A Tangle-based High Performance Architecture for Large Scale IoT Solutions

Tsung-Fu Chiang
Department of Engineering Science
National Cheng Kung University
Tainan, TAIWAN
qzsecftbhhhh@gmail.com

Shih-Yeh Chen
Department of Computer Science and Information Engineering
National Taitung University
Taitung, TAIWAN
sychen@nttu.edu.tw

Chin-Feng Lai
Department of Engineering Science
National Cheng Kung University
Tainan, TAIWAN
cinfon@ieee.org

***Abstract*—With the development of science and technology, the use of the IoT has become increasingly widespread** [1]. **At the same time, the number of IoT devices is also growing at an exponential rate. But, many problems arise that need to be solved, including the security, flexibility, and extensibility of the IoT network and its data. To this end, we hope to strengthen the security and flexibility of networking by using the concept of virtual currency. But connecting to the virtual currency network will cause a lot of time consumption and extra costs. To reduce these additional costs, we designed two architectures and analyze them in the experiment at the end.**

Keywords—Tangle, Virtual Currency, IoT, Internet of Things

I. Introduction

In recent years, there is a new field of currency - Virtual Currency. Regardless of using the technology of much recent currency speculation, this technology has an enormous influence on the application of the Internet and it is still growing. With the progress of the Internet, there are more applications integrate with the Internet to create better the better one. However, with the increasing of the connectivity of the Internet, anyone is able to access the Internet from anywhere, and eavesdrop, modify, distribute any information at the same time. This makes it difficult for us to distinguish the information on the Internet from who or even the authenticity of it. To deal with this problem, here is a new technology called Blockchain, and its application - Bitcoin which changes the form, circulation, and management of currency.

It is valuable to use the concept of virtual currency to improve the network security, stability, and scalability of the Internet of Things(IoT) devices because of the growing number of the IoT devices. Benefiting from advances in the manufacturing of human electronic components, networkable devices have been able to be placed on a cheaper and more energy-efficient item. With these diverse and tiny installations, people can live a better life. However, it is not as good as imagined. In fact, due to the limitations of its computing resources and costs, the IoT device's security and scalability are often compromised. Imagine that in order to protect your home from burglary, you placed a camera at the doorway for having a good watch effect. However, if the camera is hijacked by an offender, the offender is able to use this camera to get some private information and even find out the daily schedule of the person living at the home. As for stability, unfortunately, your home was invaded, and indeed the camera witnessed the invasion. To make the offender caught by the police efficiently, the camera has to connect to the police system, but this is a big issue for the IoT device to be connected with the other system, because of the variety of user's environment. For another scenario, there is a factory using fully automated production, but one day, the measurement data at one of the process is abnormal. However, at this time no one in the factory can understand whether this anomalous data has been illegally tampered with, or if the production line is really in trouble. Thus, it would cost a lot of time to find out the problem, and at the same time, the production line must be stopped, which will be a huge cost. For these scenarios above, we can use the concept of virtual currency to ensure permission of the IoT device, preventing it from being abused. On the other hand, it is also possible to ensure that the source of the measurement data and instructions is not modified. In addition, with this technology, the IoT device connects to another system more flexible without heavy software or costly hardware. Hence, we use the concept of virtual currency to strengthen the network security and stability of the IoT device and minimize the extra time and cost at the meantime.

II. Relatded Work

In the basic technologies of virtual currency, Blockchain, the basic technology of Bitcoin, is currently used most widely [2] [3]. Also, it is crucial to connect Blockchain and the IoT application to the real world [4]. To achieve this scope, it will need some legal support and some system structure design. Apart from its application in the financial field, there is more and more non-financial information starting to appear in the Blockchain network. In other words, on behalf of people are trying to combine Blockchain with other areas, hoping to create innovative applications.

As everybody knows, the IoT network actually means a network composed of various networkable sensors and actuators connected to the Internet. These IoT devices can send and receive data via the Internet to achieve the "Internet access" function of all things. Thanks for the IoT devices, it is easier to control the environment in a more flexible and smarter way, while at the same time larger amounts of data were extracted from the environment more instantaneously and more accurately. Nonetheless, the security requirements of such a powerful network application are more stringent than those of the past [5]. For example, if a temperature sensor on a farm fails or is attacked, causing the temperature measurement must be 10 degrees higher than the actual value. Thus, the farm manager turns down the air conditioner to cool the farm will

978-1-5386-5059-2/18/$31.00 ©2018 IEEE
DOI 10.1109/IC3.2018.00012

bring serious damage to it. For another scenario, such as the various observation values of the life-sustainer, has a very high requirement for the accuracy of the observed numerical values. If the accuracy of the data cannot be ensured at all times, the consequences will be catastrophic. For these reasons above, by combining the Blockchain with the IoT, making it has the potential to create more secure and powerful applications different from the traditional Internet applications. With the concept of Blockchain, the related areas that have benefited include many key areas such as food safety, health, smart cities and so on [6] [7] [8].

In the practical use case, it is crucial that how to use Blockchain to record each data and track any changes in the Blockchain [9]. It proposed many solutions that are attractive to the IoT, to improve the privacy, scalability, and economy for the IoT application by using Blockchain. Although Blockchain is notorious for the time cost of transaction attachment, there is still a method which is to use privacy Blockchain to increase throughput while eliminating processing fees [9].

Even so, it is still a key issue that must be considered that how to reduce system construction costs and operating cost, while improving transaction throughput. For dealing with this problem, there is another decentralized ledger technology, the Tangle [10]. It only needs to verify the other two transactions before attaching the transaction to the Tangle network. And there is one virtual currency currently implemented using this technology called IoTA. IoTA uses the above characteristics of the Tangle to reduce the transactional additional cost, so it eliminates the need for a high calculation power and high power consumption miner. Therefore, through the combination of IoTA and IoT applications, it will have a great opportunity to solve the problem of the low response speed of the Blockchain and also to ensure the security and flexibility of the IoT application.

Despite the Tangle's performance of confirming a transaction was much better than the bitcoin's based on the Blockchain theoretically, it took several minutes to put a transaction to the Tangle network in the actual test. It is clear that there is still some distance for Tangle to be applied on the IoT.

III. Proposed Approach

To address these problems above, we designed two systems to be applied to the combination of IoT and Tangle. In these two systems, the operation in the IoT network of the accessor-to-device and the device-to-device are discussed. And the discussions mainly focus on the security of IoT network, the speed of service response, and the flexibility of the service.

A. Accessor to Device

This type of application is as conventionally conceived that the use of a mobile phone to view home conditions through a home monitor IoT device. This type of application, however, requires extremely high security and may also require high response speed and also high transmission efficiency. Thus, the monitor application, in this case, uses the Tangle network to assist in recording permissions, so that the service provider is able to complete the authentication without having to establish a central server, and the monitor must issue a permission confirmation request to any IoTA Node, which is the interface connected to Tangle. Compared with the method of controlling the security of all IoT devices by the central server in the past, the new one combined Tangle is obviously more effective. Nonetheless, due to the current reality of IoTA, not only the speed of accessing permissions is not fast enough, but the average time spent on establishing a transaction falls between minutes to tens of minutes.

Therefore, we design a system to accept permission application quickly and cache permission authentication. An IoT management device named IoT Cloud and a transaction cache database named TxDB are added to the system. With the IoT Cloud, the IoT network is able to respond to permission requests quickly, and all of these permission applications will be buffered in TxDB. After filling in buffers in TxDB, TxDB will attach these request to the Tangle through IoTA Node. Besides, this IoT Cloud can be completely decentralized, as long as a device is managed by exactly one IoT Cloud at the same time. The system is shown below.

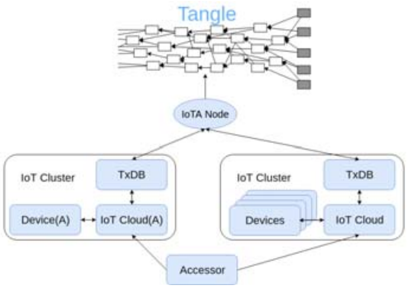

Fig. 1. The system structure of accessor-to-device model.

Multiple IoT Clusters are defined for managing devices in this system. And clusters synchronize messages with Tangle, in addition, to directly delivering messages. At the same time, each cluster needs to connect to an IoTA Node. The IoTA Node acts as a window to interact with the Tangle network. It shares a single IoTA Node among multiple Clusters, either it uses one IoTA Node per Cluster.

During actual operation of applying for permission, if the Accessor wants to operate Device(A), it must first apply for permission from IoT Cloud(A), and it cannot apply for the use of Device(A) to the IoT Cloud which is not IoT Cloud(A). And, if the application is legal then it will be accepted immediately. After the application is successful, it can actually initiate an operation request to Device(A). At the same time, Device(A) also records the operation request on Tangle through IoT Cloud(A). The following are the pseudocodes for applying for permission and getting access.

In addition, in terms of getting access, IoTCloud uses this cache in TxDB that contains permission records first, if the cache has relevant information, it does not need to access the Tangle network. Compared to an average of one to two seconds of search time for each record, the time to access the cache can be millisecond-level. With a large number of simultaneous request features of IoT applications, it is clear that cache is necessary.

Although it needs to build several IoT Clouds and TxDBs which is different from the traditional method of controlling multiple devices with one IoT Cloud, it is free to choose the number and type of devices to be controlled. Besides, it is also possible to set up any number and type of IoTA Nodes according to requirements while ensuring security and performance of IoT Cluster. In this system, the IoT Cloud accepts applications quickly, and each operation is eventually uploaded to Tangle to make sure that the record is impossible to be modified.

B. *Device to Device*

As mentioned above, if the monitor and the phone are able to cooperate, it will be possible to call the police while the house is invaded even the house's owner isn't looking at the monitor at the same time. In order to alert more accurately, devices that need to be connected may include monitors, infrared detectors, and police station reporting systems. To make the judgment even more accurate, it is necessary to link the remote artificial intelligence server. Such diverse and complicated connection methods will cause great confusion to the authentication systems.

The connection between the devices is not only for monitoring. For example, the road system which adjusts the traffic light autonomously according to the road conditions. With this IoT network, it can detect accidents or other accidents on the road through the monitor, and notify the nearby traffic lights to stop guiding the vehicle to the road having accidents, simultaneously, the road system informed the police station. For achieving this goal, it is necessary for a road system to combine a variety of devices, such as road monitors, traffic lights, police station, and also the device in this system need to establish a connection to another networkable device quickly and correctly. If this system is built as a whole, the large amount of device security will be an annoying problem. In order to reduce the coupling between IoT devices, multiple IoT Cluster is established. The devices within different IoT Cluster is able to cooperate with each other. The system is shown below.

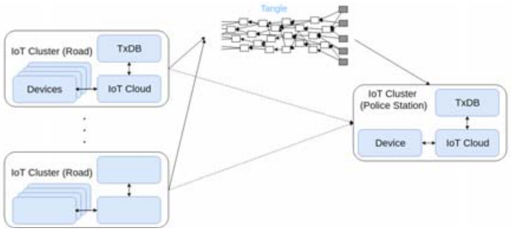

Fig. 2. The system structure of device-to-device model.

This system also contains a certain number of IoT Clusters. Besides, the size of the IoT Cluster and the device are determined based on some effective assessment methods. Once a problem is found on a road of a city road system, the IoT Cluster on the road section will gather information through the sensor to starts the emergency program and notify other IoT Clusters on the road section that may be affected and gives an alarm to the police station(dotted line). At the same time, all actions would be uploaded to the Tangle for logging(solid line).

Using this method, there are no need for a central control server, but it is allowed to respond quickly on any road section and notify the management unit at the same time. The actual operation flow is similar to that of the Accessor-Device scenario. Except, in this scenario, it must be ensured in advance that the permission has already been applied for.

IV. Experiment Result

This experiment simulates IoTCloud and Accessor to compare the time consumption of permission applications and access to the system under various parameters. The experimental equipment used this time is:

TABLE I. Hardware Specification

	Hardware			
Platform	CPU	RAM	DISK SPEED	ROLE
PC	I7-6700	40GB	7200rpm	IoTCloud/Accessor
Google Cloud Platform	vCPU*4	5.33GB	7200rpm	IoTA Full-node

[a] The speed of the network connection within the PC and GCP is 10MB/s and the delay is roughly 40ms, and the minimum weight magnitude which determines the difficulty level of attaching is set to 18.

This experiment will be divided into two parts and will be conducted through this experiment's dedicated IoTA Node.

Firstly, the speed test is performed for permission application, the performance is tested by calculating the time interval between the time of the accessor requesting for permission until accessor receiving the response. The experiment includes two parameters, test size, and buffer size. Test size is the number of the request established at the same time, and buffer size refers to the number of permission application are buffered in TxDB before sent to IoTA Node which costs tons of time. In addition, it is equivalent to the control group while the buffer size is zero.

The second part of the experiment is to simulate the accessor to getting access to IoT device, it test the speed of the query transaction. the experiment calculates. The time consumed by the accessor to initiate the connection request until the response is obtained. Besides, there are two parameters, test size and cache. Test size has the same meaning as above, and cache indicates whether to record the last permission query result. In addition, cache is not available in control group.

A. *Permission Application*

TABLE II. Apply Permission Mean Time Cost

Delay(sec)	Test Size			
Buffer Size	2	4	16	32
0	894.2945	704.6366	4921.04868	7859.4631
4	0.1317	426.3739	3777.6177	7767.6034
16	0.1299	0.2211	394.0207	4806.7102
32	0.1342	0.2293	0.7874	547.6407

The above data shows that when the buffer size is greater than the test size, its performance is good, but this is because these permissions have not actually been synchronized to the Tangle. Despite the performance is worse when the Buffer Size is equal to or less than the Test Size, the performance is clearly better than when the Buffer Size is zero, and it improves as the Buffer Size increases. This is because almost all requests can be returned immediately before the buffer is full. Only when the Buffer Size is full, the rest of the requests need to wait for the transaction to be uploaded. Thus, this method is obviously more efficient rather than uploading a transaction directly while getting an application of permission and making all the other requests waiting while uploading.

B. Getting Access

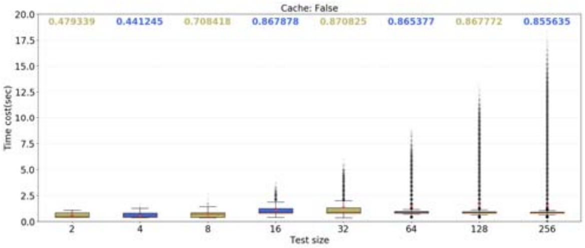

Fig. 3. The latency of getting access while the cache is not enabled.

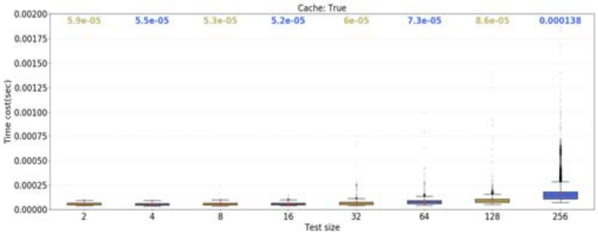

Fig. 4. The latency of getting access while the cache is enabled.

In the test, a maximum of 256 simultaneous access requests was initiated. It can be found that in the case of no cache, the response time is in second, and the distribution is also scattered. On the other hand, the cases with cache are basically below one millisecond and are more concentrated. Although the practical application must take into account the size of the cache, but considering that the size of each permission is under kb level, as long as it cooperates with a reasonable cache mechanism, the best results are achievable.

V. Conclustion

From the above experiments, it can be seen that the cache of permission and buffer of permission application are very effective for accelerating the application of Tangle to IoT devices. In terms of getting access, it can even achieve thousands of times acceleration. Although the cache space is not unlimited, it will effectively reduce the memory consumption if we allocate device properly for each IoTCloud. In addition, in the aspect of applying for permission, although it takes the same time for uploading multiple transactions one by one and uploading them as a bundle containing the same number of transactions, this structure allows a certain number of requests to return quickly. In other words, if multiple requests occur at almost the same time, the waiting time for each request will be greatly reduced. However, it must be noted that the current Tangle is not suitable for storing large amounts of data. If it is necessary to store IoT data, it will be required to use other technologies. For now, the Tangle combined with our approach is well suited as a communication intermediary between IoT devices. And, in the future, we will continue to use concept of virtual currency to enhance the security and correctness of the Internet of Things, while improving its performance and reducing deployment complexity.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] M. Swan, *Blockchain: Blueprint for a new economy*. O’Reilly Media, Inc., 2015, ch1.

[3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system, 2009,” 2012. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf. [Accessed: 16-Sep- 2018]

[4] L. W. Mcknight, R. Etwaru, and Y. Yu, “Commodifying Trust Trusted Commerce Policy Intersecting Blockchain and IoT,” March, 2017. [Online]. Available: https://ssrn.com/abstract=2944466. [Accessed: 16-Sep- 2018]

[5] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, “IoT security: Ongoing challenges and research opportunities,” *Proc. IEEE 7th Int. Conf. Service-Oriented Comput. Appl. (SOCA)*, Nov. 2014, pp. 230–234.

[6] F. Tian, “A supply chain traceability system for food safety based on HACCP, blockchain and Internet of Things,” *Proc. ICSSSM*, 2017, pp. 1–6.

[7] M. Hassanalieragh *et al.*, “Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges,” *Proc. 2015 IEEE Int. Conf. Serv. Comput. SCC 2015*, 2015, pp. 285–292.

[8] K. Biswas and A. B. Technology, “Securing Smart Cities Using Blockchain Technology,” *2016 IEEE 18th Int. Conf. High Perform. Comput. Commun.*, 2016, pp. 5–6.

[9] R. Neisse, G. Steri, and I. Nai-Fovino, “A blockchain-based approach for data accountability and provenance tracking,” in Proceedings of the 12th International Conference on Availability, Reliability and Security, ser. ARES ’17. New York, NY, USA: ACM, 2017, pp. 14:1–14:10

[10] S. Popov, “The Tangle”, *IOTA Whitepaper*, 2017. [Online]. Available: https://iota.org/IOTA_Whitepaper.pdf [Accessed: 16-Sep- 2018]