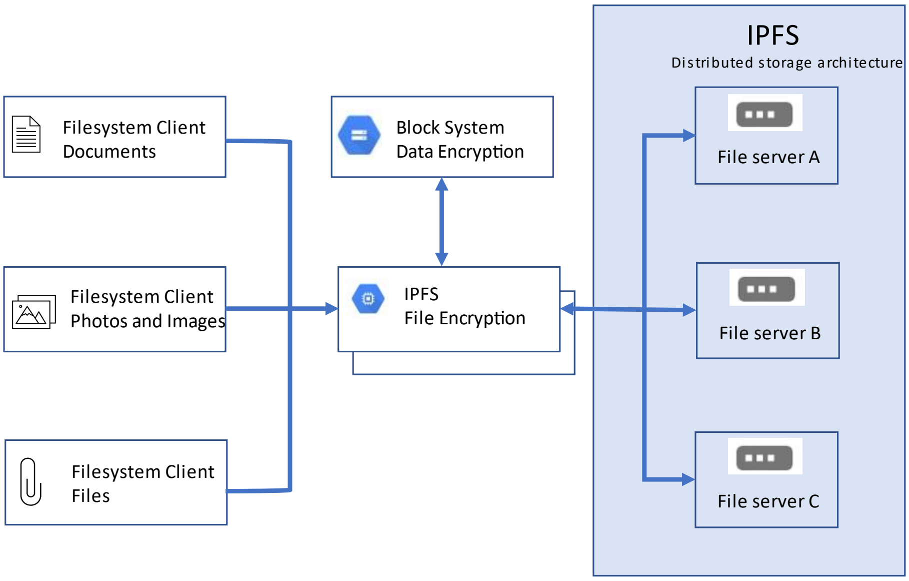


Figure 3. The operation of blockchain IPFS.

- Asymmetric encryption technology integrates the data file management process

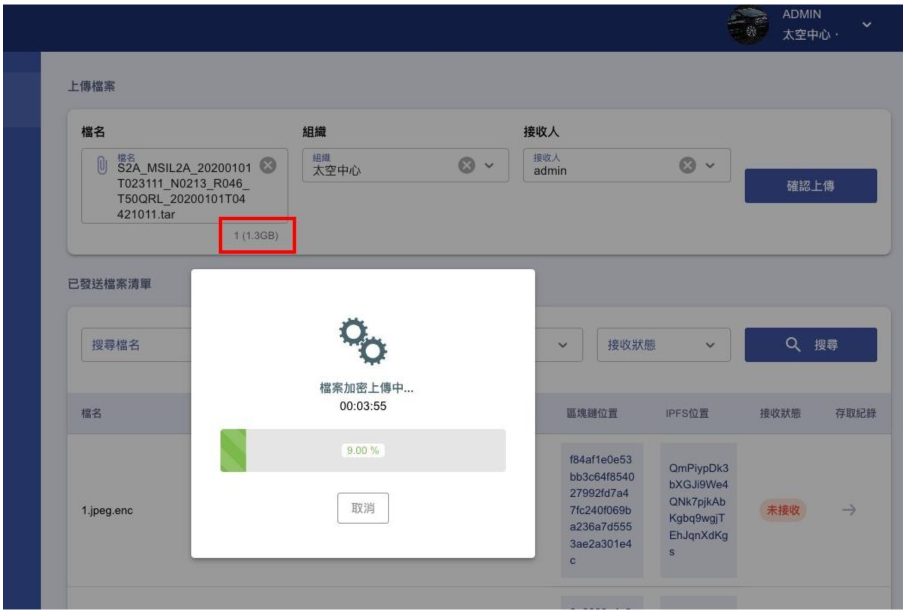
When NSPO user creates an asymmetric encrypted key, it will generate two paired keys: one "private key" and one "public key.” The "private key" will be delivered to the user in various storage methods, and the "public key" is stored in the cloud with a management mechanism. When the file is uploaded with public key encryption, the recipient uses the "private key" to unlock the corresponding "public key" encrypted file. The private key and the public key are generated in pairs, which will only be one group in the world that cannot be duplicated [10].

- Problems faced by large file transfers

(1) In order to ensure the information security of the file transmission process, front-end encryption and decryption need to be performed before uploading. Due to the cache capacity of the browser, it will not be able to handle the encryption and decryption of large files.

(2) The upload of large files is limited by the memory and browser cache capacity of the uploading computer. The time out problem caused by insufficient memory browser crash or long downtime often occurs. iOne has overcome these problems by using file cutting technology encryption

when uploading and downloading large files, and can complete files above 1G in a reasonable time is shown in Figure 4



ADMIN
太空中心 ·

上傳檔案

檔名: S2A_MSIL2A_20200101T023111_N0213_R046_T50QRL_20200101T04421011.tar
1 (1.3GB)

組織: 太空中心

接收人: admin

已發送檔案清單

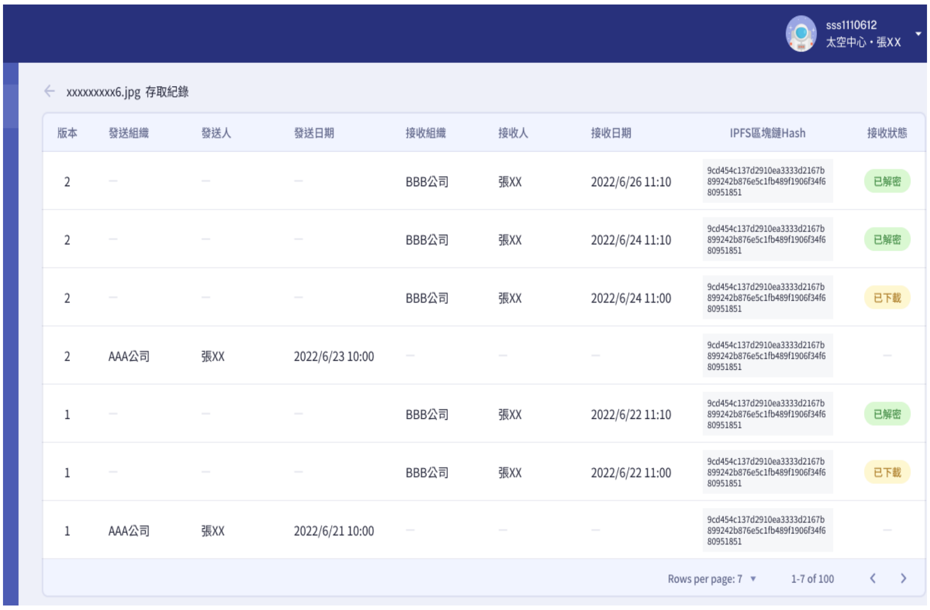
檔案加密上傳中...
00:03:55
9.00 %

檔名	區塊鏈位置	IPFS位置	接收狀態	存取紀錄
1.jpeg.enc	f84af1e0e53bb3c64f854027992fd7a47fc240f069ba236a7d5553ae2a301e4c	QmPiypDk3bXGJi9We4QNk7pjkAbKgbq9wgjTEhJqnXdKgs	未接收	→

Figure 4. Using file cutting technology encryption to solve upload and download problems.

- Data transmission cloud node and efficiency analysis and evaluation
  File transmission speed is also very important. We apply the national high-speed network center cloud computing environment to build a cloud platform and set up three nodes (VM) processing. In the future, according to the size of the data file uploaded by the space center, the IPFS file sharing mechanism will be tested to adjust whether to increase the node (VM) or increase the server specification (VM), and set the mechanism to generate a block time through the tuning process to improve the exchange speed and efficiency of satellite telemetry data files on the network [11]、[7]

- The platform records all files uploaders and recipients on the blockchain, and these records will not be tampered with, which can be used as an important basis for tracking and analysis is shown in Figure5.



sss1110612
太空中心・張XX

xxxxxxxxx6.jpg 存取紀錄

版本	發送組織	發送人	發送日期	接收組織	接收人	接收日期	IPFS區塊鏈Hash	接收狀態
2	—	—	—	BBB公司	張XX	2022/6/26 11:10	9cd454c137d2910ea3333d2167b899242b876e5c1fb489f1906f34f680951851	已解密
2	—	—	—	BBB公司	張XX	2022/6/24 11:10	9cd454c137d2910ea3333d2167b899242b876e5c1fb489f1906f34f680951851	已解密
2	—	—	—	BBB公司	張XX	2022/6/24 11:00	9cd454c137d2910ea3333d2167b899242b876e5c1fb489f1906f34f680951851	已下載
2	AAA公司	張XX	2022/6/23 10:00	—	—	—	9cd454c137d2910ea3333d2167b899242b876e5c1fb489f1906f34f680951851	—
1	—	—	—	BBB公司	張XX	2022/6/22 11:10	9cd454c137d2910ea3333d2167b899242b876e5c1fb489f1906f34f680951851	已解密
1	—	—	—	BBB公司	張XX	2022/6/22 11:00	9cd454c137d2910ea3333d2167b899242b876e5c1fb489f1906f34f680951851	已下載
1	AAA公司	張XX	2022/6/21 10:00	—	—	—	9cd454c137d2910ea3333d2167b899242b876e5c1fb489f1906f34f680951851	—

Rows per page: 7 ▾ 1-7 of 100 ‹ ›

Figure 5. File sent and received access records.

4. Benefits

- Advanced blockchain platform technology can replace traditional image transmission methods

  After the successful implementation of this blockchain platform, all future data file transmission, sharing and download will be quickly completed on this cloud platform, so data files can be safely transmitted and data will not be tampered with and traceable.

- Blockchain IPFS technology can replace traditional file transmission and sharing

  The disadvantage of the current file transfer and sharing is that there is no platform to manage who shares the data file with. The shared file cannot confirm that it is the same file as the original file, and centralized file storage cannot ensure the security of the file. The application of blockchain technology to operate data archives in data security transmission and cloud management platform can achieve four management benefits: file synchronization, file authenticity, full monitoring, and clear responsibility.

- This platform is extensible

  In the future, the platform can be expanded through API intermediary with heterogeneous systems, such as integration with satellite telemetry technology. That is, according to the needs of different users, different satellite telemetry methods, international satellite telemetry cooperation, planning satellite telemetry image file sharing content and methods, can be applied to this platform.

- Other applications

  The file transmission platform built with blockchain asymmetric encryption and IPFS technology can not only solve the transmission problem of important and confidential files between government agencies, but also be applied to the transmission between military and wartime military orders in the future, which will not be hacked and will not receive false orders, etc., to ensure the absolute accuracy of information.

5. Conclusion

This report discusses the development of the blockchain encryption system with data security transmission and cloud management platform for NSPO applications in Taiwan. It is crucial to manage the complete operation process of file transmission with the technology of blockchain IPFS file sharing and asymmetric encryption. The establishment of this platform is expected to enhance the security of file transmission with distinct institutional units. Advanced technologies for NSPO and the related applications can be developed based on this platform in the future [3].

References

[1] B. Guttman, D. R. White, T. Walraven, “Digital Evidence Preservation: Considerations for Evidence Handlers,” NIST Interagency Report, NIST IR 8387, 2022, https://doi.org/10.6028/NIST.IR.8387

[2] J. Benet, “IPFS-content addressed, versioned, P2P file system,” arXiv preprint, 2014, https://arxiv.org/abs/1407.3561

[3] E. Daniel and F. Tschorsch, "IPFS and Friends: A Qualitative Comparison of Next Generation Peer-to-Peer Data Networks," IEEE Communications Surveys & Tutorials, 24, 1, 31-52, 2022, https://ieeexplore.ieee.org/document/9684521

[4] https://study.com/learn/lesson/cryptography-overview-uses.html

[5] Smart Logistic Blockchain Platform, http://www.ioneit.com/bp.html

[6] https://ethereum.org/zh-tw/bridges/Smart Logistic Blockchain Platform

[7] Taiwan Computing Cloud (TWCC), https://www.twcc.ai/

[8] Hashing | IPFS Docs, https://docs.ipfs.tech/concepts/hashing/

[9] https://docs.ipfs.tech/concepts/hashing/

[10] Cryptography Overview & Uses | What is Cryptography? | Study.com

[11] NCHC Block Chain as a Service (BaaS), https://baas.twcc.ai/

[12] Kubernetes, https://kubernetes.io/docs/home/