A Cooperative Evaluation Approach Based on Blockchain Technology for IoT Application

Hsing-Chung Chen[1,2*], Bambang Irawan[1,3] and, Zon-Yin Shae[1,5*]
[1] Dept. of Computer Science and Information Engineering, Asia University, Taiwan
[2]shin8409@ms6.hinet.net, [2]cdma2000@asia.edu.tw, and [5]zshae1@asia.edu.tw
[2] Dept. of Medical Research, China Medical University Hospital, China Medical University, Taiwan.
[3] Department Of Computer Science, Esa Unggul University, West Jakarta, Indonesia
[3] bambang.irawan@esaunggul.ac.id,parikesit.irawan@gmail.com
* Corresponding e-mail addresses: shin8409@ms6.hinet.net, cdma2000@asia.edu.tw, and zshae1@asia.edu.tw

Abstract. The Blockchain is the world's leading software platform for digital assets. The development of Blockchain technology is now growing very rapidly. Blockchain technology could be also deployed in the Internet of Things (IoT) Networks during their transaction processes. However, safe methods for different types of transactions still have major problems. A good trust management system (TMS) is essential for success between IoT devices and Blockchain node during transaction processes. This paper illustrates how IoT devices could be evaluated by the sink nodes acted as a blockchain nodes in order to give the contribution for cooperative evaluation in the blockchain for the integration IoT application. The cooperative evaluation method is required while executing transaction process in Blockchain network, which could validate IoT devices by these collaboration blockchain agent nodes. Finally, the scheme we proposed cooperative evaluation for private blockchain IoT application, which could give trust evaluation for IoT devices by the blockchain nodes during the blockcahin transaction processes.

Keywords: IoT, Blockchain, cooperative evaluation, trust management.

1 Introduction

Since the blockchain technology was introduced by Satoshi Nakamoto [1], blockchain technology is now growing very rapidly in various fields, among industry, social, health, agriculture and others [2, 3, 4, 5]. The blockchain is a technology that became the precursor of distributed ledger technology. It was originally developed to support the cryptocurrency, such as Bitcoin, Ripple, Litecoin, and others [2, 3, 4, 5]. Peer-to-peer transactions could occur in the absence of a third party to ensure validity and security by applying this technology. There are still many problems appeared in the integrated Internet of Things (IoT) application based on blockchain technology, *e.g.* one of them is how to secure each IoT device status [1]. Blockchain technology is

now widely integrated with a set of IoT device, but there are still many weaknesses in implementing security in IoT devices, blockchain technology seeks to address this growing security problem in a better way [5]. In this paper, we describe a blockchain agent as a node that manages blockchain software and as an interface of a set of IoT sensor devices. The blockchain agent node will also monitor the condition of the IoT sensor device, whether the condition of the IoT sensor device is "normal" or "abnormal". The condition of the IoT sensor device in this scenario consists of three conditions and can be developed again according to the requirement as described below. Blockchain agent nodes will ensure that all IoT sensor devices will be in "normal" condition, by collecting information provided by IoT sensor devices and performing a calculation operation before transacting and placing in the Blockchain network. The next step is each blockchain agent node to evaluate each other based on trust value obtained from the previous calculation stage. In this paper, we propose a cooperative evaluation method in order to support cooperative evaluation function which co-works by a set of registered IoT devices can work together in a Blockchain network.

The remainder of this paper is organized as follows: in Section 2, we introduce the related works. In Section 3, we first formalize a cooperative evaluation approach based on Blockchain technology for IoT application. Then, we present discussions in Section 4. Finally, we draw our conclusions and examine future work in Section 5.

2 Related Works

There are two subsections illustrated in this section. First, the basic Blockchain technology is described in subsection 2.1. The IoT wireless sensor network is addressed in subsection 2.2.

2.1 Basic Blockchain Technology

Blockchain or distributed ledger technology (DLT) is a protocol technology that data will be directly exchanged between two distinct users in a network without the need for intermediaries [1]. Network participants interact with an encrypted identity (unnamed); each transaction is then added to the unchanged transaction chain and distributed to all network nodes [3, 4, 5]. The blockchain is a distributed data structure that is replicated and shared among its network members. Blockchain was originally introduced as a solution for double spending on coin [6]. There are three types of blockchain technology: public blockchain, private blockchain, and consortium Blockchain [3]. Blockchain protocol is a transaction procedure stored in a distributed database that is used to maintain a growing list of records, called blocks. Each block contains a timestamp and a link to the previous block *e.g.* Bitcoin, Ethereum, Hyperledger, *etc.* [2]. In general, blockchain is managed by peer-to-peer networks that collectively adhere to certain protocols to validate new blocks [3, 4, 5, 7]. Interaction with blockchain using pairs of public key and private key. The private key is used to mark (sign) the transaction.

2.2 IoT wireless sensor network

With the IoT technology, various devices can be connected to a network and controlled remotely or automatically to get the information needed [8, 9, 10]. One that is developing today is the WSN (Wireless Sensor Network) [13]. A WSN could generally be described as a network of nodes that cooperatively sense and control the environment, allowing interaction between people or computers and the surrounding environment [11, 12]. WSNs current usually includes sensor nodes, actuator nodes, gateways, and clients.

3 Our Approach

The cooperative evaluation approach based on Blockchain technology is proposed in this section for IoT application in WSNs. The system architecture is assumed and presented in *Subsection 3.1*. Moreover, the system processes and procedures are presented in *Subsection 3.2*.

3.1 System Architecture

The access control handling and authentication issues are the most challenging problems in IoT currently [4]. We want to propose cooperative evaluation approach to measure the trust level of blockchain agent nodes that communicate each other. In general, we give an overview of the system architecture shown in Fig. 1, which there are 4 components that will be used in the system architecture are as follows:

1. Blockchain agent node;
2. Wireless sensor network;
3. Blockchain database (“distributed ledger”);
4. Private Blockchain network.

The blockchain agent node is a node that can be a sink. It is an interface to connect IoT wireless sensor devices that receive information encoded by a protocol, *e.g.* IAPF (Constrained Application Protocol) IETF RFC [5]. The blockchain agent node will connect to other blockchain agent nodes to authenticate the trust level before forwarding the transaction to the Blockchain network. The wireless sensor network is a set of IoT sensors that can be controlled remotely or automatically connected to the network. Each device will be uniquely identified to interact with the Blockchain network through the blockchain agent node. Then, it obtains a public and private key pair from the public key generator. The task of IoT sensor device provides information to blockchain agent node about the monitored area condition. It consists of three symbolized conditions as mentioned below. One binary bit represents a condition where bit "1" denotes an abnormal condition and the bit "0" indicates a normal state. Transactions performed by an IoT sensor device will be stored on the ledger distribution at the Blockchain network. A Blockchain database is the Blockchain distributed ledger stored all transactions performed by IoT sensor devices in a private Blockchain network. This Blockchain database could be also used as a corresponding blockchain agent node to determine trust level in the Blockchain

network. The private Blockchain network is one type of blockchain technology that exists. Thus, we propose a system based on private blockchain and it can be extended to a public blockchain that has its own cryptocurrency. As explained previously, in private blockchain, write-permissions are stored centrally in one node.

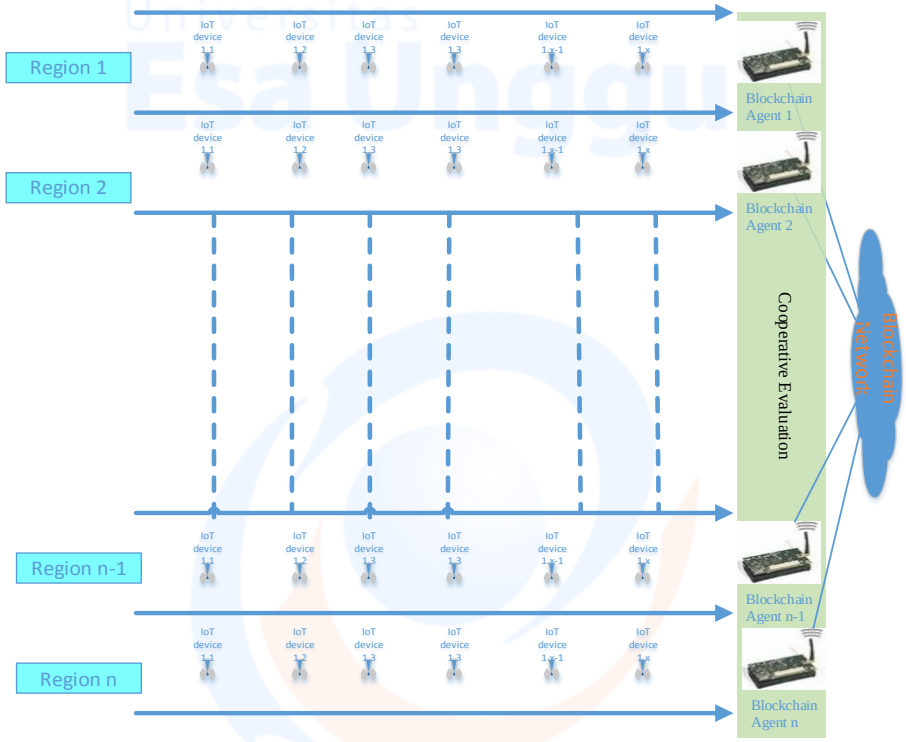

Fig. 1. The overview of the system architecture.

3.2 The system processes and procedures

The system processes and procedures are presented as followings. Each region has several IoT sensor devices that will provide information or events about the environment. Previously, the IoT sensor device performs registration phase on the blockchain agent node in each region. The blockchain agent node will collect the information and events provided by each IoT sensor device. After collecting information stored in the blockchain agent node ledger database, among the blockchain agent nodes will do a cooperative evaluation. It sees the behavior of the condition of each IoT sensor device. Whether the IoT sensor device is in abnormal condition before any further transactions between blockchain agent nodes. Blockchain agent nodes will perform authentication based on trust level before forwarding the transaction to Blockchain network. Each IoT sensor device sends a subregion monitored information signal to the blockchain agent node in each region. The blockchain agent node will collect and calculate the information obtained by using the formulas listed in definition 1 to monitor the condition of each IoT sensor device as in

Stage 1. Next, the blockchain agent node will evaluate each blockchain which are the transaction records stored in Blockchain database by using some trust evaluation algorithms [14, 15, 16] in order to detect out the untrusted the Blockchain agent node and his IoT devices. It will be described in **Stage 2**.

Stage 1

In this case, the normal conditions can be explained as follows. Each IoT sensor device provides information to the blockchain agent node that is the use of the subregion sent at a certain time. Then the blockchain agent node will collect and write the data into the Blockchain database within a specified time period *e.g.* in every 5 minutes. The IoT sensor device will send an information signal consisting of 3 bits where the first bit (1st) represents *Condition 1*, the second bit (2nd) represents *Condition 2*, and the third bit (3rd) represents *Condition 3*. The bit "0" represents satisfied and "1" for an unsatisfied condition respectively. Finally, the three IoT sensor device information conditions are shown Fig. 2 below. The trust operation by adopting ' Θ ' trust operation according to the trust evaluation algorithms in Ref. [14, 15, 16] is used to define *Definition 1* and Equation (1) shown below. From the result of sending information transmitted by IoT sensor device to blockchain agent node in each region. Then, an example is given that the trust value for the IoT sensor devices calculated by the blockchain agent node shown in Table 1.

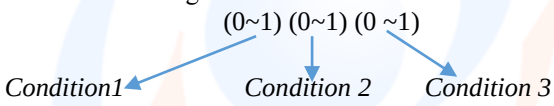

Fig. 2. Three condition information for IoT device.

Definition 1: *Assume that the trust operation for the IoT devices calulated by blickchain agent noode is represented as* $t_{S_i}^{BA_j} = t_{i,1}^{j} || t_{i,2}^{j} || t_{i,3}^{j}$, *where* $t_{i,1}^{j}$ *represents as the condition 1,* $t_{i,2}^{j}$ *represents as the condition 2, and* $t_{i,3}^{j}$ *represents as the condition 3. For example, first,* $t_{S_2}^{BA_3}$ *represents that the trust values are evaluated by a blockchain agent node* BA_3 *which evaluates an IoT device* S_2. *Second,* $t_{2,1}^{3} || t_{2,2}^{3} || t_{2,3}^{3} = 0 || 1 || 0$ *means that the trust value* $t_{2,1}^{3}$ *is the condition 1 for IoT device* S_2 *which is belonging to the blockchain agent node* BA_3, *the trust value* $t_{2,2}^{3}$ *is the condition 2 for IoT device* S_2 *which is belonging to the blockchain again* BA_3 *and trust value* $t_{2,3}^{3}$ *is the condition 3 for IoT device* S_2 *which is belonging to the blockchain again* BA_3. *Therefore, the final trust operation for all blockchain agent node during a blockchain transaction is defined as Equation (1) below.*

$$\Theta\left(t_{S_i}^{BA_j}\right)_{i=1,2,\ldots,m;\, j=1,2,\ldots n} = \Theta\left(t_{i,1}^{j} || t_{i,2}^{j} || t_{i,3}^{j}\right). \quad (1)$$

Table 1.The trust value of bit combination of the IoT sensor device to the blockchain agent node.

IoT device S_i / Blockchain agent node BA_j	IoT Devices						Trust Values
	S_1	S_2	S_3	...	S_{m-1}	S_m	$\Theta\left(t_{i,1}^{j} \mid\mid t_{i,2}^{j} \mid\mid t_{i,3}^{j}\right)$, $i=1,2,\ldots,m$; $j=1,2,\ldots n$
	$c_1c_2c_3$	$c_1c_2c_3$	$c_1c_2c_3$	$c_1c_2c_3$	$c_1c_2c_3$	$c_1c_2c_3$	
Blockchain agent node BA_1	000	000	000	...	00 0	000	$\Theta\left(t_{i,1}^{1} \mid\mid t_{i,2}^{1} \mid\mid t_{i,3}^{1}\right)_{i=1,2,\ldots,m}$
	001	001	001	...	00 1	001	
	010	010	010	...	01 0	010	
	011	011	011	...	01 1	011	
	100	100	100	...	10 0	100	
	101	101	101	...	10 1	101	
	110	110	110	...	11 0	110	
	111	111	111	...	11 1	111	
Blockchain agent node BA_2	000	000	000	...	00 0	000	$\Theta\left(t_{i,1}^{2} \mid\mid t_{i,2}^{2} \mid\mid t_{i,3}^{2}\right)_{i=1,2,\ldots,m}$
	001	001	001	...	00 1	001	
	010	010	010	...	01 0	010	
	011	011	011	...	01 1	011	
	100	100	100	...	10 0	100	
	101	101	101	...	10 1	101	
	110	110	110	...	11 0	110	
	111	111	111	...	11 1	111	
. . . .	- - - -	- - - -	- - - -	...	- - - -	- - - -	- - - -
Blockchain agent	000	000	000	...	00	000	$\Theta\left(t_{i,1}^{n} \mid\mid t_{i,2}^{n} \mid\mid t_{i,3}^{n}\right)_{i=1,2,\ldots,m}$

node BA_n					0		
	001	001	001	...	001	001	
	010	010	010	...	010	010	
	011	011	011	...	011	011	
	100	100	100	...	100	100	
	101	101	101	...	101	101	
	110	110	110	...	110	110	
	111	111	111	...	111	111	

Normal information can be explained as follows, information provided by an IoT sensor device on transactions occurring within a specified time frame corresponding to the number of costs obtained and stored to be a blockchain block stored in the Blockchain database. The transaction could be known from the public key which is generated into an address key of any IoT sensor device. The transaction is valid after it is signed by the sender's private account key. Suppose, the 6 installed IoT device sensors will have 42 states, the sensors will send data every 1 minute, and those deliver packet every 60: 6 = 10 seconds.

Abnormal conditions of IoT sensor device are illustrated below.

Condition 1:
begin
If IoT sensor device is always used or occupied and it is compared to the payment status of receiving cryptocurrency value stored in the blockchain agent database ledger, it is not in accordance with lease time.
End;
Condition 2 :
begin
If IoT sensor device always sends plentiful of abnormal information
End;
Condition 3 :
Begin
IoT sensor device never sends information.
End.

Stage 2.
In this stage, the Blockchain database will be deal with the data mining together with trust evaluation processes. Each blockchain agent node in the private Blockchain

network will evaluate each transaction record not only the record from his own managed IoT devices, but also the records from the others' blockchain agent nodes blockchain which are stored in Blockchain database by using some trust evaluation algorithms [14, 15, 16] in order to detect out the untrusted the Blockchain agent node and his IoT devices. The detail is presented below.

Each blockchain agent node receives information transmitted by IoT sensor devices as follows $\Theta\left(t_{i,1}^{j} || t_{i,2}^{j} || t_{i,3}^{j}\right)_{i=1,2,...,m;\, j=1,2,..n}$. Then, it will launch a data mining process and trust evaluation algorithm to mine according to the three condition mentioned above. Then, it will get the result whether the IoT sensor device is under one of the three abnormal conditions or not. Finally, each blockchain agent node could perform cooperative evaluation process by correspondence with other blockchain agent nodes using the trust values collected from the IoT sensor device. Moreover, the transaction information in the distributed ledger could be also accessed by all blockchain agent nodes connected to the private Blockchain network in order to evaluate each others' trust values.

4. Discussions

In this section, the current IoT and blockchain by exploring recent research and up to date trends are disscussed below. Ali Dorri et al. [9], they conducted systematic research, claiming that the IoT-based blockchain architecture handles most security and privacy threats, while considering the resource constraints of many IoT devices. Mahmoud Ammar et al. [6] conducted a systematic literature review on the IoT, their surveies had covered a subset of the commercially available framework and platform for developing industrial and consumer based IoT applications. Arshdeep Bahga et al. [12] they presented a Blockchain Platform for Industrial Internet of Things (BPIIoT). The BPIIoT platform could enable a marketplace of manufacturing services where the machines have their own Blockchain accounts and the users who are able to provision and transact with the machines directly to avail manufacturing services. In Ref. [4], they had identified the key security and trust related challenges and shown how blockchains could be used to overcome them. Also presented the design of a blockchain assisted information distribution system for the IoT and analyzed how the key security mechanisms could be built by leveraging blockchain technology. Thereefore, IoT application development has been done with various technologies to improve service and security. In this paper, the proposed approach compared with the related works mentioned above, which could be the highlighted common themes are integration IoT application based on private Blockchain network, and given trust evaluation between IoT devices and Blockchain node during the blockcahin transaction processes.

5 Conclusion

The IoT application based on blockchain technology is highly credible and developed. Due to cooperative evaluation method is getting more and more important requirement in developing the system with an integration IoT application based on

Blockchain technology. Therefore, the cooperative evaluation approach proposed in this paper, it will improve the value of trustworthiness among the blockchain agent nodes to increase the degree of a successful transaction in the Blockchain network. In addition, the blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority. Thus, the sink node in this paper acts as a blockchain agent node which could evaluate the behaviours of the managed and monitored IoT devices. It could also evaluate another blockchain agent node based on the transaction history or events logged in private blockchain network. Finally, the cooperative evaluation method proposed in this paper has an impact on enhancing security in IoT application based on blockchain technology.

Acknowledgments. This work was supported by the Ministry of Science and Technology (MOST), Taiwan, Republic of China, under Grant MOST 106-2632-E-468-003.

References

1. Swan, M.: Blockchain: Blueprint for a New Economy. 1st Edition. O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol (2015)
2. Cag, D.: [Online] https://richtopia.com/emerging-technologies/review-6-major-blockchain protocols. It had retrieved on April 20, 2018
3. Voshmgir, S., Kalinov V.: [Online] https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-ingeneral/. It had retrieved on April 20, 2018
4. Polyzos G.C., Fotiou, N.: Blockchain-assisted Information Distribution for the Internet of Things. IEEE International Conference on Information Reuse and Integration, San Diego (2017) 75-78
5. Nakamoto, S.: Bitcoin : A Peer-to-Peer Electronic Cash System. (2008) 1-9
6. Ammar, M., Russello, G., Crispo, B.: Internet of THINGS: A survey on the security of IoT framework. Journal of information security and applications, Vol. 38. (2018) 8-27
7. Kruijff, J. d., Weigand, H.: Understanding the Blockchain Using Enterprise Ontology. OTM 2017 Conferences, Greece Rhodes (2017)
8. Sun, Y. Song, H. Jara, A.J., Bie, R.F.: Internet of Things and Big Data Analytics for Smart and Connected Communities. IEEE Access, Vol. 4. (2016) 766-773
9. Dorri, A. Kanhere, S.S. Jurdak. R.: Blockchain in Internet of Things: Challenges and Solutions. eprint arXiv:1608.05187 (2016)
10. Lin, Y.P. Petway, J.R. Anthony, J. Mukhtar, Liao, H. S.W. Chou, C.F. Ho Y.F.: Blockchain: The Evolutionary Next Step for ICT E-Agriculture. Environments (2017) 1-13
11. Wang, Y. Varadharajan, V.: Interaction Trust Evaluation in Decentralized Environments. Springer, Berlin Heidelberg, Vol. 3182. (2004) 145-153
12. Arshdeep Bahga, Vijay K. Madisetti.: Blockchain Platform for Industrial Internet of Things. Journal of Software Engineering and Applications, Vol. 9 (2016) 533-546
13. Yinbiao, S. *et al*.: Internet of Things: Wireless Sensor Network. International Electrotechnical Commission, Switzerland Geneva (2014) 1-78
14. Chen, H.C.: TCABRP: A Trust-Based Cooperation Authentication Bit-Map Routing Protocol Against Insider Security Threats in Wireless Ad Hoc Networks. IEEE Systems Journal, Vol. 11. No. 02. (2017) 449 – 459

15. Chen, H.C.: A Negotiation-based Cooperative RBAC Scheme. International Journal of Web and Grid Services, Vol. 13. No. 1, (2017) 94-111
16. Chen, H.C.: A Cooperative RBAC-Based IoTs Server with Hierarchical Trust Evaluation Mechanism. The 3rd EAI International Conference on IoT as a Service (IoTaaS 2017). Taiwan, Taichung City. (2017)