IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 10, 2020, accepted April 28, 2020, date of publication June 1, 2020, date of current version June 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2998803

An Improved Proof-of-Trust Consensus Algorithm for Credible Crowdsourcing Blockchain Services

XIAOYU ZHU[1], YI LI[2], LI FANG[1], AND PING CHEN[3]

[1]Beijing Laboratory of Advanced Information Networks, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]Key Laboratory of Universal Wireless Communication, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China
[3]School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

Corresponding author: Yi Li (liyi@bupt.edu.cn)

ABSTRACT In online crowdsourcing services, credible accountability mechanisms are crucial for guaranteeing a good interactive environment. However, the crowdsourcing systems are established in virtual environments, the identities of the participants are various and complicated, the systems could scarcely identify malicious nodes automatically. So it is very hard to preserve the complete evidence of malicious behaviors and investigate relevant legal responsibilities. Blockchain is regarded as a very promising solution to these problems because it possesses characteristics of decentration, non-modifiability and traceability. However, a main challenge is to design an applicable blockchain consensus algorithm which can reach an agreement on credibility of participants automatically, prevent transaction data from tampering, and trace to the source of malicious behaviors. In this paper, an improved Proof-of-Trust (PoT) consensus scheme is proposed with the underlying technology of blockchain, which is properly to the crowdsourcing service scenarios. Firstly, this PoT consensus selects nodes with high credibility using subjective logic reputation algorithm. Only selected nodes have the chance to generate blocks, participate in verification, and claim crowdsourcing tasks. Secondly, the choice scheme of generate-block nodes is further optimized through the unpredictability of timestamp and digital signature. Moreover, an incentive mechanism based on game theory is designed in this consensus. With this mechanism, candidate nodes prefer to give honest verification results rather than engage in collusion with malicious nodes. The analysis and simulation results demonstrate the effectiveness, feasibility and scalability of the proposed approach.

INDEX TERMS Blockchain, crowdsourcing, reputation model, incentive mechanism.

I. INTRODUCTION

With the rapid growth of the global sharing economy, crowdsourcing has become a very active Internet service, and has been widely used in various fields of Internet economy. However, all crowdsourcing platforms are facing with a critical problem to be solved: how to ensure that every participant can strictly abide by crowdsourcing agreements in the trading process? There is no trusted third party to monitor whether providers and consumers meet their engagements or not during the execution of the crowdsourcing contract. In the event of a dispute, it is very hard to arbitrate and investigate for responsibility according to law. This will seriously hinder the healthy and sustainable development of crowdsourcing services.

Because there is no credible centralized regulator, it's necessary to establish a decentralized accountability mechanism to ensure healthy operation of crowdsourcing services. This kind of mechanism depends on the transparency of contract execution, consistency of work logs, traceability of service process, etc. Blockchain technology happens to have these characteristics, providing an important solution to such problems. Nevertheless, the integration of blockchain technology into crowdsourcing service systems is a major challenge, the biggest obstacle of which is that existing consensus algorithms are hardly applied to crowdsourcing service scenarios.

At present, PoW, PoS and DPoS are the most widely used public blockchain consensus algorithms. PoW is difficult to apply in large-scale online service systems owing

The associate editor coordinating the review of this manuscript and approving it for publication was Patrick Hung.

to large consensus latency, low throughput and high energy consumption. Although PoS [1] has the characteristic of low consensus latency and high throughput, it has the tendency of centralization and the fairness becomes weaker. If used in crowdsourcing service scenarios, the rights and interests of newly admitted nodes may be compromised compared with older users. DPoS [2] is an optimized and ugraded version of PoS, which further shortens the delay, improves consensus efficiency, and compensates for the lack of fairness through democratic voting. But DPoS still has a certain degree of centralization, so there are potential security risks. DPoS, similar to a joint-stock company, cannot prevent collusion between main shareholders if used in crowdsourcing scenarios. Reference [3] presents a ‘‘Proof-of-Trust’’ (PoT) consensus protocol which integrates a trust component and incentive measures to address the unfaithful behaviors that often occur in crowdsourcing services. The PoT protocol avoids the low throughput and high energy consumption. However, in the consensus process of PoT protocol, the only leader selected by Raft algorithm may be unreliable. This is because Raft has high efficiency but poor safety. In addition, for each validator candidate, the followers check their own trust database to select validation nodes in PoT, but the specific selection basis is not given in the protocol. Finally, if the reward and punishment mechanism of PoT is applied to the actual scene, nodes still have a great probability to implement malicious behaviors.

As stated above, blockchain consensus algorithms suitable for crowdsourcing service systems should be designed to effectively solve the problem of mutual trust among participating members. Because even with the distributed accountability infrastructure, the procedure of accountability after the event is always cumbersome. At present, most of the current research on reputation algorithms focuses on the improvement of traditional reputation algorithms. Since Resnick *et al.* proposed credibility [4], its researches and applications have received great attention of researchers. Minhas *et al.* present a reputation model based on multiple factors to detect malicious nodes, which combines roles, experience, priorities, and majority-based trusts for real-time decision making [5]. Gurung *et al.* put forward a trust model that directly evaluates message credibility based on content similarity, content conflict, routing similarity and other factors [6]. He *et al.* used a watchdog to monitor the behavior of neighbors. If an erroneous behavior is detected, the user broadcasts the neighbor's uncooperative reputation to other users in the network [7]. Although there are many related achievements of reputation algorithms, very few of them are applicable to crowdsourcing.

This paper combines the crowdsourcing with blockchain consensus process, designs a reputation algorithm appropriatefor the crowdsourcing and presents an improved Proof-of-Trust consensus scheme. Its main contributions are summarized as follows:

1. The improved PoT consensus uses subjective logic algorithm to optimize the choice of consensus nodes, and utilize timestamps and digital signatures to increase the unpredictability of generate blocks nodes. Improved algorithm can automatically finish reputation evaluation of crowdsourcing participating members. The division standard of reputation must be complied with by all members, thus greatly reducing the probability of malicious members participating in the crowdsourcing.

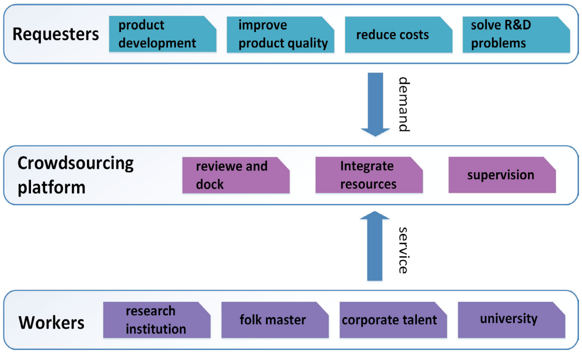


FIGURE 1. Crowdsourcing business model.

2. The improved PoT consensus algorithm can ensure participating members have equal opportunities to take part in crowdsourcing activities. Due to variability of reputation values, the consensus nodes will not be a few fixed members. So, the fairness of the improved algorithm is significantly better than the existing PoT protocol.

3. We propose an incentive mechanism based on game theory, and ensure that honesty is the best strategy for each node by setting appropriate prices. This method is able to encourage the verification nodes to proactively check and provide a trusted verification results, to furthest prevent collusion between nodes with malicious nodes.

The rest of this article is structured as follows. Section 2 details the design of the system model and consensus scheme. Section 3 describes reputation algorithm model and design process. Section 4 introduces the selection of generate block nodes. Section 5 assesses security based on the game model. Section 6 analyzes fairness, effectiveness and safety of consensus protocol, and discusses simulation and test result. Finally, we summarize the main work of this paper and point out future research directions.

II. SYSTEM MODEL AND CONSENSUS SCHEME

A. CROWDSOURCING SYSTEM

The crowdsourcing system consists of the initiator of the system task (the requester), the executor of the system task (the worker), and a crowdsourcing platform. In the initial state, the reputation value of all crowdsourcing nodes are set to 0.7. This value is obtained through simulate and calculate under different cases. We will explaine it in detail in section IV. After the system operating for some time, the worker has several interactions with the requester. Then, the requester i issues a task, the system stipulats that each bidders can participate in only one bidding activity in a period of time. Combined with the recommended opinions of other requesters for worker x, the comprehensive reputation value

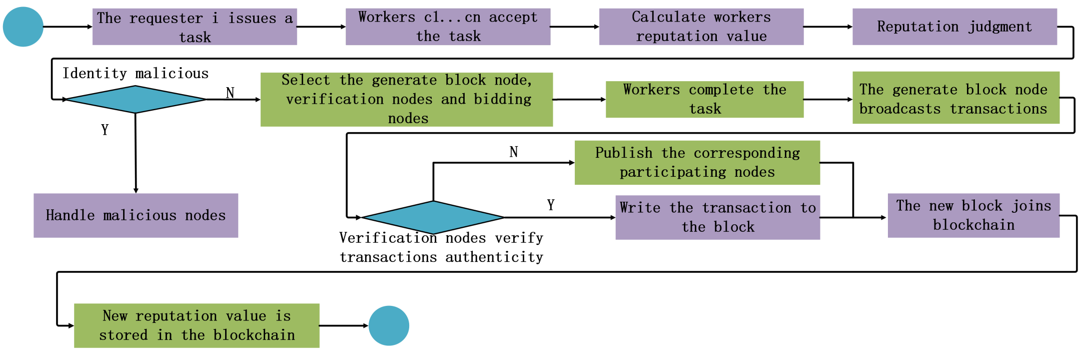

The requester i issues a task
Workers c1...cn accept the task
Calculate workers reputation value
Reputation judgment
Identity malicious
N
Y
Select the generate block node, verification nodes and bidding nodes
Workers complete the task
The generate block node broadcasts transactions
Handle malicious nodes
N
Publish the corresponding participating nodes
Y
Write the transaction to the block
The new block joins blockchain
Verification nodes verify transactions authenticity
New reputation value is stored in the blockchain

FIGURE 2. The crowdsourcing process of a bidding event.

of the requester i to the worker x is obtained. If requester i has interacted with worker x, the reputation value calculated by the local opinion algorithm is used as the local opinion of i to x at this time. When the comprehensive opinion is calculated, the system stores it in the new block and serves as the local opinion of the next round of i to x. After calculating the reputation value of all the crowdsourcers who want to participate in the bidding, the system selects the top K high reputation value nodes, including one generate block node, m bidding nodes and n verification nodes. The generate block node is selected using a random selection algorithm [18].

In each round of bidding, some nodes will receive corresponding rewards and the reputation value will increase.They are either the activists in the bidder selection process or the selected bidder itself. The nodes with malicious behaviors will be punished. The system model is shown in figure 2.

B. CONSENSUS SCHEME

The crowdsourcing system is deployed in the consortium blockchain. First, the requester initiates a crowdsourcing task, the workers who want to join the crowdsourcing have to go through a rigorous identity process. After becoming a miner candidate, the workers need to pay a deposit to their blockchain account. Second, system automatically calculates the worker reputation value by reputation algorithm, and then evaluates the credibility of workers. The worker use the reputation value to compete for miners. The higher the reputation value of the miner is, the more likely it become the generate block node. Due to using random selection algorithm, it is almost impossible to predict which one will be the generate block node. To some extent, it solves the problem that the bidding node and the generate block node collude to obtain the illegitimate interest. Third, the remaining miners with higher reputation value become the verification nodes. The incentive mechanism based on game theory encourages nodes to actively participate in verification,provide credible verification results and prevent collusion with other nodes. A miner who becomes a generate block node or a verification node will have the opportunity to get rewards, and the reputation value of the miner will be stored in the new block. Next, the new block will be uploaded to the blockchain system. The data stored in the blockchain has the characteristics of transparency, so each requester can share and download.

1) SYSTEM INITIALIZATION

All entities participating in the crowdsourcing system should be authenticated by the trust institution before they become legal entities. Each legal entity has its own public key, private key, encryption and decryption certificate [8]. A candidate who wants to join a miner should provide the information about his identity first. Participants are eligible to join the miner candidates only after they have been verified by the trust institution.

2) JOIN THE MINER CANDIDATES

After becoming a miner candidate, each miner provides a deposit to the account. If the miner candidate has malicious behaviors, the deposit will be deducted from the account. For example, the miner can not generate a block within the specified time, the deposit will be deducted by the blockchain system [9]–[11].

3) REPUTATION VALUE CALCULATION

The reputation of the miner candidates is based on the historical interactions of the miners themselves and the recommended opinions of other stakeholders. Section IV of this paper introduce the reputation calculation method based on the subjective logic model. Comprehensive opinions for each miner candidate are formed based on a number of different weights, and new reputation value can be downloaded from the blockchain.

4) MINERS SELECTION

After calculating the reputation value of the miner candidates, the miner is divided into four trusted states according to the reputation as follows: trustworthy, normal, abnormal and fault. It is helpful for the system to divide different node roles, and then identify normal nodes and malicious nodes. Because of the unpredictability of the time stamp and signature we used, the generation of the block node is random, and then malicious behaviors of nodes are reduced. The specific calculation process is in section V of this paper.The process of miner selection is shown in figure 3.

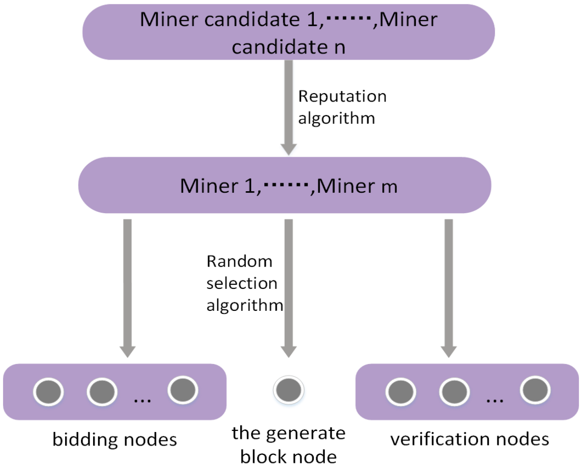


FIGURE 3. Miner selection process.

5) CONSENSUS PROCESS

An unverified block is generated by the generate block node, and the block is broadcast to the verification nodes, and the block is verified by the verification nodes. If the transaction is valid, it is written to the local transaction pool and forwarded to other consensus nodes, and if the transaction is invalid, it will be discarded directly.

In order to ensure mutual check, the verification nodes verify the local data blocks, then signs the verification results and broadcasts them in a distributed manner. Each verification node compares its verification results with the other miners', and sends the comparison results to the miners who generate the blocks. The feedbacks include the miner's results, the comparison results, the signature, and a record of the other miners' verification results. The generate block node analyzes the response information. If more than two-thirds of the miners agree to the block, the generate block node will send the record and the corresponding signature to all miners for storage [12], [13].

When the authenticated block is added to the blockchain, the miners that generate the block and participate in verifications will receive the transaction fee based on their contributions. New reputation values are stored in the blockchain. The consensus process is shown in figure 4. In a blockchain system, the more verification nodes, the more secure the consensus scheme [13]. Therefore, in order to obtain the correct verification results, there must be a reasonable incentive mechanism to encourage more nodes to participate in the verification. The specific analysis process is in section VI.

6) REPUTATION UPDATE

After the end of a round of consensus, the new reputation value of the worker j will be stored in the blockchain, which becomes the local reputation value of the requester i to the worker j for next time, and can be viewed and verified by other nodes. The reputation value update process is shown in figure 5.

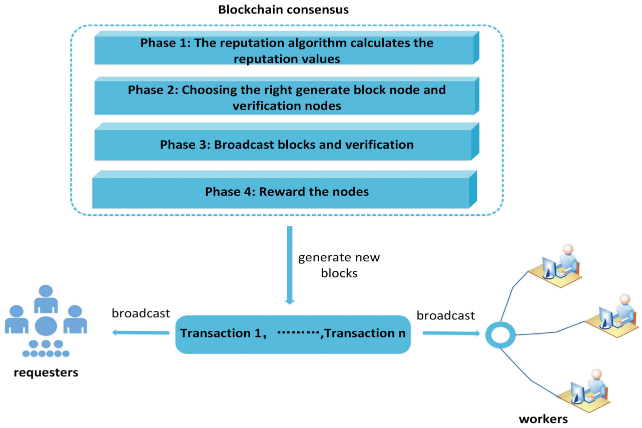

Blockchain consensus
Phase 1: The reputation algorithm calculates the reputation values
Phase 2: Choosing the right generate block node and verification nodes
Phase 3: Broadcast blocks and verification
Phase 4: Reward the nodes
generate new blocks
broadcast
Transaction 1, ………,Transaction n
broadcast
requesters
workers

FIGURE 4. System model.

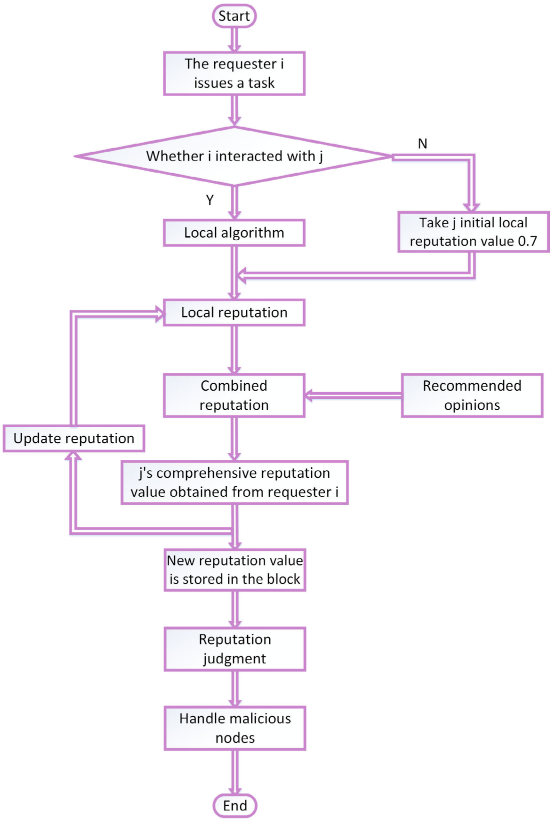

Start
The requester i issues a task
Whether i interacted with j
N
Y
Local algorithm
Take j initial local reputation value 0.7
Local reputation
Combined reputation
Recommended opinions
Update reputation
j's comprehensive reputation value obtained from requester i
New reputation value is stored in the block
Reputation judgment
Handle malicious nodes
End

FIGURE 5. Reputation update process.

III. REPUTATION ALGORITHM MODEL AND DESIGN PROCESS

Subjective logic is used to assess the credibility of a transaction. Subjective logic models are widely used in the security field. The categories evaluated are respectively denoted by b, d, u, and satisfy [19]:

$$b + d + u = 1, b, d, u \in [0, 1]$$

where b represents the degree of trust of the node, d represents the degree of distrust of the node, and u represents the uncertainty of the node.

The active interaction between the crowdsourcing participating members means that workers generate the correct block, the requester obtains the solution from the workers and then honestly distributes the bonus. This indicates that the requester trusts the services provided by workers. The higher the reputation value, the more credibility the data block generated by the miners. Since most of the requesters are trustworthy, the opinions of the low-credit requesters have only a small impact on the calculation of the reputation. In addition, the reputation algorithm of this paper combines the recommended opinions of other miners, it is an improvement of the traditional reputation algorithm, as shown in figure 6.

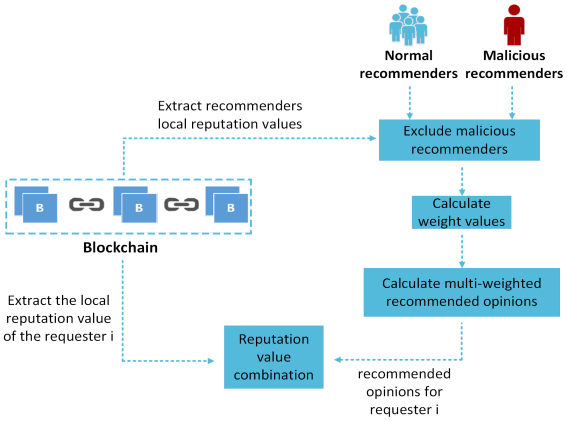

Normal recommenders
Malicious recommenders
Extract recommenders local reputation values
Exclude malicious recommenders
B
B
B
Blockchain
Calculate weight values
Calculate multi-weighted recommended opinions
Extract the local reputation value of the requester i
Reputation value combination
recommended opinions for requester i

FIGURE 6. **Reputation combination process.**

A. LOCAL OPINION

In the interaction between the requester and the worker, the opinion of the requester i to the worker j is called local opinion, its calculation process is as follows:

$$\omega_{i\to j} := \{b_{i\to j}, d_{i\to j}, u_{i\to j}\}$$

where $b_{i\to j}, d_{i\to j}, u_{i\to j}$ represent trust, distrust and uncertainty, respectively. And $b_{i\to j}, d_{i\to j}, u_{i\to j} \in [0, 1]$.

$$b_{i\to j} + d_{i\to j} + u_{i\to j} = 1$$

According to the subjective logic model [19]:

$$\begin{cases} b_{i\to j} = (1 - u_{i\to j})\dfrac{m_i}{m_i + n_i}, \\ d_{i\to j} = (1 - u_{i\to j})\dfrac{n_i}{m_i + n_i}, \\ u_{i\to j} = 1 - q_{i\to j}. \end{cases}$$

where m_i is the number of correct transactions, n_i is the number of erroneous transactions, q_i is the quality of the connection between the requester and the worker, which is related to the successful transfer rate of the packet. The trust value of the requester i to the worker j is represented by $B_{i\to j}$ [15], [19],

$$B_{i\to j} = b_{i\to j} + \varepsilon u_{i\to j}$$

where $0 \le \varepsilon \le 1$ represents the weight of uncertainty [14].

B. MULTI-WEIGHTED RECOMMENDATION

The subjective logic model is also related to other weights. This paper proposes the following related weights.

1) INTERACTION TIMELINESS

The trust of the requester to the worker changes over time. It is impossible to ensure that the worker is always reliable. The reliability of the worker is related to the interaction with the requester in the past, but the recent interaction with the worker should occupy a larger proportion. Judging the recent and past time points t_1 can be set, for example, two days. φ represents the weight of the recent interactions, ψ represents the weight of the past interactions, and [15]

$$\varphi + \psi = 1, \quad \varphi > \psi.$$

2) EFFECT OF SELFISH TRANSACTIONS

Proper trading behaviors will increase the reputation of the worker, and selfish trading behaviors will reduce the reputation of the worker. Therefore, in order to ensure proper trading behaviors better, the weight of selfish behaviors should be set even larger. μ denotes the weight of the honest trading behaviors, ν denotes the weight of the selfish trading behaviors, and [15]

$$\mu + \nu = 1, \quad \mu < \nu$$

Combined with the timeliness of interaction and the impact of selfish transactions, a new frequency of interaction is formed [15]:

$$\begin{cases} m_i = \varphi\mu m_1^i + \psi\mu m_2^i, \\ n_i = \varphi\nu n_1^i + \psi\nu n_2^i. \end{cases}$$

when the current time belongs to the recent time, i.e. $t > t_1$, the number of honest transactions and selfish transactions respectively are m_1^i and n_1^i. When the current time does not belong to the recent time, i.e. $t \le t_1$, the number of honest transactions and selfish transactions respectively are m_2^i and n_2^i.

3) INTERACTION FREQUENCY

The interaction frequency represents how much prior awareness of the requester to the worker. The higher the interaction frequency, the more the requester has prior knowledge about the worker. So the requester's viewpoint is more credible. The calculation of the interaction frequency is as follows [15]:

$$F_{i\to j} = \frac{Num_{i\to j}}{\overline{N_i}}$$

$Num_{i\to j}$ represents the number of interactions between the requester i and the worker j in time T, which is [15]:

$$Num_{i\to j} = m_i + n_i$$

$$\overline{N_i} = \frac{1}{|E|}\sum_{e\in E} Num_{i\to e}$$

E represents the set of all workers that interacted with the requester i during time T.

$$F_{i\to j} = \frac{Num_{i\to j}}{\overline{N_i}} = \frac{\mu(\varphi m_1^i + \psi m_2^i) + \nu(\varphi n_1^i + \psi n_2^i)}{\frac{1}{|E|}\sum_{e\in E} Num_{i\to e}}$$

In summary, the weight of local reputation is [15]:

$$\tau_{i\to j} = l_i F_{i\to j}$$

$0 \le l_i \le 1$ is the weight of interaction frequency which is predefined.

C. RECOMMENDED OPINIONS

The recommended opinions come from the opinions of other requesters who have interacted with the worker j. The opinions of different recommenders are weighted by different weights, and this form a comment value, which is [15]:

$$\begin{cases} b^{rc}_{x\to j} = \dfrac{1}{\sum_{x\in X}\tau_{x\to j}} \displaystyle\sum_{x\in X} \tau_{x\to j} b_{x\to j}, \\ d^{rc}_{x\to j} = \dfrac{1}{\sum_{x\in X}\tau_{x\to j}} \displaystyle\sum_{x\in X} \tau_{x\to j} d_{x\to j}, \\ u^{rc}_{x\to j} = \dfrac{1}{\sum_{x\in X}\tau_{x\to j}} \displaystyle\sum_{x\in X} \tau_{x\to j} u_{x\to j}. \end{cases}$$

Among them, $x \in X$ represents other requester that interacts with worker j.

D. COMBINE LOCAL OPINIONS WITH RECOMMENDED OPINIONS

The ultimate credibility of the requester i to the worker j is calculated by combining local opinions with recommended opinions [15], [19]:

$$\begin{cases} b^{f}_{x\to j} = \dfrac{b_{i\to j}u^{rc}_{x\to j} + b^{rc}_{x\to j}u_{i\to j}}{u_{i\to j} + u^{rc}_{x\to j} - u^{rc}_{x\to j}u_{i\to j}}, \\ d^{f}_{x\to j} = \dfrac{d_{i\to j}u^{rc}_{x\to j} + d^{rc}_{x\to j}u_{i\to j}}{u_{i\to j} + u^{rc}_{x\to j} - u^{rc}_{x\to j}u_{i\to j}}, \\ u^{f}_{x\to j} = \dfrac{u^{rc}_{x\to j}u_{i\to j}}{u_{i\to j} + u^{rc}_{x\to j} - u^{rc}_{x\to j}u_{i\to j}}, \\ u_{i\to j} + u^{rc}_{x\to j} - u^{rc}_{x\to j}u_{i\to j} \neq 0, \end{cases}$$

The final reputation value of the requester i to the worker j is expressed as $B_{i\to j}$ [19]:

$$B^f_{i\to j} = b^f_{i\to j} + \varepsilon u^f_{i\to j}$$

IV. THE SELECTION OF THE GENERATE BLOCK NODES

After calculating the reputation value of the requester i to the worker j, the generate block node should be selected according to the reputation value of each worker. The higher the reputation value, the higher probability of the worker be selected as the generate block node. In order to reduce the predictability of the generate block node, we propose the following algorithm to improve the randomness of the selection of the generate block node, while ensuring that the selected node has higher credibility.

TABLE 1. Reputation value reference.

$Value$ $Ratio$ NoI	$1:0$	$2:1$
10	0.835	0.729
30	0.898	0.792
50	0.910	0.805
70	0.916	0.810

A. TRUSTWORTHY STATE OF THE REPUTATION MODEL

The calculation result $B^f_{i\to j}$ is divided into four cases, and the following $B^f_{i\to j}$ is abbreviated as B:

- *trustworthy:* $B \in [0.85, 1]$, at this time, the trusted state st is set to 1.
- *normal:* $B \in [0.7, 0.85]$, at this time, the trusted state st is set to 2.
- *abnormal:* $B \in [0.5, 0.7]$, at this time, the trusted state st is set to 3.
- *fault:* $B < 0.5$, at this time, the trusted state st is set to 4.

The conversion relationship between node states is shown in figure 7, where 0.85 and 0.7 respectively are two critical values of the trust state, as shown in the table 1, and NoI indicates the number of interactions.

In order to ensure the security of the system, the system requires that the reputation values of the nodes cannot be lower than a certain threshold. Therefore, we calculated the following sets of data as a reference, the node is set to have only once malicious behavior. For example, in 10 times interactions, the node reputation value is 0.729 in the case the ratio of positive to negative recommended opinions is 2:1, and the node reputation value is 0.835 in the case the ratio of positive to negative recommended opinions is 1:0. From the calculation results and the actual situation we can see when the reputation value exceeds 0.85, this node is eligible for generating blocks. When the reputation value exceeds 0.7, this node can qualify for joining the system.

The four trust states of a node can be converted to each other. When a normal node continues to generate a valid block, or keep other good behaviors, its reputation value will exceed 0.85, and the reputation state will be converted to a trustworthy state. A trustworthy node has a greater chance to be selected as the generate block node. If a trustworthy/normal node exhibits anomalous behaviors, for example, it do not generate a new block for a period of time or its verification results are different from most nodes, its reputation value will decrease and it will be convert to an abnormal node. When the reputation value drops below 0.5, the reputation status will be converted to a fault state, and this node needs to be repaired or removed. A new consensus node will be defaulted to a normal node when it joins the system.

B. RANDOMLY SELECT THE GENERATE BLOCK NODE

For the requester i, assuming its reputation status is st_i, then the probability that it is selected to be the generate block

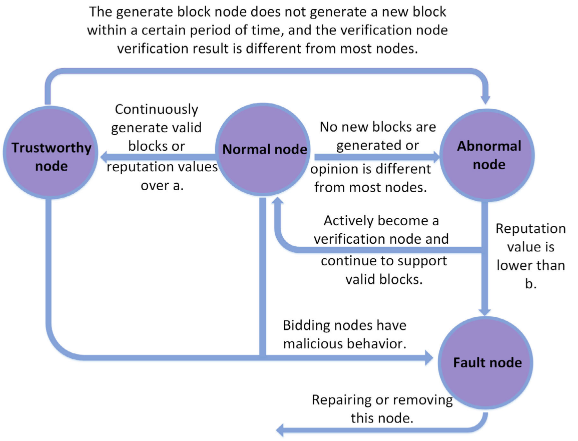

The generate block node does not generate a new block within a certain period of time, and the verification node verification result is different from most nodes.
Trustworthy node
Continuously generate valid blocks or reputation values over a.
Normal node
No new blocks are generated or opinion is different from most nodes.
Abnormal node
Actively become a verification node and continue to support valid blocks.
Reputation value is lower than b.
Bidding nodes have malicious behavior.
Fault node
Repairing or removing this node.

FIGURE 7. Conversion relationship of node trusted state.

node is [20]:

$$P(p = i) = \frac{l}{st_i}$$

So for any two workers a and b, if $st_a < st_b$, $\frac{l}{st_a} > \frac{l}{st_b}$, which is $P(p = a) > P(p = b)$. Assuming that $NSum_i$ represents the number of worker with $st = i$, then l can be calculated as follows [20]:

$$l = \frac{1}{\sum_{i=1}^{4} \frac{NSum_i}{i}}$$

In order to ensure unpredictability of the generate block node, a random number R needs to be calculated by the following formula:

$$R' = TimeStamp \oplus Signature$$
$$R = StrToInt(SubStringEnd32(Hash_{t+1}(R')))modN$$

We XOR timestamp with signature of current block header to get R', and then perform $t + 1$ times hash operations on R'. If no new blocks were generated in the previous round, the node needs to count the times t that the system does not produce blocks in continuous consensus rounds. Further, the first 32 bits of $Hash_{t+1}(R')$ is converted to an integer value. We can get R by taking the modulo-N residue of this result. N is the number of consensus nodes.

Since the time stamp and signature of the block header are unpredictable, R is unpredictable. According to the probability that node is selected to the generate block node, the node is finally selected as the generate block node only when satisfy the following formula, and we assume node i is the generate block node [20]:

$$\sum_{j=1}^{i-1} P(p = j) \leq \frac{R}{N} < \sum_{j=1}^{i-1} P(p = j) + P(p = i)$$

This inequality can ensure that the selected generate block node is unique.

V. SECURITY ASSESSMENT BASED ON GAME MODEL

In Section III and Section IV, the reputation algorithm based on the subjective logic model is introduced. Nodes with higher reputation values are more likely to be selected as nodes for generating blocks and verifying. However, there are still potential risk of verification node's collusion in crowdsourcing scenarios. In this section, we will design an incentive mechanism based on game theory, which makes the collusion cost of verification nodes is higher than the profit, and encourages the node to actively participate in block verification. We ensure the safety of incentive mechanism in the face of malicious behaviors by setting appropriate prices [16], [17].

A. DESCRIPTION OF THE GAME MODEL

- *player:* This game model has $n + 1$ players, $V = (v', v_1, v_2, \ldots, v_n)$ stands for verification node cluster, v' is the verification node that may initiate collusion, $G = (v_1, v_2, \ldots, v_n)$ is the collusion node cluster of v'.
- *strategy:* Player v has two strategies: honest H and malicious M. Honest players will follow the agreement, and malicious players will behave maliciously, such as colluding with other nodes. We use S to represent the player v's strategy.
- *benefit:* The player's benefit refers to the difference between the player's profit and the cost. Without collusion attacks, the player's benefit u is calculated as:

$$u = \begin{cases} \frac{\zeta}{2^{n-1}} - \theta_i, & i \in G \; and \; S = M, \\ \xi - \theta_v, & i = v \; and \; S = H, \end{cases}$$

where θ_i is the cost of verification of V, such as the communication cost, providing verification information, etc. θ_v is the cost of the node v, for example, the transmission signature confirmation, etc. ζ is remuneration that should be paid to the collusion node when there has collusion between verification nodes, ξ is remuneration that should be paid to the verification nodes in the absence of collusion.

For a player, the best response strategy is to maximize the expected benefit to its own, regardless of the strategy of the other players. We should set up a mechanism to ensure that honesty is the best strategy for each node. That is, if the collusion cannot increase the benefit, the incentive mechanism is effective.

B. SECURITY ASSESSMENT UNDER COLLUSION ATTACKS

When $\zeta < \xi/k^2$ is satisfied, our incentive mechanism can be effectively implemented, where k is the probability that two arbitrary nodes encounter each other.

1) Considering the case with one conspired node
Suppose $C = \{V_1, v\}$ is a collusion group and $E(u_C)$ is the expected benefit of the collusion group. Our goal is to confirm

$$E(u_c) \leq u_v$$

The verification node v that initiates the collusion and the verification node V_1 participates in the collusion will eventually obtain the proceeds from the requester A. When A has encountered both v and V_1 at the same time (with a probability of k^2), the expected sum of the payment of C is:

$$P_c = q^2(\zeta + \xi) + (1 - q^2)\xi = q^2\zeta + \xi$$

Considering the cost of communicating with V_1 and the cost of providing verification information:

$$u_c = q^2\zeta + \xi - \xi - \theta_v = q^2\zeta - \theta_v$$

because of $\zeta < \xi/k^2$,

$$u_c = q^2\zeta - \theta_v < \xi - \theta_v = u_v$$

2) Considering the case with n conspired nodes
Suppose $C = \{V_1, V_2, \ldots, V_n, v\}$ is a collusion group and $E(u_C)$ is the expected benefit of the collusion group. Our goal is to confirm

$$E(u_c) \leq u_v$$

When $(A, V_1), (V_1, V_2), \ldots, (V_n, v)$ encounter each other, the expected payment amount of collusion group C is:

$$P_c = q^{n+1}(\frac{n\zeta}{2^{n-1}} + \xi) + (1 - q^{n+1})\xi = q^{n+1}\frac{n\zeta}{2^{n-1}} + \xi$$

Considering the cost of the collusion group:

$$\begin{aligned} u_c &= q^{n+1}\frac{n\zeta}{2^{n-1}} + \xi - n\xi - \theta_v \\ &< \frac{q^{n+1}n\xi}{2^{n+1}q^2} - n\xi + \xi - \theta_v \\ &= (\frac{q^{n-1}}{2^{n-1}} - 1)n\xi + \xi - \theta_v \\ &< \xi - \theta_v \\ &= u_v \end{aligned}$$

Therefore, if $\zeta < \xi/k^2$ is satisfied, our incentive mechanism can resist the collusion attack of the verification nodes and improve the security of the system.

VI. PERFORMANCE

A. FAIRNESS

The Improved PoT consensus is based on the reputation algorithm, which has an important characteristic of fairness.

Different from the DPoS consensus protocol, consensus results are not depend on a few fixed nodes. The generate block node plays an important role in the consensus process, its choice directly affects own reputation value. And the system can not only ensure the unpredictability of the node selection, but also ensure that the generate block node is selected from those with higher reputation values. And the verification results are decided by all verification nodes. The transaction is confirmed only when more than two-thirds of verification nodes agree on it. The consensus process of the improved PoT can guarantee neutrality. The discourse power of node depends on its reputation value. And the choice of the generate block node is random. Before the generate block node is selected, no node can predict which node will be responsible for generating block.

B. EFFECTIVENESS

In the reputation calculation phase, the reputation value is related to the local opinion and the recommended opinions of the node. The reputation algorithm can exclude the malicious nodes and pick out the generate block node and the verification nodes. In the verification phase, the generate block node publishes the transaction information to the verification nodes to check. And each verification node examines the the authenticity of transactions separately and does not disclose the verification result to other verification nodes. After the verification phase, the generate block node accept the majority verification result.

Even if there is collusion between most of the verification nodes, the cost of the collusion verification group will be higher than the gain of the acquisition under the constraint of $\zeta < \xi/k^2$. This is not the choice of rational nodes in game theory, so honestly verifying behavior is the best strategy for nodes. The correct transaction will eventually be written to the block.

C. SAFETY

Through the analysis of blockchain and crowdsourcing scenarios, this paper evaluates two typical security issues in the system. One is the generate block node and verification nodes collusion. The generate block node selects favourable verification node to participate in the verification, and then intervenes the consensus result. The other is the collusion between the verification nodes. In the improved PoT consensus, the selection of the verification node is related to its reputation value. The reputation value will be stored in the block and cannot be modified, any node can query it. Even if a malicious node becomes a verification node, its verification result will be invalid if the result is different from other nodes. The verification result requires more than two-thirds of the verification nodes to agree. Otherwise the malicious node will be penalized by reducing the reputation value and deducting the deposit. The incentive mechanism based on game theory guarantees that the cost of colluding between verification nodes will be much higher than the benefits it will receive.

D. SIMULATION RESULTS

1) THE EFFECT OF NODE BEHAVIORS ON NODE REPUTATION VALUES

Figure 8 and figure 9 respectively show the change of the reputation values of the normal node and the malicious node with the number of interactions.

It can be seen from the figure that the reputation values of normal nodes keep rising with the increase of the number of interactions, whether we adopt the subjective logical

TABLE 2. Parameters setting of simulation experiment.

Parameter	Value
interaction timeliness parameter φ and ψ	0.9, 0.1
effect of selfish transactions parameter μ and ν	0.1, 0.9
weight of interaction frequency l_i	0.9
weight of uncertainty in subjective logical reputation ε	0.01
total number of nodes	21
number of generate block node	1
number of verification nodes	15
number of bidding nodes	5
number of simulation experiments	500
reputation threshold	0.7

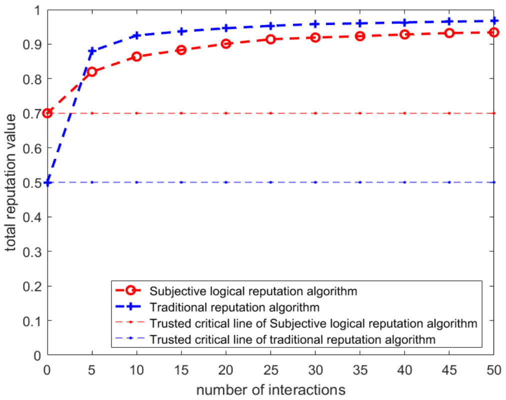


FIGURE 8. The reputation values of a normal miner.

reputation algorithm or the traditional reputation algorithm. However, the initial reputation values of nodes are different, which specified by the subjective logical reputation algorithm and the traditional reputation algorithm. The former is 0.7, the latter is 0.5. So we can see from the figure 8, in the first five interactions, the reputation values of the subjective logical reputation algorithm are higher than the traditional reputation algorithm. But in the subsequent interactions, the reputation values of the traditional reputation algorithm are higher than the subjective logical reputation algorithm. This is because the traditional reputation algorithm does not consider the impact of the recommended opinions on the node, which lead to high node's reputation values.

Figure 9 compares the reputation values of a malicious miner under three consensus algorithm, they are respectively the subjective logical reputation consensus algorithm, the traditional reputation consensus algorithm and the traditional DPoS consensus algorithm. As can be seen from the figure, when the node has malicious behaviors after five normal interactions, the reputation value of both the subjective logic reputation algorithm and the traditional reputation algorithm decline immediately, but the former dropped faster. Since there is no reputation algorithm in DPoS, its reputation value continues to rise, and infinitely close to 1. After one or two interactions, it quickly drops below the trusted critical line of 0.7. The traditional reputation algorithm does not take into account the recommended opinions, that is, does not consider the effect of interaction timeliness and selfish transactions, so the reputation values of nodes cannot be quickly dropped below the trusted critical line. The experimental parameter settings are shown in table 1.

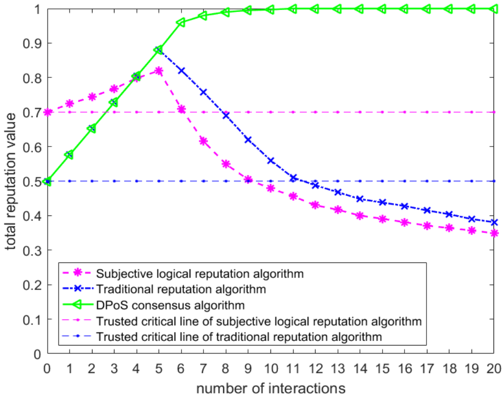


FIGURE 9. The reputation values of a malicious miner.

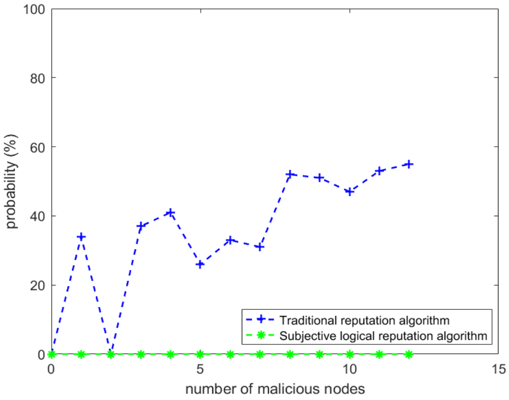


FIGURE 10. The probability that a malicious node is elected to the generate block node.

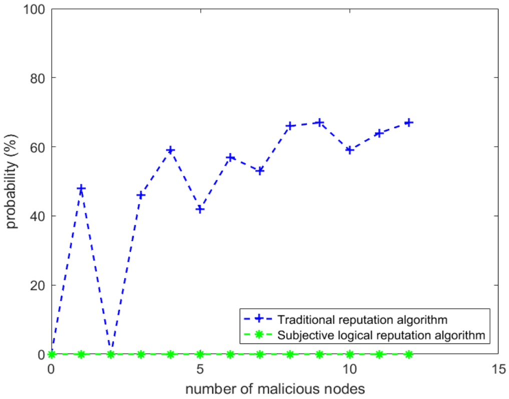
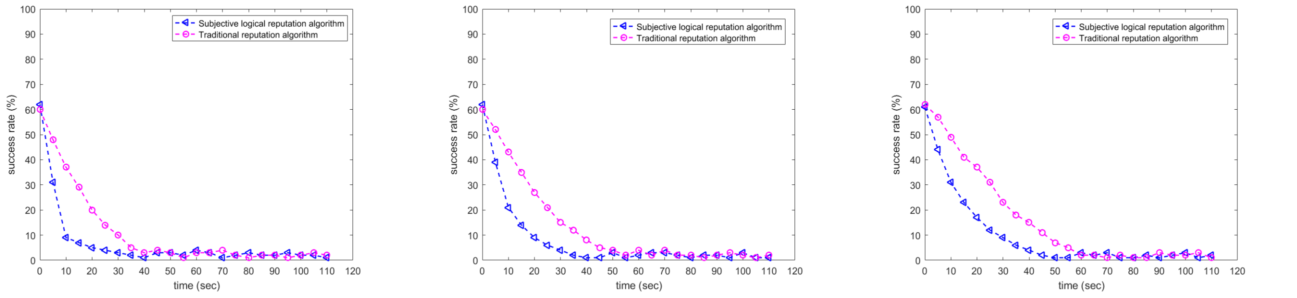


FIGURE 11. The probability that a malicious node is elected to a verification node.

2) THE PROBABILITY THAT A MALICIOUS NODE IS SELECTED AS THE PRIMARY NODES

Figure 10 and figuer 11 respectively show the probability that a malicious node is selected as the generate block node or a verification node with the number of malicious nodes



(a) $\varepsilon = 0.05$ (b) $\varepsilon = 0.055$ (c) $\varepsilon = 0.06$

FIGURE 12. The success rate of hidden malicious nodes implementing malicious behaviors under the influence of ε.

increase. It can be inferred from figure 10 that the subjective logic consensus algorithm will not select a malicious node to be the generate block node. However, under the traditional reputation algorithm, a malicious node becomes the generate block node with high probability, and the probability is increasing as the number of malicious nodes grows. Therefore, the reputation consensus algorithm is more sensitive to malicious nodes and can distinguish malicious nodes in time. The reputation value of the generate block node must reach 0.85 or higher in this paper. If nodes' reputation values can reach 0.85 or higher, their local opinions and recommended opinions are also very high, that is, they have almost no malicious behaviors in the past interactions. So this type of node is the most trustworthy and most unlikely to do malicious behaviors. In the traditional reputation algorithm, because the recommended opinions are not be considered, the reputation value of the node is usually high, even higher than 0.85, this will make such nodes easy to be generate block node. But such nodes may still have malicious behaviors in the past, this will bring a big risk to the system, and this trend is increasing with the number of malicious nodes grows.

The situation in figure 11 is similar to figure 10, but with one difference: a malicious node is selected as verification node with higher probability, when using the traditional reputation algorithm. This is because a verification node's reputation value only need to be greater than 0.7. This is to improve fairness of the system. The numerous calculations show that if the node's reputation value can reach 0.7 or above, they are basically in a normal interaction state, although they have once or twice malicious behaviors. This kind of node have the opportunity to become a trustworthy node. Therefore, such nodes cannot be completely excluded. Furthermore, the incentive mechanism makes the node hard to engage in malicious behaviors, otherwise there will be penalties such as lowering the reputation value and deducting the deposit.

3) THE SUCCESS RATE OF HIDDEN MALICIOUS NODES IMPLEMENTING MALICIOUS BEHAVIORS UNDER THE INFLUENCE OF ε

In the reputation algorithm, ε represents the impact of the uncertainty of the node, especially hidden malicious nodes. This parameter determines the reputation of the unknown node. So this paper sets different ε to evaluate its impact on the success rate of malicious behaviors. When a node's reputation value greater than 0.7 and this node successfully participates in the block generation process, it will still implement malicious behaviors with a certain possibility. We test the success rate of such hidden malicious nodes entering the system, as shown in figure 12.

When $\varepsilon = 0.05$, the reputation algorithm based on subjective logic reduces the success rate of malicious nodes to near zero in about 35s. Based on the traditional reputation algorithm, the success rate of malicious nodes perform malicious behaviors is reduced to about zero in near 40s. When $\varepsilon = 0.055$, the length of time that the success rate falls to near zero is about 40s and 55s respectively. When $\varepsilon = 0.06$, the required time are respectively 45s and 60s. It takes a while for the success rate reaching near zero under both algorithms. But the traditional reputation algorithms need a longer time.

VII. CONCLUSION AND FUTURE RESEARCH

Due to features of decentralization, traceability, tamper-proof, etc., the blockchain technology offers a feasible method to restricting malicious behaviors in crowdsourcing systems. However, most existing blockchain consensus protocols are not suitable for large-scale online services. In this paper, we combine the crowdsourcing scenario with the blockchain, and propose a improved PoT consensus protocol based on subjective logical reputation algorithm to provide the distributed governance and accountability. The trust component meets the practical requirements of crowdsourcing scenarios. Together with the incentive measures based on game theory, our consensus protocol can make the verification process more credible. Through the simulation experiment, we compare the proposed scheme to other existing schemes. The results show that the improved PoT consensus outperforms in validity, fairness and security.

In future research, we will further combine cryptography to enhance the privacy and reliability of the system.

REFERENCES

[1] W. Wang, D. Thai Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. In Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," 2018, *arXiv:1805.02707*. [Online]. Available: http://arxiv.org/abs/1805.02707

[2] EOS Block Producer Voting Guide. *New Directions in Communications*. Accessed: Apr. 5, 2019. [Online]. Available: https://medium.com/coinmonks/eos-block-producer-voting-guide-fba3a5a6efe0

[3] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A Proof-of-Trust consensus protocol for enhancing accountability in crowdsourcing services," *IEEE Trans. Services Comput.*, vol. 12, no. 3, pp. 429–445, May 2019.

[4] P. Resnick, K. Kuwabara, and R. Zeckhauser, "Reputation systems," *Commun. ACM*, vol. 43, no. 12, 45–58, 2000.

[5] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," *IEEE Trans. Syst., Man, Cybern., C (Appl. Rev.)*, vol. 41, no. 3, pp. 407–420, May 2011.

[6] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *Proc. Int. Conf. Netw. Syst. Secur.* Berlin, Germany: Springer, 2013, pp. 94–108.

[7] Q. He, D. Wu, and P. Khosla, "SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2004, pp. 825–830.

[8] J. Kang, R. Yu, X. Huang, and S. Maharjan, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[9] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "Secure multiparty computations on bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, p. 443.

[10] M. Andrychowicz, S. Dziembowski, D. Malinowski, and. Mazurek, "Fair two-party computations via bitcoin deposits," in *Financial Cryptography and Data Security* Berlin, Germany: Springer, 2014, pp. 105–121.

[11] I. Bentov and R. Kumaresan, "How to use bitcoin to design fair protocols," in *Advances in Cryptology*. Berlin, Germany: Springer, 2014, pp. 421–439.

[12] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled Internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, Mar. 2019.

[13] J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye, and D. I. Kim, "Incentivizing consensus propagation in Proof-of-Stake based consortium blockchain networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 157–160, Feb. 2019.

[14] N. Oren, T. J. Norman, and A. Preece, "Subjective logic and arguing with evidence," *Artif. Intell.*, vol. 171, nos. 10–15, pp. 838–854, 2007.

[15] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. In Kim, and J. Zhao, "Towards secure blockchain-enabled Internet of vehicles: Optimizing consensus management using reputation and contract theory," 2018, *arXiv:1809.08387*. [Online]. Available: http://arxiv.org/abs/1809.08387

[16] M. Felegyhazi, J.-P. Hubaux, and L. Buttyan, "Nash equilibria of packet forwarding strategies in wireless ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 5, no. 5, pp. 463–476, May 2006.

[17] H. Zhang, B. Liu, H. Susanto, G. Xue, and T. Sun, "Incentive mechanism for proximity-based mobile crowd service systems," in *Proc. IEEE 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Apr. 2016, pp. 1–9.

[18] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A blockchain based truthful incentive mechanism for distributed P2P applications," *IEEE Access*, vol. 6, pp. 27324–27335, 2018.

[19] A. Jsang, R. Hayward, and S. Pope, "Trust network analysis with subjective logic," in *Proc. 29th Australas. Comput. Sci. Conf.*, 2006, pp. 85–94.

[20] K. Lei, Q. Zhang, L. Xu, and Z. Qi, "Reputation-based byzantine fault-tolerance for consortium blockchain," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2018, pp. 604–611.

XIAOYU ZHU is currently pursuing the M.S. degree with the Beijing Laboratory of Advanced Information Networks, Beijing University of Posts and Telecommunications. Her current research interests include blockchain and security issues.

YI LI received the Ph.D. degree in communication engineering from the Beijing University of Posts and Telecommunications. He is currently an Associate Professor with the Key Laboratory of Universal Wireless Communication, Ministry of Education, Beijing University of Posts and Telecommunications. His research interests include blockchain technology, the Internet of Things, big data, and machine learning.

LI FANG received the M.S. degree in information engineering from the Beijing University of Posts and Telecommunications. Her research interests include blockchain technology, wireless networks, and signal processing.

PING CHEN received the M.S. degree in electronic engineering from the Beijing University of Posts and Telecommunications. She is currently a Senior Engineer with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications. Her research interests include signal processing and blockchain technology.