Blockchain Enabled Distributed Cooperative D2D Communications

Yulan Gao[1], Mingming Wu[1], Yue Xiao[1], Ping Yang[1], Bin Fu[1], Dongyan Wang[2]
[1]The National Key Laboratory of Science and Technology on Communications,
University of Electronic Science and Technology of China, Chengdu, 611731, P. R. China
[2] Tencent, Tencent Building, Midwest District of Hi-tech Park, Nanshan District, Shenzhen, 518057, P. R. China
(e-mail: xiaoyue@uestc.edu.cn)

***Abstract*—In this paper, we propose a blockchain (BC)-enabled relay selection method in distributed cooperative communication networks, where non-cell-edge users (NCEUs) consume transmit power to relay cell edge users (CEUs) for uplink transmission in exchange for payments from CEUs. The proposed BC-enabled relay selection method aims at eliminating the failure of cooperative device to device (D2D) communication while maintaining privacy protection. By exploiting BC in the probe-reply phase, both CEU request and NCEU reply messages can be recorded in a verifiable manner. Once the feedback messages are received, the next step is decision making, which can be implemented by a two-sided matching game, in which the players include the CEUs party and the NCEUs one. In addition, the information recorded on the BC contains not only the probe-reply messages but also the optimal matching profile (e.g., transmission power sequence of NCEUs and the corresponding payment sequence of CEUs) in the second phase. The simulation results show that the proposed method is improved compared with the traditional matching scheme.**

***Keywords*—Blockchain (BC), relay selection, cooperative D2D communications, matching theory.**

I. Introduction

ONE of the main challenges faced by the design of fifth-generation (5G) wireless technologies is addressing high data rate and ubiquitous communication links for cellular users (CUs) [1]. However, for cell edge users (CEUs), the channel conditions are typically severely degraded so that the direct uplink transmissions to the base station (BS) suffer from the unacceptable quality of service (QoS). An efficient technique to address this problem is the cooperative device to device (D2D) communication which supports the transmission through the relay node, which forwards the signals received from the source node to its destination [2]– [4].

Up to now, cooperative D2D communication, with cooperative relay transmission via D2D links as its important feature, has been a critical building block to unlock the potential of 5G networks. In cooperative D2D communications, the source user equipment (UE) can choose to transmit to the target node over direct link, or cooperative relay via relay UE, according to the state of network, e.g., the channel conditions and the amount of transmitted data by the source node, etc. In addition, along with the wide spread of various wireless devices, especially with the advent of user configurable intelligent devices, employing wireless terminals acting as temporary relays may bring data integrity and privacy leakage concerns, thus, the relay selection procedure is particularly important for cooperative D2D communications. Currently, a vast corpus of literature has focused on developing relay (peer) selection methods for cooperative D2D communications [5]– [7]. However, the existing works may not provide strict means of privacy protection and data security, since there is no verification process for the reliability and trust of the relay node. If a non-trustworthy non-cell-edge user (NCEU) joins the network by any means, it can result in D2D communication failure of a certain CEU. Thus, the problem of providing successful cooperative D2D communication can be mapped into the problem of how to reliably authenticate the trust level between all communicating participants. In this context, for the cooperative D2D communication, a vast corpus of literature has focused on the utilization of the Social Internet of Things (SIoT) [8] paradigm, according to which objects are capable of establishing social relationship in an autonomous way, with respect to the rules set by their owners. The resulting social network enables faster and more trustworthy relay selection as well as significantly enhances the privacy protection by exploiting the social network of "trust" objects [9]– [11]. More precisely, the authors of [9] have proposed a game-theoretical approach to promote efficient cooperation between devices in cooperative D2D communications by leveraging the social trust and social reciprocity, respectively. The works in [10], [11] have proposed a social awareness-assisted dynamic relay selection scheme designed to balance the achieved data rate and privacy protection. However, a centralized trust management used in existing work will result in excessive overhead and make the entire network vulnerable. An efficient solution can be obtained by utilizing the features of the blockchain (BC), which can ensure trust between the devices from different individuals.

In this paper, we argue that BC technology underpinning Token [12] can provide an effective solution to promote successful cooperative D2D communications. The core idea of BC is that it realizes a distributed, verifiable, and synchronized ledger of transactions [12]. In order to motivate mobile users to serve as relays and maintain a balance in the relay forwarding service agreement, it is required to pay payment to the relay users. Without loss of generality, we assume that any form of digital currency on the Ethereum, called token, can be used to pay for relay forwarding services. This combination can

978–1–7281–1244–2/19/$31.00 © 2019 IEEE

realize privacy, data security and independent peer to peer (P2P) transactions between CEU party and NCEU one. In cooperative D2D communications, the relay selection process mainly consists of two phases: probing phase and decision making phase. Specifically, in the probing phase, the CEU may broadcast a probing message embedded with its wallet address, the size of transmission data and the public key. The NCUEs close to the CEUs can receive the message, and they will decide whether to response to the request depending on their own situations (e.g., the maximum transmit power) as well as the confirmation of CEUs' relay access rights, i.e., whether they have enough digital currency. Then, the NCEUs need to sign a confirmed probing message and destined for the corresponding source nodes (i.e., CEUs). Moreover, both the probing message of the CEUs and the reply message of the NCEUs are recorded on the BC. Once the feedback messages are received and processed by the source nodes (i.e., CEUs), the next step is decision making. The optimal selection profile can be obtained by executing the knowledge of *potential relays* (e.g., the responsive NCEUs) and two-side matching theory and will be recorded on the BC. Thus, in this transaction pattern, CEUs can choose more reliable relay nodes based on the contribution history recorded on the BC to introduce high level of effective cooperative D2D communications.

The reminder of this paper is organized as follows. In Section II, we will give the main three phases of the relay access process in the cooperative communication networks, then provide the basic background on BC technology in terms of our proposal. The system model and BC-enabled relay access protocol are presented in Section III. In Section IV, we describe the simulations and compare our findings with the traditional matching algorithm. Finally, concluding remarks are given in Section V.

II. Related Work

In this section, we present an overview of BC, and the general relay selection process in cooperative D2D communications is introduced afterwards.

A. Blockchain

BC technology was first proposed by Satoshi Nakamoto that underpins Bitcoin, and the first cryptocurrency system launched in 2008 [13]. BC is a P2P immutable ledger of blocks that inherently maintains the transactions contained within them. It is resistant to modification of data, because the ledger is distributed to any node who has participated in the network as well as the revolutionary consensus mechanism known as "Proof of Work". Thus, BC is an attractive technology for addressing the mentioned security and privacy challenges in the relay selection process as a result of its key features including decentralization, anonymity and security.

B. Relay Selection Process in Distributed Cooperative D2D Communications

The cooperative D2D communication provides a way to request forward transmission on an user equipment (UE, i.e., relay node) from an UE (i.e., source node) possibly on different networked nodes. In line with [11], cooperative D2D communication consists of three phases as: measuring phase, requesting phase and decision making phase. Moreover, the authors of [10] have updated the social trust levels (i.e., social trust) by considering the contribution history of UEs helping each other to relay data. However, the social trust recognized in this way is doubtful, since any participating user who has accessed the network can modify the history according to its interest and requirement. If it is possible to monitor the transactions between UEs, we can create centralized validation method, but this will incur excessive processing overheads and a central-authority node is needed. Even if a central-authority node helps to create validation method, the authenticity of the method will still be doubtful because the central-authority node may be destroyed by the attackers. The transactions among UEs can also be altered by malicious potential relays. For these reasons, creating reliable method of user trust verification is difficult or even impossible.

III. System Model and Blockchain Usage in Cooperative D2D Communications

In our case, for the uplink transmission of CEUs, the transmit power consumption is the performance limiting factor for CEUs since they generally operate at low signal-to-noise ratio (SNR) regimes [14]. The promising cooperative D2D communication is defined as finding an optimal relay access (e.g., collision-free access) to forward transmission.

A. System Model

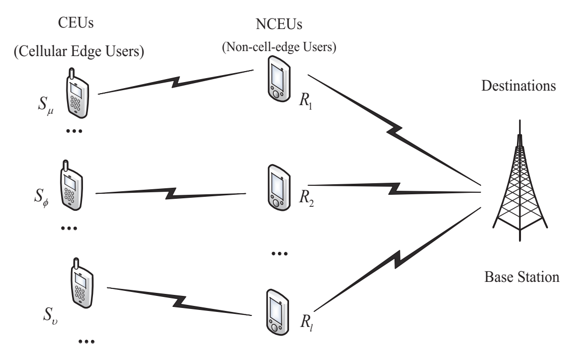

Fig. 1: Cooperative D2D communication between CEUs and NCEUs.

As depicted in Fig. 1, we consider a wireless communication network which consists of multiple NCEUs and CEUs. We assume that the CEUs are far away from the BS and require NCEUs to serve as temporary relays in order to reduce their power consumption. To motivate some NCEUs to serve as relays, it is required to pay for per relay service immediately. We consider the scenario that there are totally K mobile CEUs in our considered cooperative networks, indexed by $\mathcal{S}_k \in \boldsymbol{S} = \{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_K\}$, with the mobile-user $\mathcal{S}_k$ attempting to transmit information to the BS. We assume that all the CEUs can only access for $\mathcal{R}_l, \forall\, \mathcal{R}_l \in \boldsymbol{R} = \{\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_N\}$, with $|\boldsymbol{R}| = N$, where $|\cdot|$ indicates the cardinality of a set. Without loss of generality, we only study the optimal access in single-relay-action, i.e., each CEU is relayed by only one NCEU. In addition, we also assume that the number of CEUs is no longer than that of NCEUs, i.e., $N \geq K$.

The channels of cooperative communications are assumed to experience quasi-static block fading, i.e., the channel coefficients from the CEUs to the NCEUs, and that from the NCEUs to the BS remain constant during each time slot, but may vary from one to another [15]. In line with [16], we take the amplify-and-forward (AF) cooperation protocol as an example. This is mainly motivated by the following two factors. Firstly, the AF strategy has lower hardware complexity than the decode forward (DF) startegy and is more suitable for mobile terminals. Secondly, the temporary relay adopting the AF does not require any priori information on its received signal and can be easily implemented. Therefore, AF strategy is employed at NCEUs, and for each CEU $\mathcal{S}_k \in \boldsymbol{S}$, the cooperative transmission consists of two phases. We denote the instantaneous received SNR between $\mathcal{S}_k$ and $\mathcal{R}_n$ by $\gamma_{k,n}^{(\mathrm{R})}$, for source $\mathcal{S}_k$ in phase 2 as $\gamma_{k,\psi(k),d}^{(\mathrm{R})}$, from the direct transmission at the BS in phase 1 by $\gamma_{k,k}^{(\mathrm{D})}$, where $\psi(k) : \boldsymbol{S} \mapsto \boldsymbol{R}$ is a generic function that assigns each CEU with $\mathcal{S}_k$ as its cooperating relay access node.

B. Cooperative D2D Communication

In Phase 1, source node (i.e, CEU) $\mathcal{S}_k$ broadcasts its information signal to both each $\mathcal{R}_n$ and the BS. Therefore, the received signals at the BS d and the NCEU $\mathcal{R}_n$ can be respectively expressed as

$$y_{k,d}^{(\mathrm{D})} = \sqrt{P_k G_{k,d}^{(\mathrm{D})}}x + n_{k,d}^{(\mathrm{D})}, \tag{1}$$

$$y_{k,n}^{(\mathrm{R})} = \sqrt{P_k G_{k,n}^{(\mathrm{R})}}x + n_{k,n}^{(\mathrm{R})}, \tag{2}$$

where P_k represents the transmit power at the CEU $\mathcal{S}_k$, x is the broadcast signal with unit energy at the source device, $G_{k,n}^{(\mathrm{R})}$ and $G_{k,d}^{(\mathrm{D})}$ are the channel gains from CEU $\mathcal{S}_k$ to the relay NCEU $\mathcal{R}_n$ and that to the BS d, respectively, $n_{k,d}^{(\mathrm{D})}$ and $n_{k,n}^{(\mathrm{R})}$ are the additive white Gaussian noise (AWGNs). Without loss of generality, we assume that the noise power is the same for all the links and is denoted by σ^2. We also assume that the transmission frame length is small compared with the channel coherence time such that all the channel gains are stable over the time of interest. Without the help of NCEUs, the SNR that results from the direct transmission at the BS in Phase 1 can be written as

$$\gamma_{k,k}^{(\mathrm{D})} = \frac{P_k G_{k,d}^{(\mathrm{D})}}{\sigma^2}, \tag{3}$$

and the achievable rate of the direct transmission is

$$r_{k,d}^{(\mathrm{D})} = B \log_2\left(1 + \alpha \gamma_{k,k}^{(\mathrm{D})}\right), \tag{4}$$

where α is a constant capacity gap specified as $\alpha = -\frac{1.5}{\ln(1.5 P_{\mathsf{BER}})}$ [17], P_{BER} is the target BER.

In Phase 2, relay device (i.e, NCEUs) $\mathcal{R}_n$ amplifies and forwards it to the BS with transmitted power P_n, the received signal at the BS d is

$$y_{n,d}^{(\mathrm{R})} = \sqrt{P_n G_{n,d}^{(\mathrm{R})}} x_{n,d}^{(\mathrm{R})} + n_{n,d}^{(\mathrm{R})}, \tag{5}$$

where

$$x_{n,d}^{(\mathrm{R})} = \frac{y_{k,n}^{\mathrm{R}}}{\left|y_{k,n}^{(\mathrm{R})}\right|}, \tag{6}$$

is the unit-energy transmitted signal from NCEU $\mathcal{R}_n$ to the BS d, $G_{n,d}^{(\mathrm{R})}$ is the channel gain from NCEU $\mathcal{R}_n$ to the BS d and $n_{n,d}^{(\mathrm{R})}$ is the received noise. Substituting (1) into (6), we can rewrite the received signa (5) as

$$y_{n,d}^{(\mathrm{R})} = \frac{\sqrt{P_n G_{n,d}^{(\mathrm{R})}}\left(\sqrt{P_k G_{k,n}^{(\mathrm{R})}}x + n_{k,n}^{(\mathrm{R})}\right)}{\sqrt{P_k G_{k,n}^{(\mathrm{R})} + \sigma^2}} + n_{n,d}^{(\mathrm{R})}. \tag{7}$$

From (7) we can get the relayed SNR for CEU $\mathcal{S}_k$ in Phase 2 as

$$\gamma_{k,\psi(k),d}^{(\mathrm{R})} = \frac{P_{\psi(k)} P_k G_{\psi(k),d}^{(\mathrm{R})} G_{k,\psi(k)}^{(\mathrm{R})}}{\sigma^2\left(P_{\psi(k)} G_{\psi(k),d}^{(\mathrm{R})} + P_k G_{k,\psi(k)}^{(\mathrm{R})} + \sigma^2\right)}. \tag{8}$$

Therefore, using (4) and (8), we can calculate the achievable rate at the BS d. At a given transmission time, the achievable rate of CEU $\mathcal{S}_k$ is

$$r_{k,\psi(k),d}^{(\mathrm{R})} = \frac{1}{2} B \log_2\left(1 + \alpha\gamma_{k,k}^{(\mathrm{D})} + \alpha\gamma_{k,\psi(k),d}^{(\mathrm{R})}\right), \tag{9}$$

where the coefficient $\frac{1}{2}$ is due to the fact that cooperative transmission with the help of relay user utilizes only half of the resources (e.g., time slots, frequency bands).

C. Blockchain Usage in Cooperative D2D Communications

The above procedures in traditional cooperative D2D communications may not provide strict means of data security and privacy protection. Unlike the traditional relay selection process in the cooperative D2D communication, the probe-response messages and the optimal relay selection profile are merged into transactions in BC-base structure. Specifically, in the probing phase, we first propose a scheme using BC technology as a probe-response channel. In the decision making phase, after we have identified the *potential relays*, we need to find a proper NCEU for each CEU, especially when it has more than one candidate NCEUs and these NCEUs are candidates for reusing for more than one CEU. In addition, the final optimal relay selection profile is also stored on a block as a transaction.

1) Matching Game Formulation: We formulate the decision making phase as a two-side matching game, in Section IV, we define the utility function, which is the key concept in matching game. We assume that only one NCEU can be used per CEU. However, to get help from the NCEU, the CEU should have enough digital currency payments. Likewise, the CEU needs to rank all the NCEUs who give response messages. Therefore, our design corresponds to a one-to-one matching given by the tuple $\{\boldsymbol{S}, \boldsymbol{R}, \succ_{\boldsymbol{S}}, \succ_{\boldsymbol{R}}\}$. Here, $\succ_{\boldsymbol{S}} \triangleq \{\succ_{\mathcal{S}}\}_{\mathcal{S} \in \boldsymbol{S}}$ and $\succ_{\boldsymbol{R}} \triangleq \{\succ_{\mathcal{R}}\}_{\mathcal{R} \in \boldsymbol{R}}$ represent the set of preference relations of CUEs and NCEUs, respectively. In line with [18], we formally define the matching as follows.

Definition 1: A matching μ is defined by a function from the set $\boldsymbol{S} \cup \boldsymbol{R}$ into the set of elements of $\boldsymbol{S} \cup \boldsymbol{R}$ such that $\mathcal{S} = \mu(\mathcal{R})$ if and only if $\mathcal{R} = \mu(\mathcal{S})$.

2) BC-Based Relay Selection Scheme: Most BC implementations are devoted to optimize the decentralized currency models. For instance, recent work in [19], [20] presented a new cryptocurrency on the basis of bitcoin, which improves the scalability and flexibility of cryptocurrencies. Aside from the aforementioned cryptocurrencies, many BC implementations including, internet of things [21], robotic swarm system [22], secure logs [23], Ethereum [12] and Hyperledger Fabric [24] and so on. With any of the above three BC implementations as a basis, we can implement as follows. (1) The local storage device is an integral part of each UE, which can be used to store some of the transactions generated by the disjoint parties (i.e., CEU party and NCEU party). (2) We need any form of digital currency on the Ethereum for payment to relay forwarding service, since all the transactions are generated in the Ethereum platform. (3) UEs must periodically change their public key.

In Fig. 2, the main steps of the proposed scheme are shown and explained in more detail as the following.

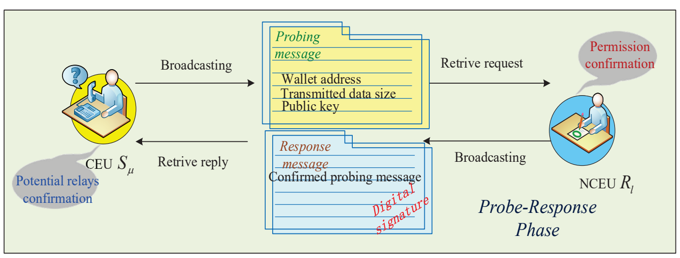

Fig. 2: The proposed blockchain-based peer selection scheme.

- *In the probing phase*: First, CEUs prepare probing messages with their wallet addresses (created by the public key), the size of the transmission data, and their public keys.
- Then, CEUs broadcast the messages, by recording the probing messages as transactions.
- The NCEUs decide whether to respond to the request, depending on their transmission capacity and the confirmation results of the CEUs (i.e, verify that the CEUs have enough digital currency). Once they decide to respond to the request, the NCEUs will prepare the reply messages.
- Then, the confirmed probing messages are signed by the NCEUs and destined for the corresponding source nodes.
- If the CEUs receive any feedback message destined to them, they enter the decision making phase.
- *In the decision making phase*: The CUEs process the feedback messages and obtain the corresponding *potential* feasible NCEUs. The collision-free relay selection can be formulated as a two-side matching game, then we define the utility functions for both parties (the details are given in the next section), and finally the preference profiles of both parties can be obtained.

Notably, the proposed relay selection scheme uses the Ethereum platform. The public key information can be exploited by the CEUs to receive and process the reply messages with their own address, since the wallet address information are encapsulated into transactions in Phase 1. Moreover, transactions are broadcasted into the network for any participating user to authenticate. It is attached to the chain if all the transactions in a new block pass the authentication process. With the help of this structure, relay selection process for the CEUs can reduce the communication and computation burden of the BS since the probe-response information is directly sent to the UEs rather than passing the messages through central manager (i.e., the BS). Aside from this, the proposed relay selection scheme can achieve high level of effective cooperative D2D communications, while guarantee both the privacy of CEUs and the instant payment for the relay forwarding service. We describe them in this order.

- *High level of successful cooperative D2D communications*: the proposed scheme is implemented on the top of a BC and uses the Ethereum platform, thus the network structure follows the P2P topologies. Moreover, in the proposed relay selection scheme, we remove the central manager (i.e., BS) and the probe-response processes are verified and authenticated by all the participating users in the network. The record of these processes is shared to all the participating users in the network. The distributed nature of BC makes a modification to the transactions on the participating users to be meaningless. Another characteristic of the proposed scheme is decentralized, which mainly refers to the management of the public ledger, i.e, all the participating users jointly maintain the public ledger. By combining BC and two-side matching scheme, the transactions recorded on the BC can provide a trusted "history contribution" of relay forwarding service. The verifiability of "history contribution" helps the CEUs to timely update their public key and reject the feedback messages from the malicious NCEUs. In addition, it also helps the CEUs to choose more reliable NCEUs, so as to achieve high level of successful cooperative D2D communications.
- *High level of privacy protection of CEUs*: the proposed scheme security mainly comes from the removal of centralized authentication mechanism, i.e., the public key is used by all the participating users for verifying each transaction. Moreover, the periodic variability of public key (i.e., the user identity) can offer a high level of privacy protection.
- *Distributed payment on time*: The proposed cooperative D2D communication uses incentive mechanism and charges on the basis of services provided by NCEUs. It should be noted that the service ledgers (i.e., the CEUs'

payment sequence) are available to all the participating nodes. BC can ensure that every transaction is documented, which helps the NCEUs to validate whether the CEUs have enough digital currency.

IV. Simulation Results

In this section, the performance evaluation of BC-based relay selection scheme was carried out using simulations. This section starts with the simulation assumptions and setup. The comparison of utility results between the proposed scheme and the traditional matching scheme is demonstrated in the second part.

A. Method for Relay Selection

We assume that any CEU $\mathcal{S}_k, \forall\ \mathcal{S}_k \in \boldsymbol{S}$ has enough digital currency to pay for the relay forwarding service of any NCEU $\mathcal{R}_n, \forall\ \mathcal{R}_n \in \boldsymbol{R}$. Once the probe-reply transactions between CEUs and NCEUs are obtained in the probing phase. The next step is to decide the optimal relay access sequence by two-side matching theory. The motivation for using matching theory for the relay selection problem is that it can tackle the combinatorial problems and achieve a distributed solution [25]. Inspired by [18], the relay selection procedure is formulated as a two-side matching game, then matching is performed by the two sets of players (e.g., CUEs party and NCEUs party) using preference profiles. The preference profile for the CEUs is based on the following preference function of the achieved data rate to cost ratio on NCEU R_n as

$$u_k(n) = \frac{r_{k,n,d}}{b_k^n}, \tag{10}$$

where b_k^n is the payment of CEU $\mathcal{S}_k$ access to NCEU $\mathcal{R}_n$.

Similarly, each NCEU $\mathcal{R}_n$ also needs to have a preference profile that ranks all the validation CEUs according to its preference function. By using a two-side matching game for our problem, we can guarantee successful cooperative transmission by the CEU defined preferences. However, how to motivate NCEUs to serve as relays is a main critical problem. One of the efficient solutions is to pay for each relay service. Then, the preference function of NCEU is given by

$$u_n(k) = b_k^n \times \frac{Q_k}{r_{k,n,d}}, \tag{11}$$

where $\mathcal{Q}_k$ is the size of CEU $\mathcal{S}_k$'s transmission data.

In line with [26], in our simulations, we always assume that there are N NCEUs to provide enough available temporary relays. For each step we increase m_s to a total of $10 + N$, with $m_s = 10$ initially where N provides enough NCEUs for providing enough available relays. According to the BC-enabled relay access protocol in Section III-B, without loss of generality, there are malicious users in both the CEU party and the NCEU party.

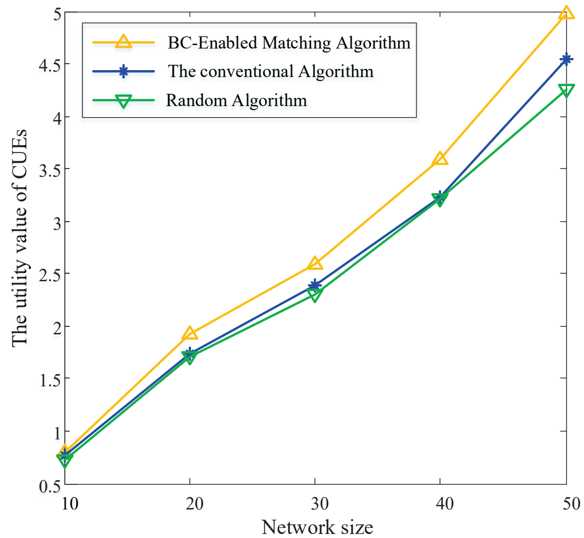

Fig. 3: The throughput of the CEUs vs. number of CEUs with and without blockchain assistance, when there are malicious users.

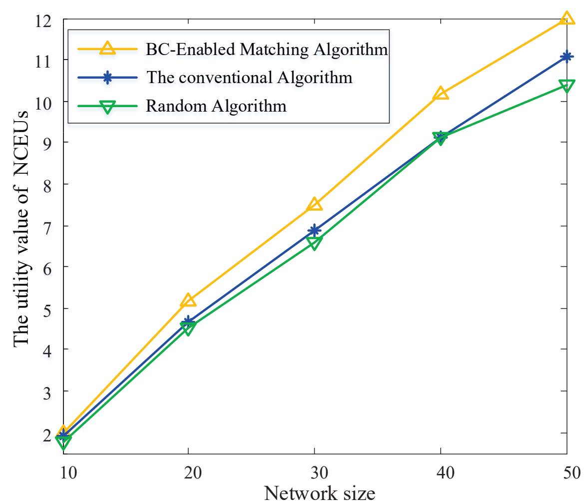

Fig. 4: The payoff of the NCEUs vs. size of network with and without blockchain assistance, when there are malicious users.

B. Performance Comparison

In order to evaluate the performance of the BC-enabled relay selection method, we show the comparison in terms of average utility under different networks sizes (i.e., the number of joined CEUs), when there are malicious users. We compare our proposed approach with two other approaches, which are denoted as random access and the two-side matching scheme, respectively.

In Fig. 3 and Fig. 4, we increase the network size (CEUs) and observe the average utility by CEUs and the average payoff (profits) by NCEUs, respectively. Obviously, we can conclude that the achieved average utility/payoff by CEUs/NCEUs in all the schemes increases with the network size. From the results we notice furthermore that, the BC-enabled matching scheme can maintain high reliability and security compared to the other schemes. The above advantages mainly due to the verification and validation action in our proposed two-side matching scheme.

V. Conclusions

In this paper, for the cooperative D2D communications, we proposed the utilization of the BC features, according to which CEUs are capable of establishing optimal NCEUs selection profile in a verifiable manner. Specifically, in the requesting phase, the CEU may broadcast a request message embedded with its wallet address and the size of transmission data, then its relay access right will be verified by the NCEU. Once the feedback messages are received and processed by the CEU, the next step is the decision making. The optimal selection profile can be obtained by executing the knowledge of potential relays (e.g., the responsive NCEUs) and two-side matching theory. Moreover, both the request-reply messages and the final optimal relay selection profile are recorded on the BC. In the presence of the malicious user, the introducing BC technology in cooperative D2D communications can not only maximize system throughput, but also ensure high level of privacy protection and data security.

Acknowledgment

This work was supported in part by the National Science Foundation of China under Grant number 61671131, the Fundamental Research Funds for the Central Universities (No.ZYGX2018J092), International Science and Technology Cooperation Project of Sichuan Province (No.2017HH0009), and the open research fund of National Mobile Communications Research Laboratory Southeast University No.2017D16.

References

[1] A. Osseiran *et al.*, "Scenarios for 5G mobile and wireless communications: the vision of the METIS project," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 26-35, May 2014.

[2] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 74-80, Oct. 2004.

[3] Y. Yang, H. L. Hu, J. Xu, and G. Q. Mao, "Relay technologies for WiMAX and LTE-advanced mobile systems," *IEEE Commun. Mag.*, vol. 47, no. 10, pp. 100-105, Oct. 2009.

[4] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3450-3460, Oct. 2007.

[5] X. Ma, R. Yin, G. Yu, and Z. Zhang, "A distributed relay selection method for relay assisted device-to-device communication system," in *Proc. IEEE 23rd PIMRC*, Sydney, NSW, Spet. 2012, pp. 1020–1024.

[6] S. M. A. Kazmi, N. H. Tran, W. Saad, H. Zhu *et al*., "Mode selection and resource allocation in device-to-device communications: a matching game approach," *IEEE Trans. Mobile Computing*, vol. 16, no. 11, pp. 3126–3141, Mar. 2017.

[7] B. Panigrahi, R. Ramamohan, H. K. Rath, A. Simha, "Dynamic relay selection and channel adaptive uplink for LTE device-to-device (D2D) communication," in *Proc. IEEE, International Symposium on Personal, Indoor, and Mobile Radio Communications*, Valencia, Spain, Sept. 2016, pp. 1–6.

[8] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (SIoT)–when social networks meet the internet of things: concept, architecture and network characterization," *Comput. Netw.*, vol. 56, no. 16, pp. 3594–3608, Nov. 2012.

[9] X. Chen, B. Proulx, X. W. Gong, and J. S. Zhang, "Exploiting social ties for cooperative D2D communications: a mobile social networking case," *IEEE Trans. Netw.*, vol. 23, no. 5, pp. 1471-1484, Oct. 2015.

[10] Y. Meng, C. X. Jiang, H. H. Chen, and Y. Ren, "Cooperative device-to-device communications: social networking perspectives," *IEEE Netw.*, no. 3, vol. 31, pp. 38-44, Mar. 2017.

[11] Y. Meng, C. X. Jiang, Q. D. La, T. Q. S. Quek, and Y. Ren "Dynamic social-aware peer selection scheme for cooperative device-to-device communications," in *Proc. Wireless Commun. Netw. Conf.*, San Francisco, CA, USA, May 2017.

[12] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, 2014.

[13] S. Nakamoto, "A peer-to-peer electronic cash system," [Online]. Available: http://reed.cs.depaul.edu/lperkovic/csc536/lecture10/bitcoin.pdf

[14] D. Tse and P. Viswanath, "Fundamentals of Wireless Communication." Cambridge, U. K.: Cambridge Univ. Press, 2005.

[15] D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, G. Feng, and S. Li, "Device-to-device communications underlaying cellular networks," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3541-3551, Aug. 2013.

[16] B. Xie, W. A. Zhou, C. X. Hao, X. L. Ai, and J. D. Song, "A novel bargaining based relay selection and power allocation scheme for distributed cooperative communication networks," in *Proc. Veh. Techn. Conf.*, Ottawa, ON, Canada, Sep. 2010, pp. 1-5.

[17] A. J. Goldsmith and S.-G. Chua, "Variable-rate variable-power MQAM for fading channels", *IEEE Trans. Commun.*, vol. 45, pp. 1218-1230, Oct. 1997.

[18] S. M. Ahsan Kazmi, *et al.*, "Mode selection and resource allocation in device-to-device communications: a matching game approach," vol. 16, no. 11, pp. 3126-3141, Mar. 2017.

[19] Bitcoin source at GitHub.(Verified on 2017/4/23). [Online]. Available: http://github.com/bitcoin/bitcoin

[20] G. Danezis and S. Meilejohn, "Centrally banked cryptocurrencies," in *Proc. NDSS Symp.*, San Diego, CA. USA, May 2016, pp. 1-14.

[21] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292-2303, May 2016.

[22] E. C. Ferrer, "The blockchain: a new framework for robotic swarm systems," *arXiv preprint arXiv: 1608.00695,* 2016.

[23] B. Schneier and J. Kelsey, "Cryptographic support for secure logs on untrusted machines," *USENIX Security*, 1998.

[24] Hyperledger/fabric. (Verified on 2017/4/23). [Online]. Available: https://github.com/hyperledger/fabric

[25] S. M. Ahsan Kazmi, N. H. Tran, W. Saad, L. B. Le, T. M. Ho, and C. S. Hong, "Optimized resource management in heterogeneous wireless networks," *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1397-1400, Jul. 2016.

[26] K. Kotobi and S. G. Bilén, "Blockchain-enabled spectrum access in cognitive radio networks," in *Proc. IEEE Wirelss Telecommun. Symposium*, Chicago, IL, USA, Apr. 2017, pp. 1-6.