Blockchain-based Internet of Thing for Smart River Monitoring System

M K Tajudin1, M A Sarijari2, A K M Ibrahim3 and R A Rashid4

1,2,3,4Telecommunication Software and Systems Research Group, Communication Engineering Department, School of Electrical Engineering, Faculty of Engineering, Universiti Teknologi Malaysia, Skudai, MALAYSIA.

E-mail: khairultajudin13@gmail.com

Abstract. The river plays an important role in the source of water in Malaysia as it is a part of the water cycle while acting as a drainage channel for surface water. One of the major threats to its sustainability is water pollution. The conventional methods for monitoring the water quality in the river are manual and continuous monitoring that will be costly and less efficient. Hence, this paper proposes the Internet of Things (IoT) as a promising technique that can provide real-time monitoring and enhances the efficiency of data collection. To make the data secure and trustworthy, blockchain technology will be used as a platform for all the data transaction in real time. The proposed system will provide a better solution to monitor the quality of the river and for the user to interact, retrieve and analyse real and historical data.

1. Introduction
Pollution is a major threat to sustainability of river in Malaysia. The pollution of rivers results in high cost of water tariffs, threat to life, ecosystem and reduced water quality. With the social and economic development, many complex pollutants are discharged into rivers. Rivers were polluted in different degrees that not only affect human health and normal life, but also constrain economic development [1]. The cost of cleaning up the rivers also will be affected. Recently, in 2019 a major accident occurred in a Sungai Kim Kim in Pasir Gudang where the river suffered from pollution due to illegal chemical toxic dumping. This has resulted in 207 people to be hospitalized as of March 11, 2019 due to shortness of breath and vomiting. Waste dumping is a major issue for water pollution. Thus, there is a need for a secure and smart water monitoring.

Nowadays, the river water monitoring in Malaysia is conducted in limited locations and in offline mode. The main disadvantage of manual monitoring systems is that they can be highly labor-intensive to operate and relies heavily on the actions of people, which increases the possibility of human errors [2]. This in turn, raises trust issues in terms of data reliability. The traditional water monitoring procedures can be improved by using the latest technologies and real time mode with IoT.

The project starts with the use of an unmanned aerial vehicle (UAV) to monitor the water quality with the aim of commercializing the solution. Recently, UAVs has been designed and developed to carry out information, sharing of navigation, orientation for localization and sensing payloads from source to another wireless communication device mounted over them [2]. The water monitoring will be conducted using UAV combined with communication technology, smart sensor devices and
supported by narrow band Internet of Things (NB-IoT). NB-IoT supports limited mobility with cell reselection in idle state handover without any connected state mobility [3].

The sampled collected data will be stored in the database, analysed and reported based on the real-time approach and historical usage. A static and dynamic database is required to be developed, where the static database holds all the data from the sensors, the dynamic database will allow the user to query the database and retrieve certain information. The data collection must be secure and trusted during the process.

To make sure that the data collected is secure during the transactions, we implement blockchain technology to the IoT based smart river monitoring system. Blockchain is a distributed database deployed in a peer-to-peer (P2P) network where nodes in the system can create and broadcast transactions continuously [4]. Blockchain consists of blocks, which are cryptographically linked and time-stamped collections of transactions. Blocks are constantly verified by nodes in the system to stand against malicious attackers [5]. Blockchain was first introduced by Bitcoin and digital currencies. It was promised as an innovative future in collaboration and business market [6]. Bitcoin’s public ledger is the first blockchain introduced in 2009 by Satoshi Nakamoto [7].

In this paper, we investigate the IoT architectural requirements to enable the technologies that integrate with the blockchain platform. The main objective of this paper is securing the water in terms of securing the IoT system for the smart river monitoring to prevent water pollution. The IoT ecosystem suffer from security issue and by introducing blockchain, we can make the IoT ecosystem more robust. Hence, blockchain is a state-of-the-art security scheme that provides significant features to overcome the security issues in the Future Internet (FI).

The other objective of this project is to achieve data integrity to solve the trust and privacy concerns as well as to evaluate the IoT data to make sure the quality of the water is preserved and up to the requirement. The outcome of the project is a green smart river monitoring system using IoT and secured using blockchain technology.

In summary, the adoption of blockchain technology in our approach has been specifically designed to solve the problem of data transaction integrity and the security of data collection.

2. Research Structure

The project started with the design and development of the smart water sensor devices. These sensors will be integrated with an embedded board and communication technology such as Ethernet, WiFi, 3G/4G and LoRa/LoRaWAN. Detecting the pollution indicators such as pH, turbidity, ammonia, dissolved oxygen, salinity, chemical oxygen, temperature and oil content is sufficient to set an alarm for the monitoring river to start counter mechanisms [8].

Based on Figure 1, the proposed solution supports the sensors with low power consuming communication network which is LoRaWAN. Smart water sensor is using small sensor modules for getting the data into the system. The prototype for the solution consists of embedded board where a small amount of computing could be done. Water Monitoring Systems is using a low cost and compact sensor for data collection. Smart water sensor is integrated with communication devices that developed and UAV drone will be built and have that application on it. The drone is autonomous and has wireless charging systems. The collected data by the drone will be stored on the database. In which, the database will include IoT cloud server, local server, web app, and mobile app development. The database is operating as data collection for any result from the drone and sensor.
Figure 1. Flow concept of the project.

Blockchain area in this project is focusing on collected data by the drone until it finish it on analysis center through mobile and web platform. The aim of this project is to provide security in terms of data integrity. Thus, every transaction or processed data during this system is recorded in real time and the data cannot be altered.

3. Main Results
The blockchain is structured as the following. First, we use Spyder IDE for development and Flask to create a mobile app. The reason for using Flask is because of its lightweight and there is a micro-framework built in, which eliminates the need for a third party to provide functional components. Second, we use POSTMAN to carry out tests for our developed blockchain and the Application Programming Interface (API) will be built using Flask.

The aim of this project is to provide security for the IoT smart river monitoring system by implementing Blockchain technology, in order to provide security services such as data integrity and prevent data manipulation which leads to water pollution. In order to achieve this, we built a local blockchain with five nodes using the Spyder IDE, which allows the use of different virtual nodes. The blockchain network is set up in port 1000 and the nodes are in ports 1001, 1002, and 1003. Figure 2 shows the nodes and their address.

```
1 {
2     "nodes": ["http://127.0.0.1:1001",
3               "http://127.0.0.1:1002",
4               "http://127.0.0.1:1003"],
5 }
```

Figure 2. Address of the nodes
The aim of the blockchain is to preserve the integrity of the transactions exchanged by the nodes. We define the transaction in the form of JavaScript Object Oriented Notation (JSON) as shown in Figure 3. In order to save the transaction, we first create a block which will later be added to the chain. Each block has a Proof of Work (POW) and the previous hash which provides the security to the block. The creation of block is shown in Figure 4.

![Figure 3. The transactions](image)

```python
def create_block(self, proof, previous_hash):
    block = {
        'index': len(self.chain) + 1,
        'timestamp': str(datetime.datetime.now()),
        'proof': proof,
        'previous_hash': previous_hash,
        'transactions': self.transactions
    }
    self.transactions = []
    self.chain.append(block)
    return block
```

![Figure 4. Block creation](image)

After the block is created, a transaction is added to the block as shown in Figure 5. For proof of concept, the transactions include the sender, the receiver address, temperature, and the pH level of the water.

![Figure 5. Adding the transaction to the block](image)

```python
def add_transaction(self, sender, receiver, temp, ph):
    self.transactions.append({
        'sender': sender,
        'receiver': receiver,
        'temp': temp,
        'ph': ph
    })

previous_block = self.get_previous_block()
return previous_block['index'] + 1
```

The remaining step in the blockchain part is to mine the created block with the transactions as shown in Figure 6. Mining provides the hash for the created block with the transactions which cannot be forged, hence providing integrity for the blockchain without using a central system.

![Figure 6. Mining the block](image)

```python
@app.route('/mine_block', methods = ['GET'])
def mine_block():
    previous_block = blockchain.get_previous_block()
    previous_proof = previous_block['proof']
    proof = blockchain.proof_of_work(previous_proof)
    previous_hash = blockchain.hash(previous_block)
    blockchain.add_transaction('node_address',
        'receiver - node', temp = 'temp', pH = 'ph')
    block = blockchain.create_block(proof, previous_hash)
    response = ({
        'message': 'Congratulations, you just mined a block!',
        'index': block['index'],
        'timestamp': block['timestamp'],
        'proof': block['proof'],
        'previous_hash': block['previous_hash'],
        'transactions': block['transactions']}
    )
    return jsonify(response), 200
```

After setting up the blockchain we create a Web app using Flask to test the blockchain and the nodes. First, we create different routes, but we discuss the important routes and observe them in POSTMAN. The first route is connecting a node to the system as shown in Figure 7.

![Figure 7. Route connecting node](image)
Each node must send a connection request using POST. The request includes the addresses of the nodes. Figure 8 shows the results of sending POST request to connect a node.

![Figure 8. The results when connecting a node to the system](image)

Once a node is connected, now we can add transactions using add node route as shown in Figure 9. This route uses POST method; hence we need to POST the transaction.

```python
146@app.route('/add_transaction', methods=['POST'])
```

![Figure 9. Add transaction node](image)

Once a transaction is posted, we need to mine the block and append it to the chain. Figure 9 shows the result of mining the newly posted transaction. As can be seen in Figure 9, the transaction now includes the key elements of blockchain technology, which is, the previous hash, proof, and the timestamp, which makes the transaction (pH and temp values) secure and cannot be forged. Thus, data integrity is achieved and this prevents manipulation which could lead to water pollution.

![Figure 10. Mined block](image)

### 4. Conclusion

In this paper we have proposed to use blockchain technology to make a more secure and trustworthy IoT model. High-end hardware requirements for the IoT is not going to be fully integrated in a blockchain network but IoT is going to benefit from the functionalities introduced by the blockchain technology. Through these functionalities, IoT could be made highly secure.

Blockchain technology is mostly used and concentrates on the finance research area, but in this paper, we try to introduce blockchain technology for IoT to make secure data transmission between the internet connected devices. In summary, blockchain will effectively solve the trust and equity difficulty in the Internet virtual world.

### Acknowledgement

The authors would like to thank all who contributed toward making this research successful. The authors wish to express their gratitude to Ministry of Higher Education (MOHE), Research Management Center (RMC) for the sponsorship, and Telecommunication Software & System Research Group (TeSS), Universiti Teknologi Malaysia for the financial support and advice for this project. (Vot number Q.J130000.2423.04G41).
References

[1] Ying He, Songyan Qin, Yijun Ji, “Water Quality Analysis and Pollution Control Measures of Urban River in Tianjin” in 2010 4th International Conference on Bioinformatics and Biomedical Engineering, IEEE Xplore, on June 2010

[2] P. Shunmuga Perumal, A. Samson Arun Raj, B. M. S. Bharathi, G. Mohan Raju, K. Yogeswari, “UAV Assisted Automated Remote Monitoring and Control System for Smart Water Bodies” in 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), IEEE Xplore, on Feb 2017

[3] Youngjunn Moon, Seongjung Ha, Mirim Park, Dongjun Lee, Junho Jeong, “A Methodology of NB-IoT Mobility Optimization” in 2018 Global Internet of Things Summit (GloTS), IEEE Xplore, on June 2018

[4] Satoshi Nakamoto. Bitcoin: “A Peer-to-Peer Electronics Cash System”. Last accessed: November 2018

[5] Kazim Rifat Ozyilmaz, Arda Yurdakul, "Integrating Low-Power IoT Devices to a Blockchain-based infrastructure,” in 2017 International Conference on Embedded Software (EMSOFT) on, pp. 1, 2018

[6] Sara Rouhani, Ralph Deters, “Performance analysis of ethereum transactions in private blockchain” in 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), IEEE Xplore, on November 2017

[7] Oscar Novo, “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT,” in IEEE Internet of Thing Journal, Vol 5, No 2, on April 2018

[8] O. Elijah, T. A. Rahman, C. Y. Leow, H. C. Yeen, M. A. Sarijari, A. Aris, J. Salleh, T. H. Chua, “A Concept Paper on Smart River Monitoring System for Sustainability in River” in International Journal of Integrated Engineering Vol. 10 No. 7 (2018) 130-139, Universiti Tun Hussein Onn Malaysia Publisher’s Office, on November 2018