How Using Blockchain for IoT Data Preserving

Rick Lin
Morrison Academy
Taichung, Taiwan

Verna Fu
Taipei European School（TES）
Taipei, Taiwan

***Abstract*—Data preservation is to preserve and maintain data security and integrity. Whether it is personal data or enterprise data loss, it may cause extremely serious impact. In order to ensure data preservation in the Internet of Things (IoT), lots of people combine the IoT with blockchain, and use the characteristics of the blockchain to ensure the integrity of the data in the IoT. However, the traditional transmission path from the sensors in the IoT to the blockchain nodes is a very complicated path, which makes the data go through many hardware devices before reaching the destination, making the transmission process vulnerable to Man-in-the-middle Attack, Sybil Attack and other attacks. We propose a method to reduce the transmission path between IoT and blockchain, and apply it in an industrial environment with many IoT devices, which combine the IoT and blockchain, and set up blockchain nodes on Raspberry Pi or IoT controllers through containerization technology. It is to simplify the transmission path between the IoT and the blockchain nodes, and to reduce the possibility of tampering, ensuring the security and integrity of data to satisfy data preservation requirements in the IoT environment.**

Keywords—— blockchain, IoT, security, Docker, Container Technology, IOTA, Tangle

I. INTRODUCTION

With the emergence of Industry 4.0, various innovative industrial technologies, including MES or AI technology, have been unveiled. Traditional factories have gradually transformed into intelligent factories, and the IoT also plays an important role in it. As IoT devices generate a large amount of data, the data preservation requirements of security and integrity are gradually being valued. Data preservation technology has become indispensable. Currently, most of the models or technologies are implemented with encryption technology. Generally, a trusted third party is required to store the data, which may lead to data leakage or attack. In recent years, the blockchain has developed vigorously. It can ensure the security and integrity of data to satisfy data preservation requirements on the chain and solve the problem of single point of failure (SPOF) in the system. Currently, some methods have emerged to combine with blockchain to save data. However, most of the methods focus on replacing the original third-party data storage and only uploading the data to blockchain, ignoring the risks that may occur during the uploading process. In the existing method [1-2], the author uses IOTA as the blockchain for storing data in the IoT. IOTA uses a tangle network based on Directed Acyclic Graph (DAG) technology, which is different from traditional blockchains. It does not require transaction fees and has faster transaction speeds. It is often used in industrial environments. In the IoT network, data is received through sensors, computer, server, and finally uploaded to the node of the blockchain. Complicated paths may lead malicious attackers to use devices in the transmission path to attack, thereby destroying the integrity of the data.

In an Industry 4.0 environment, Manufacturing Execution System (MES) is a comprehensive dynamic software system that ensures production quality. It can help enterprises to monitor, track, record and control the data generated in the manufacturing process, from receiving orders, production and process control to products.

According to the MESA Model[3] proposed by MESA, "data collection and acquisition," "product tracking and historical records" are important components in MES. On the traditional MES, the historical record of the product will upload the data to the database in the system. However, the data stored in the database may be hijacked by hackers, and the tampered data may greatly affect the judgment of decision makers or the accuracy of AI training models. Therefore, maintaining data integrity is a major challenge for enterprises in terms of information security.

We proposes a method that can shorten the transmission path. Using Docker and containerization technologies to deploy node on a variety of different devices. Traditional virtualization uses OS-level virtualization technology, while container-based virtualization technology provides more efficient resource usage, which is easier to create and expand. It helped us set up IOTA node on the Raspberry Pi more quickly.

The main contributions of our architecture are as follows:

- Upload the data to IOTA tangle, and ensure the integrity and satisfy data preservation requirements of the data through the immutability of the blockchain.
- Use containerization technology [4] to set up IOTA nodes, which can decrease the failure of setting up nodes because there are lots of different hardware devices in the IoT environment.
- Set up the IOTA node on the Raspberry Pi and upload the data to tangle after the sensor receives the data, so that it can successfully reduce the transmission path before uploading to the blockchain.

II. BACKGROUND

IoT covers a lot of hardware devices, and there are many different communication paths between IoT devices. In order to protect the communication security between IoT devices and tangle, many studies have proposed methods to detect and avoid data attacks [5]. However, the risk of data being attacked on the transmission path is still unavoidable, so how to reduce the transmission path is the key point.

A. Transmission path selection from sensors to blockchain

Fig. 1illustrates three architecture of sending data from the sensor to the tangle in the industrial environment with IoT device. This is inspired by Wellington, Fernandes, Silvano & Roderval, Marcelino, 2020[6], The main components are introduced as follows:

- Raspberry pi with Sensors: Embed the sensor on the Raspberry Pi, and use the Raspberry Pi to connect sensors and other components.

- Computer: Used to control the sensor or preprocess the received data.
- Server: Used to control all computers and manage them centrally.
- IOTA tangle: A scalable blockchain with low transaction latency.

There are many different data transmission paths in the industrial environment, and the transmission paths are divided into three types:

(i) Set up the IOTA node on the server: After the data read by the sensors, it is sent to the computer, and the computer process the data and transfer it to the server or database, collect the data centrally, and then upload the data to the tangle.

(ii) Set up the IOTA node on the computer: After the data read by the sensor is sent to the computer, the computer will upload the processed data to the tangle through the IOTA Node.

(iii) Set up IOTA Node on Raspberry pi: After sensors send signal on the Raspberry pi, they will directly upload data to the tangle.

Architecture (i) will be used in fields that require a lot of preprocessing, which can greatly reduce transmission time. Our architecture usually exists in today's smart field, where data can be centrally managed and uploaded. However, data may be lost or hacked during the transmission process, or a single point of failure may occur during the transmission process. Architecture (ii) is more secure than the previous architecture, and the computer receives and processes the data before uploading. Architecture (iii) is the most ideal architecture in the intelligent factory, which can directly upload data to the tangle, and it can also avoid the loss of transmission data caused by SPOF, so it is able to send the data to the tangle immediately.

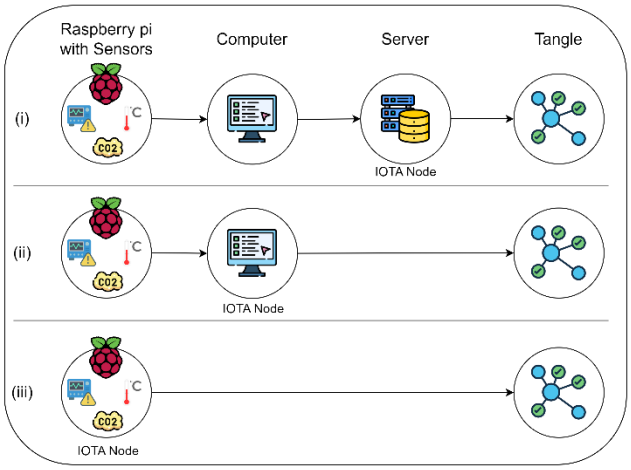

Fig. 1. Different Path to publish IoT data to blockchain

B. Tangle

When the traditional blockchain is applied to IoT, the increase in the number of transactions may lead to the consumption of handling gas fee and scalability issues. Popov proposed Tangle [7] solves the problem of gas fee and scalability. The traditional blockchain needs to use miners to verify each transaction to propose a block, and connect each block together to form a blockchain structure as linked list. Tangle proposed by the author belongs to the mesh blockchain structure. It can add new transaction blocks from any direction, improving transaction speed and ensuring its scalability. The consensus protocol adopted by Tangle is Proof-of-Work (PoW). When a transaction occurs, the node we set up will need to verify two transactions on Tangle before requesting other nodes to verify the transaction we sent. Its characteristic is that the more users can make the transaction faster.

In 2020, M. Bhandary, M. Parmar and D. Ambawade [8] proposed a method to use MAM(Masked Authenticated Messaging) technology to achieve the confidentiality of data on the IOTA chain. Our method is to ensure the integrity and confidentiality of data before uploading to the blockchain.

III. PROPOSED SYSTEM ARCHITECTURE

A. Set up IOTA Node

IOTA node allows read/write access to the tangle. Because the tangle uses Proof-of-Work (POW) consensus, it will verify transactions. When IoT device generates data and manages to upload to the tangle, first the node will verify two transactions, then it will create a transaction for the data generated by the IoT device. The transaction will be uploaded to the tangle and verified by other peers. When verification is complete, the tangle will be updated. Now, you can access the data just uploaded to the tangle through IOTA node.

Fig. 2 demonstrates how to install the IOTA node on the Raspberry pi. The main process is as follows :

1) Create Container: Install docker on the Raspberry pi and create a container by docker. It allow us to use containerization technology on our device.

2) Setup IOTA Node: Setup IOTA node by using packages on the IOTA website and modifying configuration file. The main purpose of modifying the configuration file is to increase the surrounding neighbor nodes, which is to make it synchronize with the tangle. There are many other configuration files can be modified.

3) Design a program: Design a program for uploading data to the tangle

4) Connect sensor to Raspberry pi: Connect sensors (Co2 sensor, water sensor, temperature sensor, etc.) to Raspberry pi, and design a program for collect data from sensor automatically.

5) Activate IOTA node: Enable programs that collect data and upload data simultaneously.

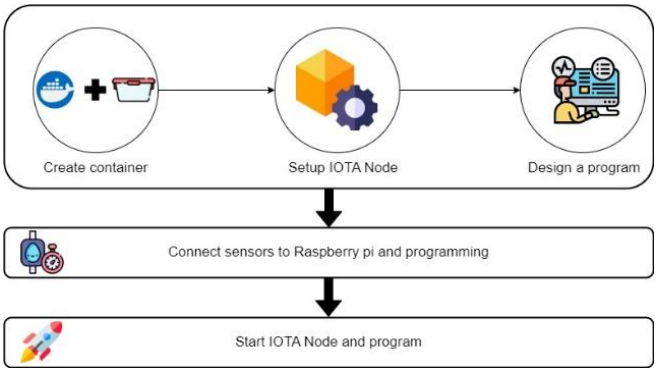

Fig. 2. A flow chart of create and setup IOTA Node in container

B. *System Architecture*

Our proposed system architecture uses IOTA tangle to ensure data integrity and satisfy data preservation requirements, it promises no fees, low transaction speed and high scalability which is suitable for intelligent factory with lots of IoT device. These devices will create lots of signals. The higher transfer speed in IoT network, the less it will cause network congestion. By using tangle DLT, data from IoT device can be uploaded to tangle rapidly. We use container technology by docker to build IOTA node, the complete data flow from sensors to tangle illustrate on Fig. 3, Steps to upload data from sensors to IOTA Tangle are given below:

Step 1: Receive all signals from sensors by using any programming language: The program define which data will be uploaded to IOTA Tangle. In IoT environment, it's common to use different program to develop application.

Step 2: Use Nodejs to connect between data from previous program and IOTA Node: In order to use Nodejs to connect with previously developed programs, the proposed architecture can use socket to connect each other or use Interprocess Communictaion （IPC）. IPC is a mechanism that allows process to access other processes data from specific memory, so IPC can also connect to previously developed programs in our proposed architecture.

Step 3: Use the iota-client module to send data to IOTA node: Send data to IOTA node, it will automatically create the transaction and waiting to be uploaded to tangle.

Step 4: Upload data to tangle: The data can only be uploaded to tangle after verifying two transactions on tangle. After upload the data to tangle, IOTA node will return a message id. The data can be search by using this message id. Transaction details are displayed after the search.

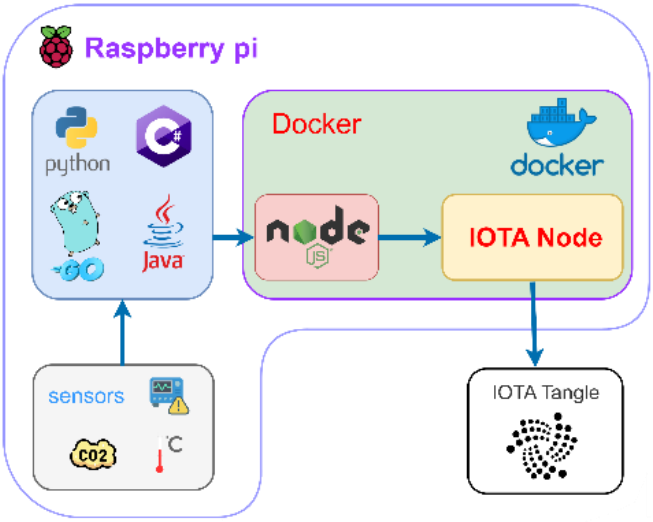

Fig. 3. Proposed system architecture showing ensuring data integrity

IV. INPLEMENTATION

A. *Hardware introduction*

We implemented that the data received by the sensor is immediately uploaded to the blockchain. Our proposed architecture can be applied in the current industrial environment, it can guarantee the integrity of the data. The implementation. In Fig.2 shows the two important components of this implementation.

- Raspberry pi: The Raspberry pi specifications are Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) 64-bit SoC, 8GB RAM and OS with Red Hat Enterprise Linux 9.
- DHT11 sensor: The DHT11 is a basic, ultra low-cost digital temperature and humidity sensor. It uses a capacitive humidity sensor and a thermistor to measure the surrounding air and spits out a digital signal on the data pin.

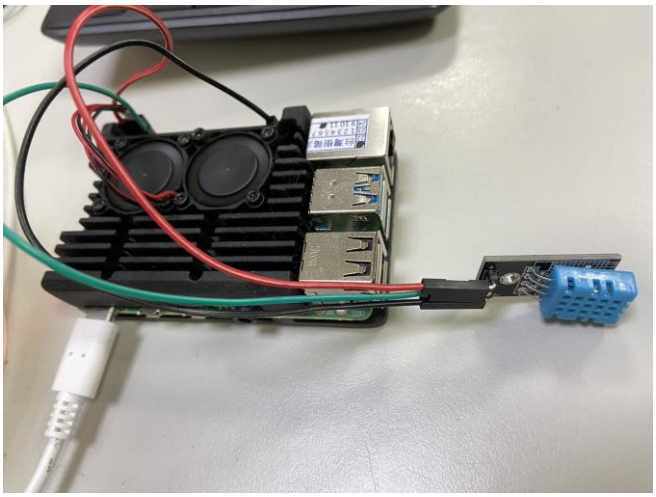

Fig. 4. Hardware in implementation.

B. *Build node with Docker*

The result of using Docker with containerized technology to set up nodes is shown in Fig.5 below. It shows that all functions have been set up, and also successfully executed.

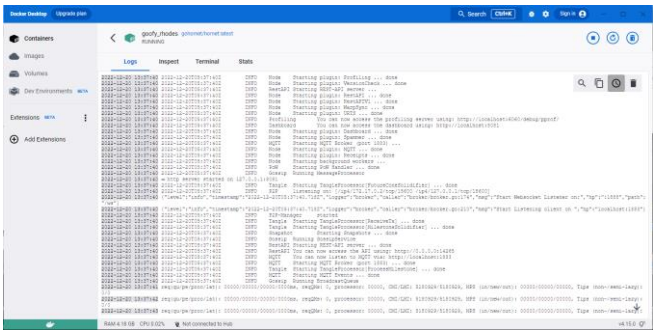

Fig. 5. IOTA node built with Docker

C. *Upload data to IOTA*

After setting up the node, we need to upload the data to IOTA tangle, Fig. 5 shows the uploaded data from dht11 sensor query using IOTA Explorer. It's a tool that you can use to search through data recorded on the blockchain.

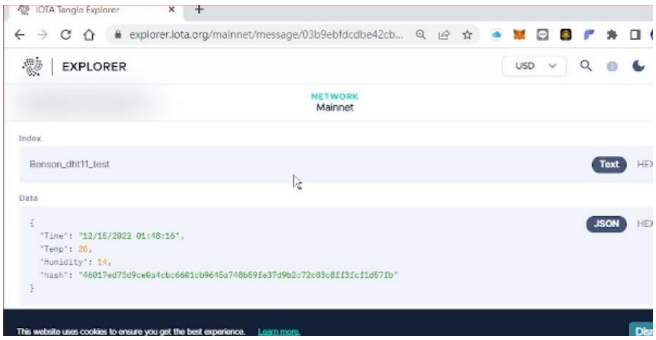

Fig. 5. Hardware in implementation.

V. CONCLUSION

In order to reduce transmission path of IoT network, we proposed a system architecture to ensure data integrity from sensors to IOTA Tangle. After the sensor generates data, the data will be uploaded to Tangle immediately. We implement an IoT environment, which can upload data from sensors to Tangle. The IoT environment is based on our proposed architecture that reduces transmission paths and ensures the integrity satisfy data preservation requirements. Our proposed architecture can be used in MES. In the traditional MES, the data including product tracking and historical records are stored in the database. Using our proposed architecture can ensure the data integrity to satisfy data preservation requirements, reducing the transmission path and avoiding the possibility of tampering. In an intelligent factory, a large amount of data generated by IoT is often used for AI training. Using our architecture can ensure the integrity of the data needed to train the model, so that the accuracy of the model will not be affected by tampering with the data. Our proposed architecture can also be applied to Environmental Social Governance (ESG). ESG is a framework that helps stakeholders understand how an organization is managing risks and opportunities related to environmental, social, and governance criteria. Applying our architecture to Co2 sensors can make the data generated by enterprises impossible to forge.

VI. REFERENCES

[1] X. Zheng, S. Sun, R.R. Mukkamala, R. Vatrapu, J. Ordieres-Meré, “Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies,” J. Med. Internet Res., 21 (6) (2019), Article e13583, 10.2196/13583.

[2] O. Lamtzidis, J. Gialelis, “An IOTA based distributed sensor node system,” 2018 IEEE Globecom Workshops (GC Wkshps) (2018), pp. 1-6, 10.1109/GLOCOMW.2018.8644153.

[3] New MESA Model: A Framework for Smarter Manufacturing, https://www.automation.com/en-us/articles/april-2022/mesa-model-a-framework-smarter-manufacturing.

[4] K. Kumar et al., “Economically Efficient Virtualization over Cloud Using Docker Containers,” IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), pp. 95-100, 2016.

[5] R. Soltani, L. Saxena, R. Joshi, S. Sampalli, “Protecting Routing Data in WSNs with use of IOTA Tangle,” Procedia Computer Science, Volume 203, 2022, Pages 197-204.

[6] W. F. Silvano and R. Marcelino, ″Iota Tangle: A cryptocurrency to communicate Internet-of-Things data,” Future Generation Computer Systems Volume 112, November 2020, Pages 307-319.

[7] S. Y. Popov, The Tangle, 2016, pp. 1–28.

[8] M. Bhandary, M. Parmar and D. Ambawade, “A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle,” 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2020, pp. 827-832, doi: 10.1109/ICCES48766.2020.9137858.