



Article

# Blockchain-Based Resource Allocation Model in Fog Computing

Haoyu Wang<sup>1</sup>, Lina Wang<sup>1,\*</sup>, Zhichao Zhou<sup>2,\*</sup>, Xueqiang Tao<sup>3</sup>, Giovanni Pau<sup>4</sup>  and Fabio Arena<sup>4</sup> 

<sup>1</sup> School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China; haoyu1989@126.com

<sup>2</sup> Asiainfo Technology Co., Ltd.; Asiainfo Technology Co., Ltd. Northwest Wang Dong Road, Haidian District, Building #19, Beijing 100193, China

<sup>3</sup> Institute of Medical Support Technology, Academy of Systems Engineering, Tianjin 300050, China; taoxue2437@126.com

<sup>4</sup> Faculty of Engineering and Architecture, Kore University of Enna, 94100 Enna, Italy; giovanni.pau@unikore.it (G.P.); fabio.arena@unikore.it (F.A.)

\* Correspondence: wanglina@ustb.edu.cn (L.W.); zhouzc@asiainfo.com (Z.Z.); Tel.: +86-137-175-43518 (L.W.); +86-185-133-01337 (Z.Z.)

Received: 19 November 2019; Accepted: 11 December 2019; Published: 16 December 2019



**Abstract:** Fog computing makes up for the shortcomings of cloud computing. It brings many advantages, but various peculiarities must be perceived, such as security, resource management, storage, and other features at the same time. This paper investigates the resource contribution model between the fog node and cloud or users when fog computing introduces blockchain. The proposed model practices the reward and punishment mechanism of the blockchain to boost the fog nodes to contribute resources actively. The behavior of the fog node in contributing resources and the completion degree of the task also for contributing resources are packaged into blocks and stored in the blockchain system to form a transparent, open, and tamper-free service evaluation index. The differential game method is employed to model and solve the above process and address the interaction between the optimal resource contribution strategy of the fog node and the optimal benefit under the optimal resource contribution strategy. Indirectly, this service evaluation index also brings long-term economic benefits to fog service providers. Besides, taking advantage of the performance characteristics of the collective maintenance of blockchain and the ability to establish a credible consensus mechanism in an untrusted environment, fog computing nodes, under the proposed architecture, can have specific security protection capabilities.

**Keywords:** fog computing; blockchain; resource contribution; differential game

## 1. Introduction

### 1.1. Background

In recent years, with the continuous development of intelligent terminals and wireless network technology, we have entered the new era of the Internet of Everything from the interconnection of people and things, and the interconnection of things and things [1]. More and more data is generated and distributed in this huge and complex network environment, bringing unprecedented pressure on computing services. The traditional cloud computing model cannot meet not only the heterogeneous, low delayed, and dense access networks but also the use of various applications for intelligent terminal users. In order to solve this problem, Cisco's Bonomi et al. proposed a new computing paradigm in 2011 (i.e., fog computing) [2]. This model deals with the addition of a fog

layer between the terminal device and the traditional cloud server to afford computing, storage, and network services. The main aim is to relocate some core functions of the cloud to the “near” location of the network edge, to overcome the defects of cloud computing regarding location awareness, mobility support, and real-time interaction [3,4]. As an enlargement of cloud computing, fog computing is alike to cloud computing, since it is also a network-based computing model that provides data sharing, computing, storage, and other services through fog nodes on the Internet. Fog computing is a processing environment with widely distributed deployment, confronted with relatively concentrated cloud computing. Data storage and processing are more dependent on edge devices, so users of fog computing usually pay a certain fee to get more effective services. The device that provides the computing service can get a particular reward by providing its redundant computing resources [5].

Nevertheless, fog computing, as an emerging computing model, has brought new problems and challenges to the computing service field due to its “fog node as a resource provider” [6]. Considering that the fog computing environment has the features of restricted resources, wide distribution, heterogeneous network, and selfish fog computing nodes, the proper management of these characteristics in fog nodes has become one of the main aims focus in the fog computing research field [7]. On the one hand, the income and cost of the fog node when contributing resources are often not excellently balanced; on the other hand, the cloud service provider lacks an effective incentive mechanism to promote the continuous and stable contribution of the fog node. Given the above problems, many scholars have carried out research and discussion [8–11], and some progress has been made. However, there are still many problems that restrict the extensive application of fog computing. As a consequence, it is necessary to seek emerging technologies and methods to solve the above difficulties.

Acknowledging the success and increasing popularity of digital cryptocurrencies such as bitcoin [12], blockchain technology is gradually emerging. Its core advantage can use data encryption, timestamp, distributed consensus, and economic incentives in the node without mutual trust in the implementation of a distributed system based on a point-to-point decentralized credit trading, coordination, and cooperation. These characteristics can solve issues related to the centralized organization, the prevalence of high cost, low efficiency, and data storage [13]. The blockchain system generally consists of a data layer, a network layer, a consensus layer, an incentive layer, a contract layer, and an application layer [14]. The data layer is used to construct data blocks, encrypt and sign data, and add timestamps. The network layer includes distributed peer-to-peer networks for communication and data verification between nodes. The consensus layer implements various consensus algorithms such as Proof of Work (PoW) [15] and Proof of Stake (PoS) [16] or Delegated Proof of Stake (DPoS) [17]. The incentive layer is mainly used to develop the corresponding incentive mechanism, and its issued token has unforgeable characteristics compared with the traditional monetary reward. The contract layer mainly uses scripts or algorithms to formulate smart contracts that all network nodes must be compliant. Finally, the application layer is based on various application scenarios of blockchain technology.

Due to the characteristics of blockchain, scholars have carried out relevant studies on the combination of blockchain technology with cloud computing, fog computing, and edge computing, including research on the combination of blockchain technology with the Internet of Things (IoT), access control technology, and other related fields. This paper focuses on the resource contribution allocation in the fog computing environment. The critical point is related to the research of proper resource management with a combination of blockchain technology and fog computing.

## 1.2. Related Works

As mentioned above, resource contribution is a critical technical issue in resource management and allocation, especially in fog computing. Resource contribution refers to the provision of computing, storage, and other resources by devices with idle resources. Although the resources and computing power of idle resource devices have different degrees of restrictions [18], they can jointly cooperatively

complete computing and storage tasks, thereby lightening the resource bottleneck problem of the primary service provider. In recent years, the issue of resource contribution has been the focus and hotspot of distributed computing in cloud computing, fog computing, and edge computing. Zhang et al. [19] proposed a game framework for resource management three-layered structure in data service operator (DSO), fog node (FN), and data service subscriber (ADSS) scenarios. Their solution is based on the Stackelberg game. The moral hazard model and the matching game strategy give the stability strategy of the fog computing system under the framework.

Zhao et al. [20] proposed a resource sharing mechanism based on the alliance game by studying the resource contribution between cooperative cloud providers. The authors consider the uncertainty of mobile users fully. The purpose is to optimize the resource utilization rate and to reduce the cost of the cloud service provider. The authors aim to form the cloud service provider alliance by using the alliance game to ensure the stability of the mechanism structure and to analyze the resource usage cost of the cloud service provider participating in the alliance game by employing the Shapley value theory Distribution situation. Nishio et al. [21] proposed a service-oriented heterogeneous resource sharing scheme, which effectively reduces the service waiting time. Dong et al. [22] studied the optimization of energy and communication resource sharing between mobile devices with limited energy and restricted data in mobile cloud computing. Ye et al. [23] offload the computational tasks in the cloud to the fog server by bypassing the private cloud allocation strategy and use a genetic algorithm to find the optimal allocation scheme. Su et al. [24] proved that the shortest path scheme based on Steiner tree theory is more efficient than the traditional scheme to minimize the path cost of the fog server contributing resources.

Alsaffar et al. [25] proposed a linear tree decision rule algorithm based on service size, completion time, and virtual machine capacity, which helps workload balancing and improves resource allocation. Shi et al. [26] used the Representational State Transfer (REST) design pattern and the IoT Constrained Application Protocol (CoAP) to enable resource cooperation in the form of a planar architecture between fog nodes. Neto et al. [27] optimized the load balancing in a fog environment using the multi-tenant allocation algorithm (MtLDF), which takes into account the latency and priority of specific multi-tenant needs. Kochar and Sarkar [28] constructed a two-tier edge computing resource sharing framework that takes into account the benefits of the fog service provider, resulting in higher system utilization. Chen et al. [29] designed a fog computing resource contribution system consisting of a remote cloud server, computing access point (CAP) and users, and designed the CAP as a mobile user. Agarwal et al. [30] used virtualization technology to analyze potential threats and attacks in the fog computing environment and constructed a cloud architecture with elastic resource allocation. Deng et al. [31] developed a systematic framework to study the trade-off between power consumption and latency in cloud systems.

In the above approaches, most of the researchers analyzed the resource contribution methods of different resource providers from a static perspective and did not consider the interaction between resource contributors. In practical applications, the resource requirements of cloud service providers or users change dynamically, and contributing resources are not 100% successful [32] (or 100% total contribution). Hence, it is significant to design a reasonable resource contribution scheme under the premise of fully considering the dynamic changes of resource demand in time and the success rate of contribution.

The authors of [33] analyze the rapid development of IoT services, carry out analysis concerning the innovative application of blockchain technology based on the fog computing architecture, and propose a fog computing architecture which is built on Hyperledger Fabric of Fog computing (HCL-BaFog) based on blockchain. This architecture enables efficient and secure collection and sharing of sensor-sensitive data, especially in smart homes and applications requiring secure electronic medical applications. The proposed architecture uses the license chain and the full virtualization capabilities of the fog compute node network. It also utilizes the container orchestration and management system

Docker and multi-chain frameworks to test some of the necessary performance metrics of the proposed architecture using Raspberry Pi System Basis Chips (SBCs).

In [34], Tang et al. consider the scenario in the fog computing offload environment in which mobile users may mistakenly transfer computing tasks to nearby fog servers that are attacked, causing a series of privacy and security issues. In response to this challenge, the authors introduced blockchain technology into the fog computing environment and sought to check the accuracy and authenticity of the fog server performing the unloading in a short time. More in detail, they use the characteristics of collective maintenance in blockchain technology to continuously maintain a set of authorized fog servers to ensure the accuracy and authenticity of the unloaded fog server when the uninstall task is executed.

A blockchain-based distributed cloud architecture is proposed in [35]. The proposed solution practices software-defined networking technologies to provide the need for on-demand access to make secure and low-cost the IoT networks. Moreover, it brings computing resources to the edge of the IoT network, implements a secure distributed fog node architecture based on Software Defined Network (SDN), and designs blockchain intending to simplify the network traffic in the core network. At the same time, in the IoT device, minimal end-to-end latency and computational resources can be achieved. The results of the evaluation show that the system performance can be significantly improved by reducing induction delays, reducing response time, increasing throughput, and detecting real-time attacks.

Andreas et al. [36] introduced a decentralized market for industrial edge applications, Industrial Internet of Things (IIoT) Bazaar, which uses the blockchain's collective maintenance, timing, and other features to create high transparency for users while ensuring edge device applications. The traceability of the installation considerably improves the safety of the edge device. At the same time, the use of fog calculations integrates resource-constrained edge devices into the IIoT Bazaar ecosystem. In the meantime, Augmented Reality (AR) technology is used to enable more intuitive human-computer interaction between users and edge devices. Through their research, software developers and users can be brought together jointly, so that people can provide a variety of performance needs more conveniently.

Gulshan et al. [37] proposed a statistical method to solve the expected value of a mathematical problem in the PoW consensus, to make the blockchain better suited for cloud computing or fog computing. This method relies on the desired mathematical model and uses polynomial matrix decomposition to make it easier to obtain the PoW consensus solution, taking into account all the constraints of the mathematical puzzle. Because the proposed method is not complicated and easy to model and configure, it also has lower time complexity and memory consumption, so that the blockchain technology can be better combined with the cloud computing or fog computing architecture.

Zhu and Youakim [38] introduced a mixture of networking architecture. This architecture combines a blockchain-based social network to support the fog computing architecture, ensuring security in an untrusted IoT environment. Therefore, users can establish tamper-resistant digital identity management intelligent objects in an environment with a low-trust level, and establish a series of new authentication and authorization mechanisms for the Internet of Things system, which significantly improves the security performance of the traditional IoT system.

Jiao et al. [39] introduced an auction-based market model to efficiently perform computational resource allocation in a cloud or fog computing environment. The main aim is to offload computing tasks in the PoW and to solve cloud problems in a cloud or fog server computing resources. The authors consider that the computing resources in the PoW-based blockchain network are limited, and the allocation of externalities is individually considered when designing the auction mechanism. Instead, they have developed two bidding options, the fixed demand plan and the multiple demand plan. The approximation algorithm solves the NP problem of maximizing the return of all participants in the multiple schemes.

Li et al. [40] consider that, in the fog-based car networking environment, the users may have a certain degree of security and privacy issues when sharing their sensitive information (such as identity and location) during carpooling. This situation could allow malicious users to upload incorrect location information to produce errors in the matching system. The authors propose a carpooling scheme that is efficient and protects user privacy. The scheme uses blockchain technology to assist vehicles to support conditional privacy, with one-to-many target matching and data auditable traceability. The performance of the scheme is evaluated based on the computational cost and communication overhead.

Randa et al. [41] propose a user authentication scheme in a fog node that involves blockchain. The fog node in the scheme and the Ethereum contract interface are employed for user access to the IoT device for authentication. The fog node provides scalability for the entire system by mitigating the heavy computational tasks of IoT devices.

Pan et al. [42] designed a marginal Internet of things framework, called EdgeChain internal tokens. This framework integrates the licensed chain system by moving the edge server resource pool and the behavior of the state of each IoT devices together. Moreover, the proposed framework is supplemented by a resource management system based on a credit scheme and intelligent contract. The solution introduced by the authors can standardize the behavior of Internet equipment, to control the IoT devices from the edge of the server resources.

In the above research, scholars mostly use the characteristics of collective maintenance, traceability, and high security in blockchain technology to solve security problems in the fog computing environment [33–35,38,40], and resource allocation issues [39,42]. Some scholars have also studied the problem of the blockchain itself so that it can better serve cloud computing or fog computing [37]. Further, some scholars have developed blockchain-based systems under the environment of cloud computing or fog computing [36,41]. Although there are still some problems in the above studies, such as low system throughput, high energy consumption, and too ideal experimental environment, it can be recognized that the use of blockchain technology could solve many problems in fog calculation, and it is a simple and efficient way.

### 1.3. Motivations and Contributions

The rise of blockchain technology provides the possibility to solve the resource management problem of fog computing. At the same time, it cryptographically guarantees the data's irreversible and unforgeable characteristics and also protects the data security of users in the fog computing environment [43]. Besides, cloud service providers, fog service providers, and users in the fog computing environment also correspond to the identity characteristics of the alliance chain participants.

Therefore, the primary goal of this paper is to propose a fog computing resource contribution model based on an alliance chain and advances the blockchain system into the fog computing network architecture. The reward and punishment mechanism of blockchain is used to boost fog computing nodes to contribute resources actively and to solve the resource management problem of fog computing. The resource contribution behavior of fog nodes and the satisfaction degree of task completion are recorded in the blockchain form, producing an untamable evaluation system, which can solve problems such as malicious bad review and brushing in practical applications.

The primary contributions of this paper can be summarized as follows:

- A blockchain-based fog computing resource contribution model is proposed, which considers a satisfaction degree (task completion degree) as an evaluation index for service provided by fog computing service providers.
- Using differential game theory to solve the proposed model, the numerical simulation is used to discuss the interaction between the optimal resource contribution strategy of the fog node and the optimal benefit under the optimal strategy.



The rest of the paper is structured as follows: In Section 2, the construction process of the proposed model is presented and explained by a differential game method. The validity of the experimental results is verified by the numerical simulation experiment in Section 3. Finally, in Section 4, the work carried out in this paper is sorted out, and the future research direction is discussed.

## 2. Materials and Methods

### 2.1. Problem Formulation and System Model

Fog computing, as an extension of the cloud computing model, is a weakly centralized computing paradigm compared to cloud computing. The coalition chain model in the blockchain is also a traditional centralized public chain. A weakly centralized form of distributed computing allows combining the two structures. This paper proposes a resource contribution model for fog computing based on the coalition chain technology in blockchain, which combines the fog calculation to make full use of the idle resource cooperation mode and the characteristics of the incentive model in the blockchain technology to solve the problem of resource contribution in fog computing. At the same time, the safety of the fog computing itself is solved by the high security and non-destructible modification of the blockchain technology.

Figure 1 shows a blockchain-based fog computing architecture diagram, which is a typical fog computing three-layer architecture scenario. Full nodes with all block information are placed in the cloud data center. The fog computing device has limited performance and storage capacity and is a weak node in some circumstances. The light nodes in the blockchain are deployed in the fog computing device and, according to the difference in device performance, can be used to run the number of blocks that the device can withstand. After the nodes in the blockchain access the system, a series of activities, such as creating a block or voting, need to be performed. Each activity needs to record the identity of the participating nodes or verify it. Therefore, each node (i.e., the fog computing device in the figure) adds an asymmetric key as the identity. Under this mechanism, every transaction in the system can be tracked, and the disguise of illegal nodes is also prevented.

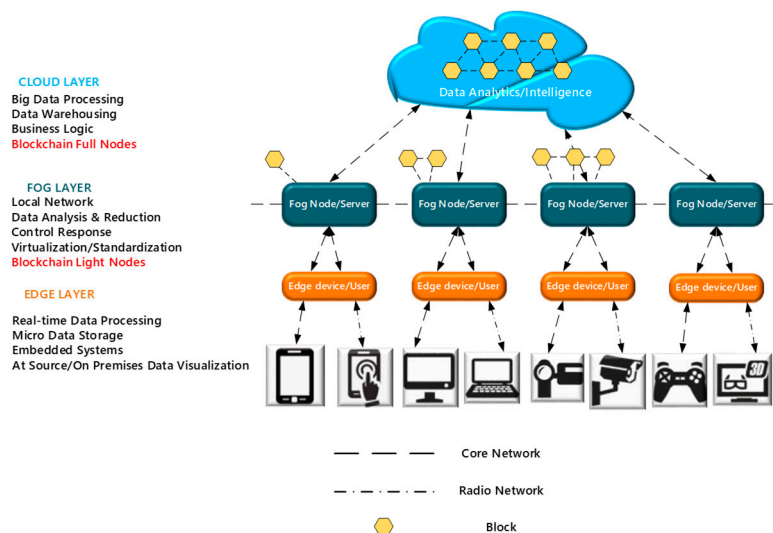


Figure 1. Blockchain-based fog computing architecture diagram.

As depicted in Figure 2, when the cloud data center issued a task (or other nodes request service), it requires fog node to contribute resource cooperation to complete the task. At this point, in broadcasting system, it is necessary to find the positive contribution of resources in fog node to complete the task, while, at the end of the task, it will be relevant the task information (start time, task types, task to complete satisfaction, equivalent public key, and signature information identification equipment) to be managed into a “deal” information. The above information is converted into a certain

length of hash through a chain system. The blockchain system verifies the rationality of the converted “transaction” information and sends it to the trading pool after verification. After the time specified by the system, the blockchain system encapsulates the transaction records in the transaction pool for some time and broadcasts them. At this time, the blockchain system decides the voting win according to the DPoS consensus [17], taking into account that the performance of fog node is limited, and the computing resources are limited. Consequently, this paper adopts the DPoS consensus with low computational requirements to complete the consensus link of the block system. Besides, the design of the consensus algorithm is not the focus of this paper, so the improved DPoS consensus algorithm is adopted [44] to complete the consensus process under the architecture proposed in this work.

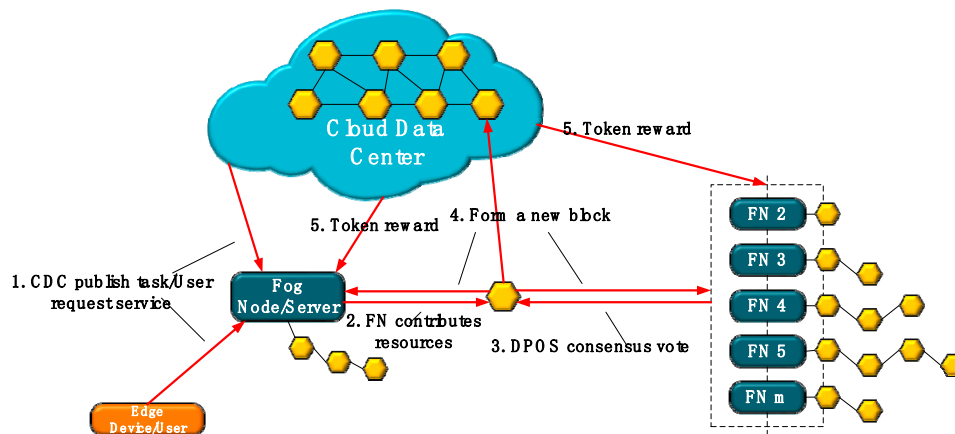


Figure 2. Fog node contribution resource behavior schematic diagram.

The DPoS consensus elects a group of proxy nodes (consensus committees) through elections. These nodes are responsible for packing and message records of the blocks, while other nodes are only responsible for monitoring and forwarding. In general, the DPoS consensus process is divided into two parts: The election of the consensus member status in the agent node group and the scheduling and production of its responsible block. Considering that block producers are primarily fixed, DPoS is a consensus solution that sacrifices decentralized features to improve system throughput. Once the rights of the consensus committee are too high, and there are malicious nodes mixed in it, it will cause more significant harm to the entire blockchain system. According to the approach introduced in [44], the improved DPoS algorithm can be applied to the environment of the alliance chain.

Specifically, the consensus program includes: setup, proposal, consensus identity generation, voting, and counting of several processes.

- Setup: When a new node  $FNode_i$  (whose public and private key is  $\langle K_i^P, K_i^S \rangle$ ) is added to the system, the newly joined node first updates its public key to the member public key  $MK_i^P$ ; next, the new public key will be used to calculate the membership signature  $MS_i$ :

$$FN \mid MS_i = (a \cdot K_i^S) \times H(MK_i^P, i), \tag{1}$$

where  $a_i = h(K_i^P \parallel K_1^P \parallel \dots \parallel K_n^P)$ . When the federation chain receives the information  $\langle K_i^P, MS_i \rangle$  disclosed by the new node, each consensus node needs to update its member public and private key to  $MK_i^S$ :

$$MK_i^S = \sum_{i=1}^{i=n} (a \cdot K_i^S) \times H(MK_i^P, i), \tag{2}$$

- Proposal: The types of proposals in the consensus phase mainly include the consensus node in the alliance chain, which allows the new node to join the new consensus member proposal in the alliance,  $prop_{creat}$ ; proposal to package “transaction information” into blocks and upload them to

the alliance chain,  $prop_{block}$ ; proposal to deal with forks and eventually reach a consensus,  $prop_{fork}$ ; proposal to discover and punish a malicious user,  $prop_{punishment}$ .

- Consensus identity generation: When the consensus node of the alliance chain receives the proposal to create a new consensus member, it verifies that the random function calculates the condition of participating in the consensus committee according to its stack. If the condition is met and the identity is legal, the consensus vote is performed. The specific algorithm is shown in Algorithm 1.

---

**Algorithm 1.** Algorithm of creating a new node in Delegated Proof of Stake (DPoS).

---

Input:  $w_{inf}$  (The influence of the fog computing node, stake);  $\langle K_i^P, MS_i \rangle$  (Node information); seed:  $H_{pre}$  or  $H_{pro}$ ;  $prop_{creat}$

Output: MCC: Membership of Consensus Committee or Null

```

1: MCC ← empty; p ← winf / ⟨KiP, MSi⟩; i ← 0
2: ⟨hash, proof⟩ ← VRFpk(Seed || propcreat)
3: index ← hash / 2len(hash)
4: while index ∉ [∑k=0i Block(k, ⟨KiP, MSi⟩, p), ∑k=0i+1 Block(k, ⟨KiP, MSi⟩, p)] do
5: i ++
6: end while
7: if i > 0 then
8: MCC.pk ← ⟨KiP, MSi⟩.pk; MCC.i ← i
9: MCC.hash ← hash.pk; MCC.proof ← proof
10: return MCC
11: else
12: return null

```

---

- Voting: consensus nodes with legal status in the alliance chain vote for consensus based on the type of proposal received, as shown below:

$$Sig_i = K_i^S \times H(MK_i^P, prop) + MK_i^S, \tag{3}$$

Then package its consensus identity and the hash value of the proposed result into  $\langle MCC, h(prop), Sig_i \rangle$ , and broadcast to other nodes in the alliance chain.

- Counting: The node of the alliance chain collects the consensus votes received. When the number of votes of a proposal exceeds the threshold set by the system and the signature set is verified, the consensus node reaches a consensus.

After the DPoS consensus process is over, the consensus node will package the proposed “transaction information” into blocks and upload them to the blockchain system database. The new block is now established.

At this time, token rewards of a certain proportion are given to the nodes that participate in the verification of voting records in the process of transaction initiator, namely resource contributor and DPoS link, so as to continuously encourage fog nodes to actively contribute resources and promote other fog nodes to jointly maintain the fog computing ecosystem based on blockchain. The token mechanism in the blockchain, due to its high security and non-tamper ability, compared to the traditional fiat currency payment incentive mechanism, has the following characteristics:

- Cryptographic digital currency is a decentralized currency compared to legal tender. As the most successful product of blockchain technology, cryptographic digital currency allows people to move freely and securely from one currency to another without the help of intermediaries. The issuance of money is done spontaneously and impartially by the participants and is not supervised by any external agency, even the central bank or government agency.



- Compared with legal tender, encrypted digital currency is encrypted and anonymous. Encrypted digital currency based on blockchain technology has all the advantages of blockchain technology to ensure the security of all aspects of currency circulation. Moreover, the private key is the only voucher for holding the currency. The public key is publicly disclosed and does not bind any personal information of the private key holder, making the operation anonymous.
- Compared with traditional electronic currency, digital currency is a kind of currency that cannot be tampered with and is open and transparent. Since accounts for encrypted digital currency are recorded in the public ledger of blockchain, it means that transactions for digital currency, once confirmed, cannot be tampered with and are open to all users across the network.
- Compared with traditional electronic money, digital money can deliver value. In the Internet, traditional electronic currency can only deliver information, but cannot deliver value. Every transfer of encrypted digital currency in the network is itself a transfer of value, and transfer is a re-authorization of the right to use value.

The process of fog nodes contributing resources and completing tasks is regarded as the “transaction” behavior in the blockchain. The behavior log of resources contributed by fog node is regarded as the “asset” in the blockchain and uploaded to the blockchain network. The new block is generated and recorded permanently in the “ledger” According to blockchain technology, once records cannot be tampered with, the time stamp can be trading information for traceability and high-security features, such as when the fog is used to calculate the abnormal conditions of network nodes. According to the record information in the “book” traceability, other blocks of tokens in the chain system are an incentive mechanism to make the fog compute node jointly maintain the entire network environment. At the same time, considering the task satisfaction  $M$  as a record to keep in the ledger, its essence is a transparent, open, non-tamper (brushing) evaluation system, which undoubtedly brings long-term economic benefits for fog providers, as shown in Figure 3.

It is particularly noticeable that the blockchain technology used in this paper is the alliance chain, and the token issued in this paper should not be qualified to exchange with legal coins, but only circulated within the economic system of the alliance, which has many functions such as purchasing upper cloud service resources, lower user information, and extra transmission bandwidth. Token issued under this architecture is not only resource currency to some extent because when the node of the alliance system has an abnormal condition, the behavior log, which has been recorded in the ledger, becomes a piece of valuable asset information. At this time, the token becomes an asset currency with an asset tag. At the same time, considering the satisfaction of task completion kept in the ledger, it provides transparent and tamper-proof evaluation indexes for upper cloud service providers and lowers users when they select the fog service, which is undoubtedly the feature of token asset currency under this architecture.

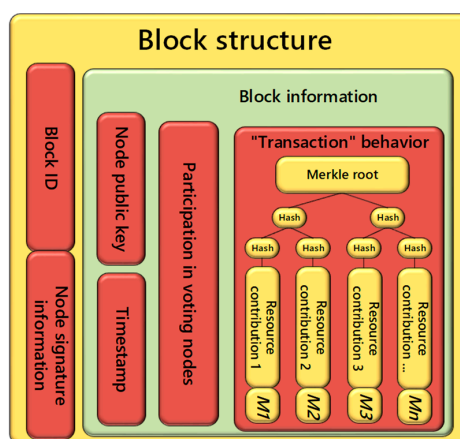


Figure 3. Block information.

The vote in all participating nodes in the process of verification records will also get a round of voting block ID, in the “the last round of voting block ID” in the collection, selected with the most votes in the block as before a block of new blocks. According to this mechanism, as shown in Figure 4, it is possible to connect the whole block following the order, under the condition of the resources consumed less as far as possible.

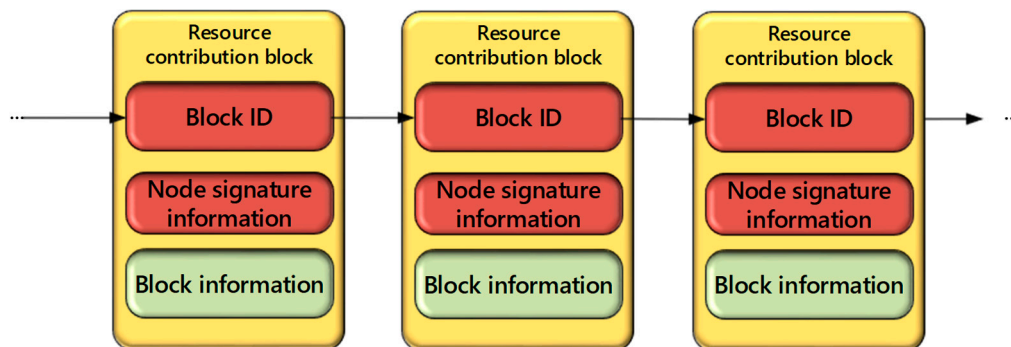


Figure 4. The chain structure.

However, the resources, computing power, and storage capacity of fog nodes are limited. For this reason, there are usually weak nodes, which consume their equipment while contributing resources. Therefore, the fog node cannot contribute to unlimited resources for the reward. Anyhow, the reward obtained by completing the task cannot be as much as the cost consumed by itself. Due to the DPoS consensus mechanism, the authorized nodes involved in bookkeeping need to maintain a specific online time rate (usually 99%), which undoubtedly leads to the loss of power [45].

Therefore, it is advisable to assume that  $N = \{1, 2, \dots, n\}$  is the collection of fog nodes,  $m$  is the number of fog nodes involved in a contribution behavior  $m \in N$ , and  $c_i(t)$  is the resource contribution of fog nodes. The above problem can be described as: How to contribute a reasonable amount of resource  $c_i(t)$  to maximize the income of fog nodes  $\phi_i(t)$ . (This paper assumes that fog nodes are rational and selfish individuals who lack trust in each other but need to cooperate to complete tasks).

Therefore, we have:

$$\phi_i(t) = R \cdot \zeta \cdot P \cdot c_i(t) - \gamma_i c_i(t) - \sum_{j \in N - m, i \neq j} \chi c_j(t) M(t), \tag{4}$$

where  $R$  is the token of system reward;  $\zeta$  is the reward coefficient, that is, in a resource contribution behavior, the proportion of the reward obtained by the node in the total reward;  $P$  is the success rate of the resource contribution by the fog node;  $\gamma_i$  is the power consumption coefficient of the fog node. Considering that the fog node is not able to complete the task with 100% probability, the success rate of introducing contributed resources is related to not only the power (in this paper, the power of fog node is used to characterize the equipment performance of fog node, that is, the larger  $\alpha_i$  is, the better the performance will be) of the fog node itself, but also the number of transactions  $k_i$  after the introduction of the blockchain system, that is,  $P(\alpha_i, k_i)$  [46]. In addition, according to the definition in literature [47], when trading blocks in the transmission will be affected by the transaction number  $k_i$  and lead to a longer confirm delay, if, in a certain period of time, it has not been confirmed or by other blocks in the first step, then the block is thought to have been discarded, so this kind of situation is called orphaning, that is, there is an orphaning probability According to [48],  $P_{gl}$  follows a Poisson distribution, namely:

$$P_{gl}(k_i) = 1 - e^{-\lambda z k_i}, \tag{5}$$

where  $\lambda = 1/600$  sec and  $z > 0$  are denoted as time delays. Since the alliance chain is adopted in this paper,  $\lambda$  satisfies  $0 < \lambda < 1$ .

Thus, we can get:

$$P = \alpha_i(1 - P_{gl}) = \alpha_i e^{-\lambda z k_i}, \tag{6}$$

In addition, through the previous narrative we know that the reward R is issued after the new block is generated. Therefore, the reward of the resource contribution of the fog node should have a weight relationship between the itself resource contribution amount  $c_i(t)$  and the  $k_i$  transaction numbers of the constituent blocks  $\zeta$ , as (7).

$$\zeta = \frac{\beta_i \cdot c_i(t)}{\sum_{i \in k_i} c_i(t)}, \tag{7}$$

where  $\beta_i$  is the power dissipation factor.

As mentioned above,  $M$  is the satisfaction of each "transaction", that is, the task completion degree of each time the fog node contributes resources. When the satisfaction of other fog nodes ( $N - m$ ) in the alliance is high, it will inevitably affect their own earnings. We assume that  $\sum_{j \in N-m, i \neq j} \chi c_j(t) M(t)$  is used to express the negative benefit of satisfaction  $M$  on the fog node, where  $\chi$  is the loss coefficient, then we can get  $\phi_i(t)$  as (8):

$$\phi_i(t) = R \cdot \frac{c_i(t)}{\sum_{i \in k_i} c_i(t)} \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i} \cdot c_i(t) - \gamma_i c_i(t) - \sum_{j \in N-m, i \neq j} \chi c_j(t) M(t). \tag{8}$$

In the architecture proposed in this paper, once the fog node completes the task, there will be a record of satisfaction  $M$ . That is, satisfaction  $M$  is a function of  $c_i(t)$ , then we assume the average level of satisfaction in the system architecture. The process of change is:

$$\frac{dM(t)}{dt} = \theta M(t) + \sum_{i \in N} \omega c_i(t) + \sum_{i \in m} H_i c_i(t), \tag{9}$$

where  $\theta \in [0, 1]$  is the change parameter of the satisfaction level; and  $\omega \in [-1, 1]$  is the effective parameter of the resource contribution;  $H_i$  is the satisfaction effect brought by the hash operation [49–51]. This is because the high-security, inextricable modification, and traceability of the blockchain, the generation and transmission of transaction information, and the verification and recording between nodes are required. Hash operation based on Secure Hash Algorithm (SHA) leads to additional waiting time, which will affect the final satisfaction evaluation. The whole system model diagram is shown in Figure 5.

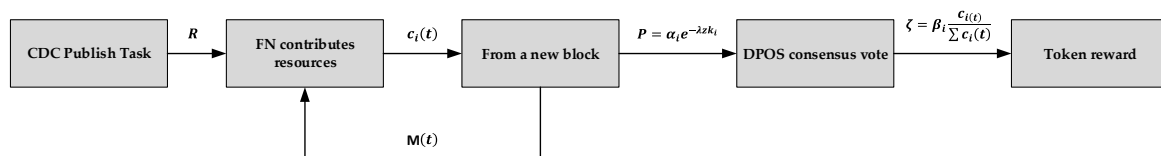


Figure 5. System model diagram.

### 2.2. Game Formulation and Model Solving

As mentioned above, fog nodes are usually selfish and rational, that is, they will not contribute resources endlessly without considering the cost. Furthermore, fog nodes should fully consider the tradeoff between income and cost. In the game, the fog node as the player needs to choose the optimal strategy to maximize its own revenue, and the differential game can clearly describe the dynamic process of the player's optimal strategy selection. Therefore, the following differential game model

can be established to optimize the resource contribution  $c_i(t)$  of fog node  $i$  and maximize its own benefit  $\phi_i(t)$ :

$$G = \max_{c_i(t)} \int_0^T e^{-rt} \left\{ R \cdot \frac{c_i(t)}{\sum_{i \in k_i} c_i(t)} \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i} \cdot c_i(t) - \gamma_i c_i(t) - \sum_{j \in N-m, i \neq j} \chi c_j(t) M(t) \right\} dt, \quad (10)$$

where  $r$  is the discounted parameter, that is, the future income of the fog node is converted into the parameter of the current value between 0 and 1, and the energy consumption change in the process of contributing the resource by the fog node satisfies the formula (9).

We assume that the strategy set  $\{c_i^*(t) = u_i^*(\cdot), i \in N\}$  constitutes a feedback Nash equilibrium solution for the finite time domain games (10) and (9), and if and only if there is a continuous differentiable function  $V^i(M, t) : R^m \rightarrow R$ , the following Bellman equations are satisfied [52]:

$$-V^i(M, t) = R \cdot \frac{c_i(t)}{\sum_{i \in k_i} c_i(t)} \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i} \cdot c_i(t) - \gamma_i c_i(t) - \sum_{j \in N-m, i \neq j} \chi c_j(t) M(t) + V_E^i(M, t) [\theta M(t) + \sum_{i \in N} \omega c_i(t) + \sum_{i \in m} H_i c_i(t)] \quad (11)$$

Deriving  $c_i(t)$  on the right side of (11) and letting it be 0 gives the optimal solution  $u_i^*(t)$ :

$$u_i^*(t) = \frac{\gamma_i + H_i \cdot V_M^i - R \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i} + V_M^i \cdot \omega - \sqrt{\frac{R \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i} - V_M^i (\omega + H_i) - \gamma_i}{R \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i}}}}{\gamma_i + H_i \cdot V_M^i - R \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i} + V_M^i \cdot \omega + \sqrt{\frac{R \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i} - V_M^i (\omega + H_i) - \gamma_i}{R \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i}}}} \quad (12)$$

Due to the characteristics of the differential game solution, considering the characteristics of (10), this paper uses the form of  $V^i(M, t) = AM + B$  to solve, that is:

$$V^i(M, t) = e^{-rt} [A(t)M + B(t)]. \quad (13)$$

The above formula is obtained by deriving  $t$  and  $M$ , respectively:

$$V_M^i = e^{-rt} \cdot A(t). \quad (14)$$

$$V_t^i = e^{-rt} [-rA(t) + \dot{A}(t)] \cdot M + e^{-rt} [-rB(t) + \dot{B}(t)]. \quad (15)$$

Simultaneous (11), (14), and (15) are obtained according to the corresponding coefficient:

$$\dot{A}(t) = (r - \theta)A(t) + \sum_{j \in N-m, i \neq j} \chi c_j(t). \quad (16)$$

$$\dot{B}(t) = rB(t) - R \cdot \frac{c_i(t)}{\sum_{i \in k_i} c_i(t)} \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i} \cdot c_i(t) - \gamma_i c_i(t) - A(t) \left[ \sum_{i \in N} \omega c_i(t) - \sum_{i \in m} H_i c_i(t) \right]. \quad (17)$$

Substituting (14) and (16) into (12), we get:

$$u_i^*(t) = \frac{\gamma_i + H_i \cdot e^{-rt} \cdot A(t) - R \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i} + e^{-rt} \cdot A(t) \cdot \omega - \sqrt{\frac{R \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i} - e^{-rt} \cdot A(t) (\omega + H_i) - \gamma_i}{R \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i}}}}{\gamma_i + H_i \cdot e^{-rt} \cdot A(t) - R \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i} + e^{-rt} \cdot A(t) \cdot \omega + \sqrt{\frac{R \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i} - e^{-rt} \cdot A(t) (\omega + H_i) - \gamma_i}{R \cdot \beta_i \cdot \alpha_i e^{-\lambda z k_i}}}} \quad (18)$$

Substituting the above formula into (4) and (9), we get the optimal income  $\phi_i^*(t)$  and satisfaction  $M^*(t)$  under optimal control:

$$\phi_i^*(t) = R \cdot \frac{u_i^*(t)}{\sum_{i \in k_i} u_i^*(t)} \cdot \beta_i \cdot \alpha_i \cdot e^{-\lambda z k_i} \cdot u_i^*(t) - \gamma_i u_i^*(t) - \sum_{j \in N-m, i \neq j} \chi u_j^*(t) M^*(t) \tag{19}$$

$$\frac{dM^*(t)}{dt} = \theta M^*(t) + \sum_{i \in N} \omega u_i^*(t) + \sum_{i \in m} H_i u_i^*(t), \tag{20}$$

$$\left\{ \begin{aligned} u_i^*(t) &= \frac{\gamma_i + H_i \cdot e^{-rt} \cdot A(t) - R \cdot \beta_i \cdot \alpha_i \cdot e^{-\lambda z k_i} + e^{-rt} \cdot A(t) \cdot \omega - \sqrt{\frac{R \cdot \beta_i \cdot \alpha_i \cdot e^{-\lambda z k_i} - e^{-rt} \cdot A(t) \cdot (\omega + H_i) - \gamma_i}{R \cdot \beta_i \cdot \alpha_i \cdot e^{-\lambda z k_i}}}}{\gamma_i + H_i \cdot e^{-rt} \cdot A(t) - R \cdot \beta_i \cdot \alpha_i \cdot e^{-\lambda z k_i} + e^{-rt} \cdot A(t) \cdot \omega + \sqrt{\frac{R \cdot \beta_i \cdot \alpha_i \cdot e^{-\lambda z k_i} - e^{-rt} \cdot A(t) \cdot (\omega + H_i) - \gamma_i}{R \cdot \beta_i \cdot \alpha_i \cdot e^{-\lambda z k_i}}}} \\ \phi_i^*(t) &= R \cdot \frac{u_i^*(t)}{\sum_{i \in k_i} u_i^*(t)} \cdot \beta_i \cdot \alpha_i \cdot e^{-\lambda z k_i} \cdot u_i^*(t) - \gamma_i u_i^*(t) - \sum_{j \in N-m, i \neq j} \chi u_j^*(t) M^*(t) \\ \frac{dM^*(t)}{dt} &= \theta M^*(t) + \sum_{i \in N} \omega u_i^*(t) + \sum_{i \in m} H_i u_i^*(t) \end{aligned} \right. \tag{21}$$

From this we can get the differential Equation (21):

Based on the above, Algorithm 2 gives the realization process of the resource contribution algorithm of the fog computing node based on blockchain:

---

**Algorithm 2.** The resources contribution algorithm of fog computing nodes based on blockchain.

---

A Differential Game Algorithm for Fog Computing Node Resource Contribution Based on Blockchain

Input: Total number of nodes N, Differential equation (21)

Output: Optimal strategy  $u_i^*(t)$ , Optimal income  $\phi_i^*(t)$ , Satisfaction  $M^*(t)$

1. Set equation parameters  $\gamma, H, k, \alpha, \beta, \lambda, z, \omega, r, R, \chi, \theta$
  2. For  $t = 1$  to T
  3. Solve the optimal strategy  $u_i^*(t)$  using equations (11), (14), and (16)
  4. Using equation (18) to solve the optimal benefit  $\phi_i^*(t)$  and satisfaction  $M^*(t)$
  5. Solving the optimal state trajectory using equation (21)
  6. End For
  7. Return optimal state, optimal strategy and optimal revenue track
- 

The results of (18), (19), and (20) are validated in the next section.

### 3. Results

In this paper, MATLAB R2018b simulation software was used to numerically simulate the optimal resource contribution  $u_i^*(t)$  (GB) of the fog node and the fog node's own income  $\phi_i^*(t)$  (Yuan.¥) under the optimal resource contribution, and the fog cluster overall satisfaction  $M^*(t)$ , the specific parameters are shown in Table 1.

**Table 1.** Simulation parameter.

	$\gamma_i$ (¥/GB)	$H_i$ (¥/GB)	$k_i$	$\alpha_i$ (W)	$\beta_i$ (GB <sup>-1</sup> ·W <sup>-1</sup> )	$\lambda$ (S <sup>-1</sup> )	$z$	$\omega$	$r$	$R$ (¥)	$\chi$ (¥/GB)	$\theta$
i = 1	0.35	0.2		12.5	0.4							
i = 2	0.45	0.3		25	0.5	0.25	1	0.5	0.05	100	0.25	0.1
i = 3	0.55	0.4	60	37.5	0.6							
i = 4	0.6	0.5		50	0.7							

The variation trend of the optimal resource contribution  $u_i^*(t)$ , fog cluster overall satisfaction  $M^*(t)$ , and its own benefit  $\phi_i^*(t)$  under the optimal contribution in the game time T, as shown in Figure 6, were first analyzed. From the figure it is possible to get that as the game time goes on, the optimal resource contribution strategy  $u_i^*(t)$ , the satisfaction level  $M^*(t)$  of fog cluster, and the income  $\phi_i^*(t)$  of fog node all increase. With the passage of time, under the control of the optimal strategy  $u_i^*(t)$ , the yield  $\phi_i^*(t)$  of the fog node reaches the maximum and tends to be stable. It can be seen that the time

node at which the fog node reaches the optimal resource strategy is almost the same as the time node with the largest gain of its own; and the different fog nodes have different power, energy consumption, and hash power. Thus, it can be found that the smaller the power of the fog node, the more resources it needs to contribute; thus with the node with higher power, the resource contribution is relatively low. Observing its own benefits, the nodes with low power have higher returns because of the higher contribution, but the nodes with higher power are not necessarily lower. This is because the higher the power, the better the performance, and the higher the degree of completion of contributing resources, which indirectly affects its own revenue. That is to say, the better the performance of the fog node, the higher the amount of resource contribution that can be achieved. At the same time, the satisfaction level of the entire fog cluster is also at a relatively high level.

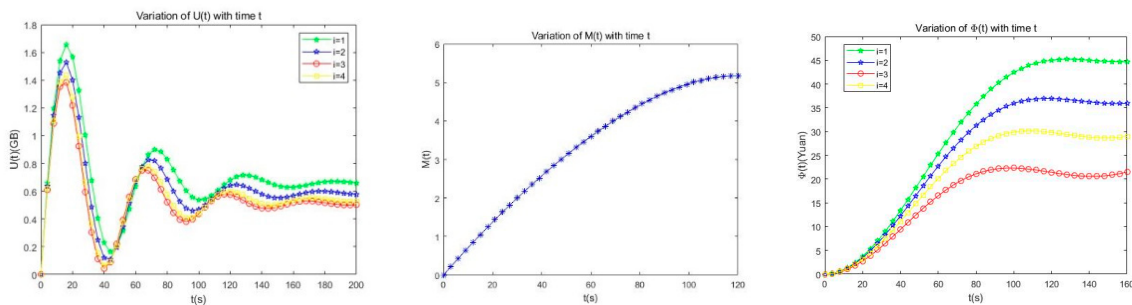


Figure 6. The variation of  $u_i^*(t)$ ,  $\phi_i^*(t)$  and  $M^*(t)$  with time  $t$ .

Figure 7 shows the trend of  $u_i^*(t)$ ,  $M^*(t)$ , and  $\phi_i^*(t)$  with parameter  $k_i$  at  $t = 4$ . We find that as the value of  $k_i$  increases,  $u_i^*(t)$ ,  $M^*(t)$ , and  $\phi_i^*(t)$  are incremented and then decremented after reaching the maximum value. This is because  $k_i$  is the number of transactions in each block. The more transactions there are, the greater the probability that the block will be orphaned. However, the smaller the number of transactions, the lower the throughput of the blockchain system will be. Therefore, it is necessary to dynamically adjust the number of transactions in the block by balancing the benefits of fog nodes with the use efficiency of the system.

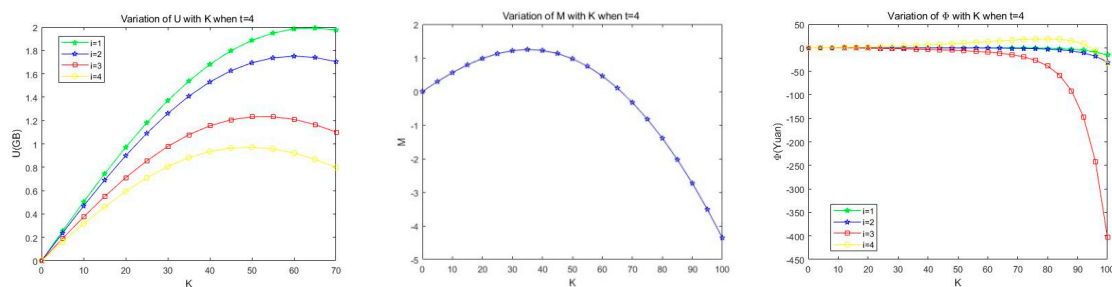


Figure 7. The variation of  $u_i^*(t)$ ,  $\phi_i^*(t)$ , and  $M^*(t)$  with  $k$  when  $t = 4$ .

Figure 8 shows that under different  $\lambda$  values the resource contribution of the fog node  $u_i^*(t)$  is increasing, and then decreasing after reaching the maximum value; while the satisfaction  $M^*(t)$  is different under four different  $\lambda$  values, when  $\lambda$  is small, the level of satisfaction is declining. This is because  $\lambda$  is the reciprocal of the trading time, that is, the transaction frequency. In [48],  $\lambda = 1/600$  sec, and “600 sec” is the transaction confirmation time of Bitcoin for one hour. So the smaller the  $\lambda$ , the slower the transaction speed, the lower the system efficiency, and the lower the level of satisfaction. When  $\lambda$  increases, the level of satisfaction  $M^*(t)$  also rises; when  $\lambda$  exceeds a certain range, the level of satisfaction  $M^*(t)$  decreases. This is because  $\lambda$  is also a parameter that affects the abandonment of the block. The larger  $\lambda$  is, the block is the probability of abandonment is also greater and thus the level of satisfaction  $M^*(t)$  is declining. Similarly, the fog node’s own gain  $\phi_i^*(t)$  also increases as the  $\lambda$  value increases, and decreases as it reaches the maximum value. In addition, when  $\lambda$  is larger, the



transaction frequency is faster, which leads to more frequent hashing, and the hash power loss  $H_i$  increases, thereby affecting the profit of the fog node itself. Therefore, the benefits of fog nodes and the use efficiency of the whole alliance chain system should be fully considered to dynamically adjust the size of  $\lambda$ .

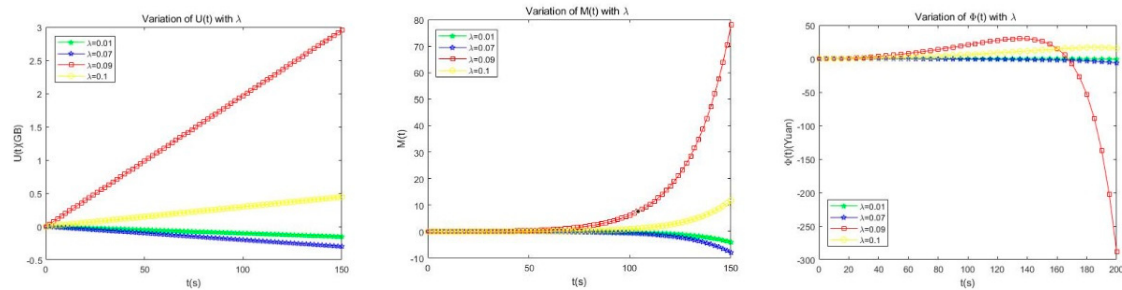


Figure 8. The variation of  $u_i^*(t)$ ,  $\phi_i^*(t)$ , and  $M^*(t)$  with  $\lambda$ .

#### 4. Discussion

In this paper, a model based on blockchain technology for resource contribution in fog computing nodes was presented. In particular, the differential game was utilized not only to construct the resource contribution model under the framework and simulate the optimal resource contribution strategy through mathematical experiments, but also to investigate the introduction of the blockchain system in the traditional fog computing architecture. It was recognized that the influence of critical parameters and the profit of the fog node can help the latter to optimize the resources management and maximize the benefits. In future works, it could be possible to model and analyze, from different perspectives (cloud service providers or users), other employments of the proposed framework to further solve the problem of fog computing in the field of resource management.

**Author Contributions:** All authors have read and agree to the published version of the manuscript. Conceptualization, H.W. and L.W.; methodology, H.W.; software, H.W.; validation, H.W., L.W. and Z.Z.; formal analysis, H.W.; investigation, X.T.; resources, H.W.; data curation, H.W.; writing—original draft preparation, H.W.; writing—review and editing, H.W.; visualization, H.W.; supervision, G.P.; project administration, F.A.; funding acquisition, L.W.

**Funding:** This research was funded by the National Natural Science Foundation of China, grant No. 61701020 and the National Key R&D Program of China, grant No. 2017YFC0806404.

**Conflicts of Interest:** The authors declare no conflicts of interest.

#### References

1. Ai, Z.; Zhou, Y.; Song, F. A smart collaborative routing protocol for reliable data diffusion in IoT scenarios. *Sensors* **2018**, *18*, 1926. [[CrossRef](#)] [[PubMed](#)]
2. Bonomi, F. Connected vehicles, the internet of things, and fog computing. In Proceedings of the Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, NV, USA, 19–23 September 2011; pp. 13–15.
3. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 17 August 2012; pp. 13–16.
4. Song, F.; Ai, Z.; Zhou, Y.; You, I.; Choo, R.; Zhang, H. Smart Collaborative Automation for Receive Buffer Control in Multipath Industrial Networks. *IEEE Trans. Ind. Inform.* **2019**. [[CrossRef](#)]
5. Vaquero, L.M.; Rodero-Merino, L. Finding your way in the fog: Towards a comprehensive definition of fog computing. *ACM SIGCOMM Comput. Commun. Rev.* **2014**, *44*, 27–32. [[CrossRef](#)]
6. Lin, F.; Zhou, Y.; You, I.; Lin, J.; An, X.; Lv, X. Content recommendation algorithm for intelligent navigator in fog computing based iot environment. *IEEE Access* **2019**, *7*, 53677–53686. [[CrossRef](#)]
7. Lin, F.; Zhou, Y.; Pau, G.; Collotta, M. Optimization-oriented resource allocation management for vehicular fog computing. *IEEE Access* **2018**, *6*, 69294–69303. [[CrossRef](#)]

8. Ai, Z.; Liu, Y.; Chang, L.; Lin, F.; Song, F. A Smart Collaborative Authentication Framework for Multi-dimensional Fine-grained Control. *IEEE Access*. in press.
9. Aazam, M.; Huh, E.N. Fog computing and smart gateway based communication for cloud of things. In Proceedings of the 2014 International Conference on Future Internet of Things and Cloud, Barcelona, Spain, 27–29 August 2014; pp. 464–470.
10. Datta, S.K.; Bonnet, C.; Haerri, J. Fog computing architecture to enable consumer centric internet of things services. In Proceedings of the 2015 International Symposium on Consumer Electronics (ISCE), Madrid, Spain, 24–26 June 2015; pp. 1–2.
11. Hui, H.; Zhou, C.; An, X.; Lin, F. A new resource allocation mechanism for security of mobile edge computing system. *IEEE Access* **2019**, *7*, 116886–116899. [[CrossRef](#)]
12. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 24 September 2019).
13. Yuan, Y.; Wang, F. Blockchain: The state of the art and future trends. *Acta Autom. Sin.* **2016**, *42*, 481–494.
14. Idelberger, F.; Governatori, G.; Riveret, R.; Sartor, G. Evaluation of logic-based smart contracts for blockchain systems. In *International Symposium on Rules and Rule Markup Languages for the Semantic Web*; Springer: Cham, Switzerland, 2016; pp. 167–183.
15. Jakobsson, M.; Juels, A. Proofs of Work and Bread Pudding Protocols (Extended Abstract). In *Secure Information Networks*; Springer: Boston, MA, USA, 1999.
16. Proof of Stack. Available online: [https://en.bitcoin.it/wiki/Proof\\_of\\_Stake](https://en.bitcoin.it/wiki/Proof_of_Stake) (accessed on 24 September 2019).
17. Delegated Proof of Stake. Available online: <http://docs.bitshares.org/bitshares/dpos.html> (accessed on 24 September 2019).
18. Song, F.; Zhou, Y.; Wang, Y.; Zhao, T.; You, I.; Zhang, H. Smart collaborative distribution for privacy enhancement in moving target defense. *Inf. Sci.* **2019**, *479*, 593–606. [[CrossRef](#)]
19. Zhang, H.; Zhang, Y.; Gu, Y.; Niyato, D.; Han, Z. A hierarchical game framework for resource management in fog computing. *IEEE Commun. Mag.* **2017**, *55*, 52–57. [[CrossRef](#)]
20. Zhao, Y.; Huang, Z.; Zhang, X.; Liu, W.; Zhang, Q.; Zhu, Z. A coalitional game based mechanism for resource sharing in geo-distributed mobile cloud computing. In Proceedings of the 2017 29th Chinese Control and Decision Conference (CCDC), Chongqing, China, 28–30 May 2017; pp. 3758–3763.
21. Nishio, T.; Shinkuma, R.; Takahashi, T.; Mandayam, N. Service-oriented heterogeneous resource sharing for optimizing service latency in mobile cloud. In Proceedings of the first international workshop on Mobile cloud computing & networking, Bangalore, India, 29 July 2013; pp. 19–26.
22. Dong, X.; Zheng, J.; Cai, Y.; Yang, J.; Wang, Y. Share communication and energy resources for mobile cloud computing: An optimal cooperative contract approach. In Proceedings of the 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 11–13 October 2017; pp. 1–6.
23. Ye, D.; Wu, M.; Tang, S.; Yu, R. Scalable fog computing with service offloading in bus networks. In Proceedings of the 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), Beijing, China, 25–27 June 2016; pp. 247–251.
24. Su, J.; Lin, F.; Zhou, X.; Lv, X. Steiner tree based optimal resource caching scheme in fog computing. *China Commun.* **2015**, *12*, 161–168. [[CrossRef](#)]
25. Alsaffar, A.A.; Pham, H.P.; Hong, C.S.; Huh, E.N.; Aazam, M. An architecture of IoT service delegation and resource allocation based on collaboration between fog and cloud computing. *Mob. Inf. Syst.* **2016**, *2016*, 6123234. [[CrossRef](#)]
26. Shi, H.; Chen, N.; Deters, R. Combining mobile and fog computing: Using CoAP to link mobile device clouds with fog computing. In Proceedings of the 2015 IEEE International Conference on Data Science and Data Intensive Systems (DSDIS), Sydney, Australia, 11–13 December 2015; pp. 564–571.
27. Neto, E.C.P.; Callou, G.; Aires, F. An algorithm to optimise the load distribution of fog environments. In Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 5–8 October 2017; pp. 1292–1297.
28. Kochar, V.; Sarkar, A. Real time resource allocation on a dynamic two level symbiotic fog architecture. In Proceedings of the 2016 Sixth International Symposium on Embedded Computing and System Design (ISED), Patna, India, 15–17 December 2016; pp. 49–55.

29. Chen, M.H.; Dong, M.; Liang, B. Resource sharing of a computing access point for multi-user mobile cloud offloading with delay constraints. *IEEE Trans. Mob. Comput.* **2018**, *17*, 2868–2881. [[CrossRef](#)]
30. Agarwal, S.; Yadav, S.; Yadav, A.K. An architecture for elastic resource allocation in Fog computing. *Int. J. Comput. Sci. Commun.* **2015**, *6*, 201–207.
31. Deng, R.; Lu, R.; Lai, C.; Luan, T.H. Towards power consumption-delay tradeoff by workload allocation in cloud-fog computing. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 3909–3914.
32. Song, F.; Zhou, Y.; Liu, C.; Zhang, H. Modeling Space-Terrestrial Integrated Networks with Smart Collaborative Theory. *IEEE Netw.* **2019**, *33*, 51–57. [[CrossRef](#)]
33. Cech, H.L.; Grobmann, M.; Krieger, U.R. A Fog Computing Architecture to Share Sensor Data by Means of Blockchain Functionality. In Proceedings of the 2019 IEEE International Conference on Fog Computing (ICFC), Prague, Czech Republic, 24–26 June 2019; pp. 31–40.
34. Tang, W.; Zhao, X.; Rafique, W.; Wanchun, D. A Blockchain-Based Offloading Approach in Fog Computing Environment. In Proceedings of the 2018 IEEE International Conference on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), Melbourne, Australia, 11–13 December 2018; pp. 308–315.
35. Pradip, K.; Sharma, P.K.; Chen, M.Y.; Park, J.H. A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access* **2018**, *6*, 115–124.
36. Seitz, A.; Henze, D.; Miehle, D.; Bruegge, B.; Nickles, J.; Sauer, M. Fog Computing as Enabler for Blockchain-Based IIoT App Marketplaces—A Case Study. In Proceedings of the 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, Valencia, Spain, 15–18 October 2018; pp. 182–188.
37. Kumar, G.; Saha, R.; Rai, M.K.; Thomas, R.; Kim, T.H. Proof-of-Work Consensus Approach in Blockchain Technology for Cloud and Fog Computing Using Maximization-Factorization Statistics. *IEEE Internet Things J.* **2019**, *6*, 6835–6842. [[CrossRef](#)]
38. Zhu, X.; Badr, Y. Fog Computing Security Architecture for the Internet of Things Using Blockchain-Based Social Networks. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1361–1366.
39. Jiao, Y.; Wang, P.; Niyato, D.; Suankaewmanee, K. Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks. *IEEE Trans. Parallel Distrib. Syst.* **2019**, *30*, 1975–1989. [[CrossRef](#)]
40. Li, M.; Zhu, L.; Lin, X. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. *IEEE Internet Things J.* **2019**, *6*, 4573–4584. [[CrossRef](#)]
41. Almadhoun, R.; Kadaha, M.; Alhemeiri, M.; Alshehhi, M.; Salah, K. A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–8.
42. Pan, J.; Wang, J.; Hester, A.; Alqerm, I.; Liu, Y.; Zhao, Y. EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts. *IEEE Internet Things J.* **2019**, *6*, 4719–4732. [[CrossRef](#)]
43. Hui, H.; Zhou, C.; Xu, S.; Lin, F. A novel secure data transmission scheme in industrial internet of things. *China Commun.* **2020**, *17*, 73–88.
44. Zhou, T.; Li, X.; Zhao, H. DLattice: A permission-less blockchain based on DPoS-BA-DAG consensus for data tokenization. *IEEE Access* **2019**, *7*, 39273–39287. [[CrossRef](#)]
45. Ai, Z.; Liu, Y.; Song, F.; Zhang, H. A smart collaborative charging algorithm for mobile power distribution in 5G networks. *IEEE Access* **2018**, *6*, 28668–28679. [[CrossRef](#)]
46. Xiong, Z.; Feng, S.; Wang, W.; Niyato, D.; Wang, P.; Han, Z. Cloud/Fog computing resource management and pricing for blockchain networks. *IEEE Internet Things J.* **2019**, *6*, 4585–4600. [[CrossRef](#)]
47. Houy, N. The Bitcoin mining game. 2014. Available online: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2407834](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407834) (accessed on 24 September 2019).
48. Orphan Probability Approximation. Available online: <https://gist.github.com/gavinandresen/5044482> (accessed on 24 September 2019).

49. Available online: <https://www.fxstreet.hk/news/lu-bi-ni-qu-kuai-lian-ke-neng-shi-you-shi-yi-lai-zui-kua-zhang-de-ji-shu-neng-hao-guo-da-201803120004> (accessed on 24 September 2019).
50. Available online: <https://www.coindesk.com/microscope-economic-environmental-costs-bitcoin-mining> (accessed on 24 September 2019).
51. Song, F.; Zhu, M.; Zhou, Y.; You, I.; Zhang, H. Smart collaborative tracking for ubiquitous power IoT in edge-cloud interplay domain. *IEEE Internet Things J.* in press.
52. Yeung, D.W.K.; Petrosjan, L.A. *Cooperative Stochastic Differential Games*; Springer Science & Business Media: Berlin, Germany, 2006.



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).