A Trust Evaluation Gateway for Distributed Blockchain IoT Network

Hsing-Chung Chen[1,2](✉)

[1] Department of Computer Science and Information Engineering,
Asia University, Taichung, Taiwan
shin8409@ms6.hinet.net

[2] Department of Medical Research, China Medical University Hospital,
China Medical University, Taichung, Taiwan

Abstract. As the number of Internet of massive Things (IoT) applications in vehicles, factory machinery, smart buildings and city infrastructure grows, a secure and automated solution of enabling a mesh network for transactional processes is an important demand. However, the trust evaluation among those unknown IoT devices which communicate and trade to each other is still the high demand in distributed BC IoT network. The idea of the trust evaluation gateway is first proposed for distributed BC IoT network. Finally, the three types of trust evaluation functionfor Machine to Individual (M2I), Machine to Machine (M2M), and Individual to Individual (I2I), selectively, are proposed and provided an appropriate solution for solving the online authentication problem in distributed BC IoT network.

Keywords: Internet of things · Blockchain · Trust evaluation
Gateway

1 Introduction

As the number of Internet of massive Things (IoT) applications in vehicles, factory machinery, smart buildings and city infrastructure grows, a secure and automated solution of enabling a mesh network for transactional processes is an important demand. IoT is in search of a secure method for automating processes and exchanging data in real time to speed transactions, Blockchain (BC) technology could be one of the perfect appropriate approaches [1, 2]. Blockchain is a kind of distributed ledger technology that uses smart contract to offer a standardized method for accelerating data exchange and enabling processes between IoT devices by removing the central server [1, 2]. In a distributed Blockchain IoT network, the IoT devices on a peer-to-peer network could authenticate transactions and execute transactions based on predetermined rules without the central server. In the other words, BC technology consolidating the cryptocurrency have been recently used to provide security and privacy on transaction domain in peer-to-peer networks with similar topologies to IoT. However, the trust evaluation among those unknown IoT devices which communicate and trade to each other is still the high demand in distributed BC IoT network. A trust evaluation gateway is then proposed for distributed BC IoT network. Finally, the three

J.-L. Chen et al. (Eds.): WiCON 2018, LNICST 264, pp. 156–162, 2019.
https://doi.org/10.1007/978-3-030-06158-6_16

types of trust evaluation functionfor Machine to Individual (M2I), Machine to Machine (M2M) [3–6], and Individual to Individual (I2I), selectively, are proposed and provided an appropriate solution for solving the online authentication problem in distributed BC IoT network.

The remainder of this paper is organized as follows: the related work is introduced in Sect. 2. The system architecture of BCTEG is first proposed for distributed BC IoT network in Sect. 3. The trust evaluation is proposed in Sect. 4. In addition, the discussions and there types of trust evaluation tables are presented in Sect. 5. Finally, the conclusion is drawn in Sect. 6.

2 Related Work

Blockchain is already a payment system for the Internet, and it could be considered as the “Internet of Money” [2]. The transactions in Blockchain can be sourced and completed directly between two parties over the Internet. The assets to be allocated and traded between two parties could be tokenized as cryptocurreny in a decentralized, distributed, and global way [2]. The Blockchain network can be a programmable open network for decentralized trading of all assets, in which the functionality of cryptocurrency is beyond the traditional currency and payments [2]. Therefore, Blockchain 1.0 for currency and payments is already extended into Blockchain 2.0 to take advantage of the more robust functionality of programmable cryptocurrency. Blockchain 1.0 is for decentralization of currency and payments, whereas Blockchain 2.0 is more generally for decentralization of markets, and concerns the transfer among other kinds of assets beyond fiat currency [2]. Some terminologies of Blockchain 2.0 includes Bitcoin 2.0, Bitcoin 2.0 Protocols, smart contract, smart property, Dapp (decentralized applications), DAOs (decentralized autonomous organizations), and DACs (decentralized autonomous corporations) [2].

Public Key Cryptography is an essential part of cryptocurrency protocol and is used in several places to ensure the integrity of messages created in the protocol [7]. Wallet creation and signing of transactions, which are the core components of any currency rely heavily on public key cryptography [7]. The cryptocurrency protocol creates a new set of private key and corresponding public key [7]. For example, the public key is then used with a hash function to create the public address that Bitcoin users use to send and receive funds. The private key is kept secret and is used to sign a digital transaction to make sure the origin of the transaction is legitimate [7].

3 BCTEG System Architecture

In this section, the system architecture of the proposed trust evaluation gateway for distributed BC IoT network is shown in Fig. 1 in which the system architecture consists of Blockchain Trust Evaluation Gateway (BCTEG), Electrical Wallet (E-Wallet), Trust Evaluation Database (TE-DB), BC Network (BCN), Local IoT Network and IoT devices is illustrated in this section. In addition, the basic elements in BCTEG are described below.

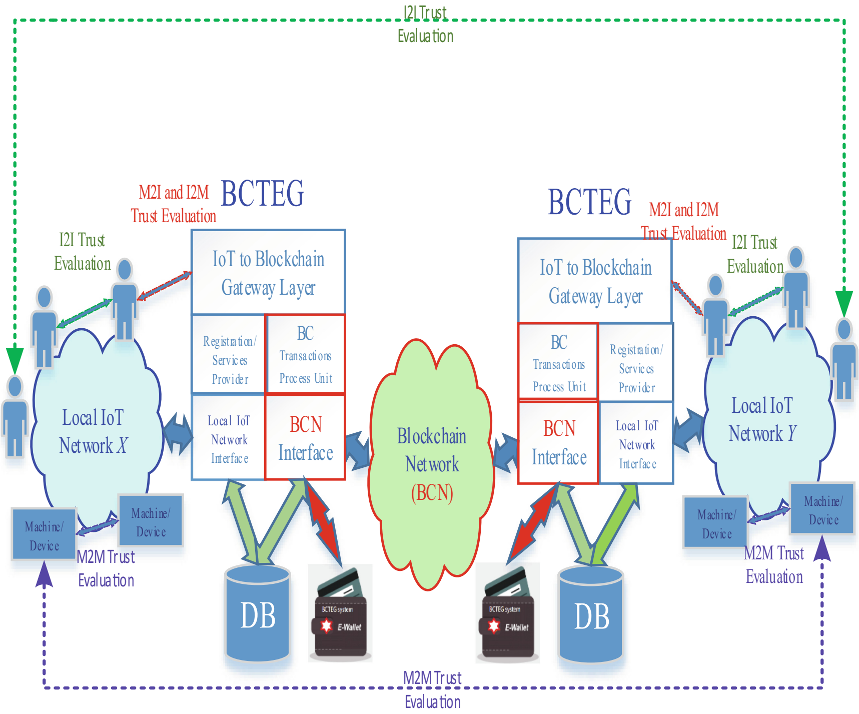

Fig. 1. The system architecture.

BCTEG is a Blockchain gateway server in Fig. 1. It supports BC protocol and serves as a BC node in BC Network. BCTEG consists of IoT to BC Gateway Layer, Registration Services Provider, Local IoT Network Interface, BC Transaction Process Unit, and BC interface. IoT devices are the digital assets belonging to the BCTEG which divided into two types: machine IoT devices and non-machine devices called individual IoT devices. Each IoT device is not a BC node in Fig. 1. Thus, BCTEG in this system architecture is proposed and designed that it could not only issue but also manage the identities for each IoT device. Moreover, BCTEG will assign a distinct as well as unique BC address according to his BC E-Wallet to each IoT device, separately. At first, each IoT device will register BCTEG using his basic identity (ID) to be a member via a secret channel. After receiving the registration request, BCTEG will generate and assign to him a private key, a public key and the corresponding BC address via the cryptocurrency wallet belonging to BCTEG. Second, each IoT device will then receive and store the information of registration. Third, each IoT device could do the BC transaction via the assigned registration information consisting ID, a private key, a public key, and a BC address.

Because each IoT device uses the distinct registration information to do any BC transaction, BCTEG will then record its activities and behaviors to TE-DB. In addition, consumers increasingly want to know that the ethical claims companies make about their products are real. Distributed ledgers provide an easy way to certify that the backstories of the things we buy are genuine. Transparency comes with Blockchain-based timestamping of a date and location—on ethical diamonds, for instance—that corresponds to a product number. Thus, BCTEG will collect all transaction information and their proof of works for each IoT device via access the distributed ledgers in BCN. Finally, BCTEG will collect all information consisting of the behaviors in local IoT network and transaction information in BCN for his all transaction records of each IoT device not only Individual but also machine IoT device via BC interface. Then, the reputation for each IoT device will be calculated via BC Transaction Process Unit and stored in TE-DB.

4 Trust Evaluation

The idea of cooperation in the three types of trust evaluation is from the terminology of Blockchain 2.0 including DAOs and DACs. Therefore, there are three types of trust evaluation function are proposed and designed in BCTEG to solving the online authentication problem in distributed BC IoT network. **Type 1** is Machine to Machine (M2M); **Type 2** is non-machine individual IoT device (called as Individual IoT device) to Individual IoT device (I2I); **Type 3** is Machine to Individual (M2I). The trust evaluation function which could deal with three types trust evaluation operations is proposed in Eq. (1) could provide an appropriate solution for distributed BC IoT network.

In Fig. 1, there are two local IoT networks, one is the local IoT network X and another is the local IoT network Y, where the local IoT network Y is the remote IoT network for the local IoT network X. In turn, the local IoT network X is the remote IoT network for the local IoT network Y.

Assume that $x \in X$ is a machine IoT device or individual IoT device and $y \in Y$ is also a remote machine IoT device or individual IoT device. The evaluation function between the local IoT device and its remote IoT device is represented as Eq. (1).

$$f(x \to y) = x\vec{\Theta}y = E_{xy}, \forall x \neq y, \tag{1}$$

where $x \to y$ means y is evaluated by x and $\vec{\Theta}$ is the evaluation operation, e.g. the trust evaluation function proposed in Refs. [4, 5] for $x \to y$.

The two properties of the evaluation function are descripted below.

1. $E_{xy} \neq E_{yx}$, $\forall x \in X, y \in Y$.
2. $E_{xx} = 1$, $\forall x \in X$ and $E_{yy} = 1$, $\forall y \in Y$.

5 Discussions

All collaboration evaluation results will be collected and recorded in system's TE-DB shown in Fig. 1. The trust evaluation tables will then be maintained by each BCTEG according to the collaboration evaluation results. In this section, the three types of trust evaluation tables are discussed below.

Type 1. The result of $f(x \to y) = f\left(m_x \to m_y\right) = m_x\vec{\Theta}m_y = E_{m_xm_y}$ according to Eq. (1) is represented as Em_1m_2 when $y = m_y$ is a remote machine IoT device evaluated by a local machine IoT device $x = m_x$. Then, the evaluation table shown in Table 1 is corrected the all results evaluated by Eq. (1) among any two IoT devices $x = m_x \in X$ and $y = m_y \in Y$.

Table 1. The all evaluation results computed by Eq. (1) between any a machine IoT device in local IoT network X and a machine IoT device in local IoT network Y.

$m_x \in Y$	$m_y \in Y$						
	m_1	m_2	m_3	$\cdots$	m_x	$\cdots$	m_z
m_1	–	Em_1m_2	Em_1m_3	$\cdots$	Em_1m_x		Em_1m_z
m_2	Em_2m_1	–	Em_2m_3	$\cdots$	Em_2m_x		Em_2m_z
m_3	Em_3m_1	Em_3m_2	–	$\cdots$	Em_3m_x		Em_3m_z
$\vdots$	$\vdots$	$\vdots$	$\vdots$	–	$\vdots$	$\vdots$	$\vdots$
m_x	Em_xm_1	Em_xm_2	Em_xm_3	$\cdots$	–		Em_xm_z
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	–	$\vdots$
m_z	Em_zm_1	Em_zm_2	Em_zm_3	$\cdots$	Em_zm_x		–

Type 2. The result of $f(x \to y) = f\left(i_x \to m_y\right) = i_x\vec{\Theta}m_y = E_{i_xm_y}$ according to Eq. (1) is represented as Em_xi_y, when $y = i_y$ is a remote individual IoT device evaluated by a local machine IoT device $x = m_x$. Next, the bit-map evaluation table shown in Table 2 is corrected the all results evaluated by Eq. (1) among any two IoT devices $x = m_x \in X$ and $y = i_y \in Y$.

Table 2. The all evaluation results computed by Eq. (1) between any an individual IoT device in local IoT networks X and a machine IoT device in local IoT networks Y.

$m_x \in X$	$i_y \in Y$						
	i_1	i_2	i_3	$\cdots$	i	$\cdots$	i_n
m_1	–	Em_1i_2	Em_1i_3	$\cdots$	Em_1i_x		Em_1i_n
m_2	Em_2i_1	–	Em_2i_3	$\cdots$	Em_2i_x		Em_2i_n
m_3	Em_3i_1	Em_3i_2	–	$\cdots$	Em_3i_x		Em_3i_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$	–	$\vdots$	$\vdots$	$\vdots$
m_x	Em_xi_1	Em_xi_2	Em_xi_3	$\cdots$	–		Em_xi_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	–	$\vdots$
m_z	Em_zi_1	Em_zi_2	Em_zi_3	$\cdots$	Em_zi_x		–

Type 3. The result of $f(x \to y) = f\left(i_x \to i_y\right) = i_x\vec{\Theta}i_y = E_{i_xi_y}$ according to Eq. (1) is represented as Ei_1i_2 when $y = i_y$ is a remote machine IoT device evaluated by a local

machine IoT device $x = i_x$. Finally, the bit-map evaluation table shown in Table 3 is corrected the all results evaluated by Eq. (1) among any two IoT devices $x = i_x \in X$ and $y = i_y \in Y$.

Table 3. The all evaluation results computed by Eq. (1) between any an individual IoT device in local IoT networks X and a individual IoT device in local IoT networks Y.

$i_x \in X$	$i_y \in Y$						
	i_1	i_2	i_3	$\cdots$	i	$\cdots$	i_n
i_1	–	Ei_1i_2	Ei_1i_3	$\cdots$	Ei_1i_x		Ei_1i_n
i_2	Ei_2i_1	–	Ei_2i_3	$\cdots$	Ei_2i_x		Ei_2i_n
i_3	Ei_3i_1	Ei_3i_2	–	$\cdots$	Ei_3i_x		Ei_3i_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$	–	$\vdots$	$\vdots$	$\vdots$
i_x	Ei_xi_1	Ei_xi_2	Ei_xi_3	$\cdots$	–		Ei_xi_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	–	$\vdots$
i_z	Ei_zi_1	Ei_zi_2	Ei_zi_3	$\cdots$	Ei_zi_x		–

6 Conclusion

In distributed BC IoT network, the trust evaluation among those unknown IoT devices which communicate and trade to each other is still the high demand. In this paper, the trust evaluation gateway is then proposed for the distributed BC IoT network in order to solve the problem mentioned above. Therefore, the three types of trust evaluation functionfor Machine to Individual (M2I), Machine to Machine (M2M), and Individual to Individual (I2I), selectively, are proposed and provided an appropriate solution for solving the online mutual trust evaluation in the proposed distributed BC IoT network.

Acknowledgments. This study was supported by the Ministry of Science and Technology (MOST), Taiwan, Republic of China, under the grants of MOST 106-2632-E-468-003 and MOST 107-2221-E-468-015.

References

1. D'Aliessi, M.: How does the blockchain work? The blockchain technology explained in simple words. a medium corporation, US (2016). https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae#.x4eu0wtnz
2. Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media, CA (2015)
3. Chen, H.-C., You, I., Weng, C.-E., Cheng, C.-H., Huang, Y.-F.: A security gateway application for end-to-end M2M communications. Comput. Stand. Interfaces **44**, 85–93 (2016)
4. Chen, H.-C.: A trusted user-to-role and role-to-key access control scheme. Soft. Comput. **20** (5), 1721–1733 (2016)

5. Chen, H.-C.: TCABRP: a trust-based cooperation authentication bit-map routing protocol against insider security threats in wireless ad hoc networks. IEEE Syst. J. **11**(2), 1–11 (2015)
6. Chen, H.-C.: A multi-issued tag key agreement with time constraint for homeland defense sub-department in NFC. J. Netw. Comput. Appl. **38**, 88–98 (2014)
7. Sharma, T.K.: How does blockchain use public key cryptography? Retrieved from https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/