applied sciences

MDPI

Article

A Blockchain-Based Trust Model for Uploading Illegal Data Identification

Jieren Cheng [1,2], Yuanshen Li [2,3,*], Yuming Yuan [4], Bo Zhang [4] and Xinbin Xu [2,3]

[1] School of Computer Science and Technology, Hainan University, Haikou 570228, China
[2] Hainan Blockchain Technology Engineering Research Center, Hainan University, Haikou 570228, China
[3] School of Cyberspace Security Academy (Cryptography Academy), Hainan University, Haikou 570228, China
[4] Hainan Huochain Tech Company Limited, Haikou 570100, China
* Correspondence: 20083900210003@hainanu.edu.cn

Abstract: Malicious users can upload illegal data to the blockchain to spread it, resulting in serious threats due to the tamper-proof characteristics of the blockchain. However, the existing methods for uploading illegal data identification cannot select trust nodes and ensure the credibility of the identification results, leading to a decrease in the credibility of the methods. To solve the problem, this paper proposes a blockchain-based trust model for uploading illegal data identification. The trust model mainly has the following two core modules: Reputation-based random selection algorithm (RBRSA) and incentive mechanism. By assigning reputation attributes to nodes, the proposed RBRSA will select nodes according to reputation values. RBRSA favors the nodes with high reputation value to ensure the randomness and credibility of the identification nodes. The incentive mechanism is designed to ensure the credibility of the identification results through the credibility analysis of the model based on game theory and Nash equilibrium. Identification nodes that identify illegal data correctly will obtain incentives. In order to obtain a higher income, the identification nodes must identify illegal data correctly. Credibility analysis and comparative experiments show that the probability of selecting credible nodes by RBRSA is up to 23% higher than the random selection algorithm. The probability of selecting the nodes with a reputation value of 20 by RBRSA is 27% lower than the random selection algorithm; that is, the probability that RBRSA selects untrusted nodes is lower. Therefore, the nodes selected by RBRSA have superior credibility compared with other methods. In terms of the effect of the incentive mechanism, the incentive mechanism can encourage nodes to identify data credibly and improve the credibility of identification results. All in all, the trusted model has higher credibility than other methods.

Keywords: blockchain; trust model; smart contract; blockchain security

check for updates

Citation: Cheng, J.; Li, Y.; Yuan, Y.; Zhang, B.; Xu, X. A Blockchain-Based Trust Model for Uploading Illegal Data Identification. *Appl. Sci.* **2022**, *12*, 9657. https://doi.org/10.3390/app12199657

Academic Editors: Zhiping Cai, Yejun He and Ruoyu Su

Received: 29 August 2022
Accepted: 20 September 2022
Published: 26 September 2022

1. Introduction

A blockchain [1] is essentially a decentralized distributed ledger, which is composed of a series of blocks that record data [2]. The block header of each block has the cryptographic hash value of the previous block and is connected to the previous block through this hash value [3]. The blockchain has the characteristics of decentralization [4], tamper-proof [5], and anonymity [6]. Due to the tamper resistance and anonymity of the blockchain, the blockchain attracts many malicious users who use these features to upload harmful information and other illegal behaviors [7]. The occurrence of these security incidents has greatly adversely affected the development of blockchain technology, so it is necessary to control the blockchain. One of the directions is to use the technology of the blockchain to control the uploading of illegal data. The first step is to identify the uploading of illegal data through the technology of the blockchain. How to use the technology of the blockchain to realize the reliable identification of uploading illegal data is an urgent problem to be solved. It is of great significance for the long-term development of blockchain technology to strengthen the identification of illegal acts on the blockchain and establish an effective blockchain risk identification system.

In recent years, many scholars have discovered illegal data information on the chain. In 2014, Spagnuolo [8] proposed a modular framework called Bitlodine for identifying blockchain, investigating CryptoLocker ransomware, and accurately quantifying the amount of ransom paid and victim information. In 2016, Matzutt [9] identified and analyzed the data stored in the blockchain, classified various contents, and found some illegal information. In 2018, based on previous research, Matzutt [10] identified blockchain fund transfers and uploaded illegal content and found that in more than 1600 documents, most of them were text or images, and these documents had obvious illegal content. In 2020, Goldsmith [11] identified and analyzed the blockchain hacker subnetwork and found that hackers would change BTC into certain specific funds. In addition, according to the network characteristics, hackers were classified into different hacker groups. From the above brief literature review, it is evident that blockchain can store illegal data, but neither of them proposes a credible method to reduce such illegal events. Therefore, it is urgent to propose a credible identification model to reduce the occurrence of uploading illegal data.

In order to solve the problem of the low credibility of existing models, this paper proposes a blockchain-based trust model for uploading illegal data identification by adding a new identification blockchain to identify illegal data that is about to be on-chain in a decentralized voting manner. Nodes are designed as anonymous participants, which can be companies or individuals who wish to obtain income by identifying illegal data. Nodes are only selected as identification nodes by the selection algorithm. In the trust model, the incentive mechanism rewards or punishes the identification nodes based on their behavior. They must act honestly in order to obtain higher returns. The analysis of game theory and the Nash equilibrium principle proves its credibility.

The main contributions of this paper are as follows:

1. This paper proposes a trust model for uploading illegal data identification. The identification blockchain identifies the data by decentralized voting. Only when the number of votes exceeds the specified number will the identification blockchain consider the data as illegal data. The identification nodes can obtain benefits through the identification service. In order to obtain a higher income, they must identify the data fairly.
2. This paper designs a reputation-based random selection algorithm. The identification blockchain generates identification nodes by the reputation-based random selection algorithm. The algorithm tends to nodes with high reputation values. The seed is hashed by node total reputation value, block height, and timestamp. Each time you select an identification node, the seeds are hashed again. Ensure the randomness and credibility of the identification nodes.
3. This paper analyzes the model with game theory and proposes an incentive mechanism based on the results. This paper conducted a game theory analysis among the identification nodes. In order to obtain higher income, the identification nodes must honestly identify the data. According to the analysis, this paper designs an incentive mechanism for identification nodes. The incentive mechanism can punish or reward the identification nodes, which can encourage identification nodes to identify data fairly and impartially, thereby improving the credibility of the model.

The rest of the paper is organized as follows. The Section 2 discusses the related work on the models for uploading illegal data identification. The Section 3 introduces the blockchain-based trust model for uploading illegal data identification. The Section 4 introduces the key technologies such as reputation-based random selection algorithms and incentive mechanism design in detail and uses the Nash equilibrium principle to prove its credibility. The Section 5 introduces the prototype and experiment of the model. The Section 6 introduces the conclusions of the paper and future work.

2. Related Work

Blockchain identification can be roughly divided into the following two ways: on-chain identification and off-chain identification [12].

Off-chain identification is similar to a traditional direct democratic structure, involving R&D personnel and users at the core of the blockchain. The most famous examples are Bitcoin [13] and Ethereum [14]. The off-chain identification models are relatively concentrated. In addition to the corresponding operation on the blockchain, some operations are also needed outside the blockchain, which will consume time. In addition, the off-chain identification models for uploading illegal data are not very credible, and the efficiency is not high.

The on-chain identification model is a relatively new concept. The main difference is that the identification models are placed on the blockchain, and the identification is mainly realized by blockchain smart contracts. The blockchain has the characteristics of decentralization and can provide a basis of trust for two parties [15]. A smart contract is one of the key technologies of blockchain, which can automatically execute the contract content under certain conditions. It can achieve credible transactions without the involvement of third parties. Li [16] proposed a blockchain-based solution to the problem that house construction operation records are easy to be forged and tampered with and used the anti-tampering properties of the blockchain to achieve credible records of operations. Yong [17] proposed a blockchain-based solution for problems such as the falsification of vaccine records, which achieves a credible record of vaccine data by using the tamper-proof features of blockchain and smart contract technology. Omar [18] used smart contracts to design a general framework to solve the problem that it is difficult to accurately track anti-epidemic materials during an epidemic. Zhu [19] proposed a blockchain method for credibly recording infectious disease information, which greatly facilitates the credible traceability of infectious disease paths. Zhou [20] designed a witness model using blockchain smart contract technology to achieve a credible record of cloud service violations. Based on this, it is feasible to use blockchain technology for credible identification of blockchain illegal data, namely, identification on the chain.

The consensus in the on-chain identification model is usually realized by protocol voting and is managed and executed automatically by an algorithm. Dursun [21] proposed an on-chain identification governance model for the cumbersome blockchain identification governance model. The model utilizes policy-based management and decentralized identification technology to realize the identification and governance of the blockchain system. Although the model is simple and friendly, it cannot filter honest nodes, resulting in low credibility of the model. Bao [22] proposed a multi-supervised licensing blockchain model for the authenticity of blockchain transactions. The model supports identification and auditing, and its security and efficiency are proved by experiments. Although the model is safe and efficient, it is difficult to guarantee the credibility of nodes. Fan [23] proposed a multi-chain token support voting framework for MULTAV. The framework can enhance the security of on-chain identification through voting, but the node may make the opposite judgment because of the interests, resulting in the low credibility of the model. Although these models realize the identification and governance of the blockchain. However, on the one hand, because these models lack a method of selecting nodes, the credibility of nodes is low. On the other hand, these models lack an incentive mechanism, and nodes may make opposite identifications because of interests, resulting in low credibility of identification results. The two reasons will lead to a decrease in the credibility of the models.

3. Trust Model for Uploading Illegal Data Identification

This chapter will introduce the trust model and identification nodes. The overall model architecture for implementing identification using smart contracts is then explained, and the tasks of the identification blockchain and nodes are described.

3.1. Symbols Involved in The Trust Model

In the trust model for uploading illegal data identification, there are the following two kinds of blockchain: the identification blockchain to identify uploading illegal data (identification blockchain, IBC) and the identified blockchain (identified blockchain, IDBC) that will upload the data. The paper will use a basic case to demonstrate the work, as follows.

The paper assumes that an IDBC will upload a piece of data. Before data is uploaded to the blockchain, data needs to be identified. In order to prevent the data retransmission problem caused by the interruption of data transmission, IDBC will upload data to IPFS and send the returned hash to IBC. IBC broadcasts hash to each identification node (identification node, IN). IN downloads data through hash and identifies data. During identification, $T_{Identification}$, IBC will return a corresponding token based on the IN voting identification result. In addition, if the data is not illegal data, part of the identification fee will be reduced, F_{Reward}. That is, IDBC will eventually pay IBC $F_{Identification}$ or $F_{Identification} - F_{Reward}$.

There are the following two kinds of nodes in IBC: identification nodes and normal nodes (normal node, NN). Blockchain, as a trusted party, provides a platform for businesses or individuals who wish to govern the blockchain or earn revenue through identification services. They need to register as NNs before they can be selected as INs. INs earn revenue by providing identification services. In order to improve credibility, $Number$ INs form an identification committee to participate in the identification process, $\{IN_1, IN_2, IN_3, \ldots, IN_{Number}\}$. INs identify illegal data together and obtain identification fees from IDBC as a reward. Here it is assumed that the aims of INs are to gain the highest revenue, that is, INs are selfish.

3.2. Scheme Architecture

The trust model for uploading illegal data identification is shown in Figure 1. The trust model consists of the following two types of smart contracts: the smart contract of identification node pool (Smart Contract of Identification Node Pool, INPSC) and the smart contract of identification (Smart Contract of Identification, ISC). INPSC mainly has the following three responsibilities: NN registration, NN state transition, and IN selection. NN has the opportunity to be a member of INs only through the registration function and being "Online". In this trust model, the incentive mechanism of IBC is to provide credit and token incentives for INs. The more INs, the more reliable the model is and the higher the credibility.

The process of a trust model for uploading illegal data identification is shown in Figure 1. Firstly, IBC generates INPSC and ISC. Before identification begins, the IBC is required to negotiate identification treaties with the IDBC, including identification time $T_{Identification}$ and identification fees $F_{Identification}$. Among them, the most important thing between IBC and IDBC is to discuss the number of INs, $Number$. The more INs, the higher the credibility of the identification. At the same time, the increase in $Number$ will also lead to an increase in identification costs. According to the negotiation result, the IBC fills these parameters into the ISC. Then, through the reputation-based node random selection algorithm in Section 4.1 to select INs. These INs will form an identification committee. The algorithm is implemented by the INPSC on the IBC, and the ISC is responsible for calling the algorithm. The design of the algorithm is biased towards nodes with high reputation values and is random; thereby, improving the credibility of IBC identification and realizing mutual trust between IBC and IDBC. IDBC will send the hash value generated by the data information and token stored in IPFS to IBC. It should be noted that IBC will send a token to IDBC. IBC will broadcast the hash to all INs of the identification committee. Each IN downloads data information through this hash value. If illegal data information is identified, INs can immediately report the data information to the IBC.

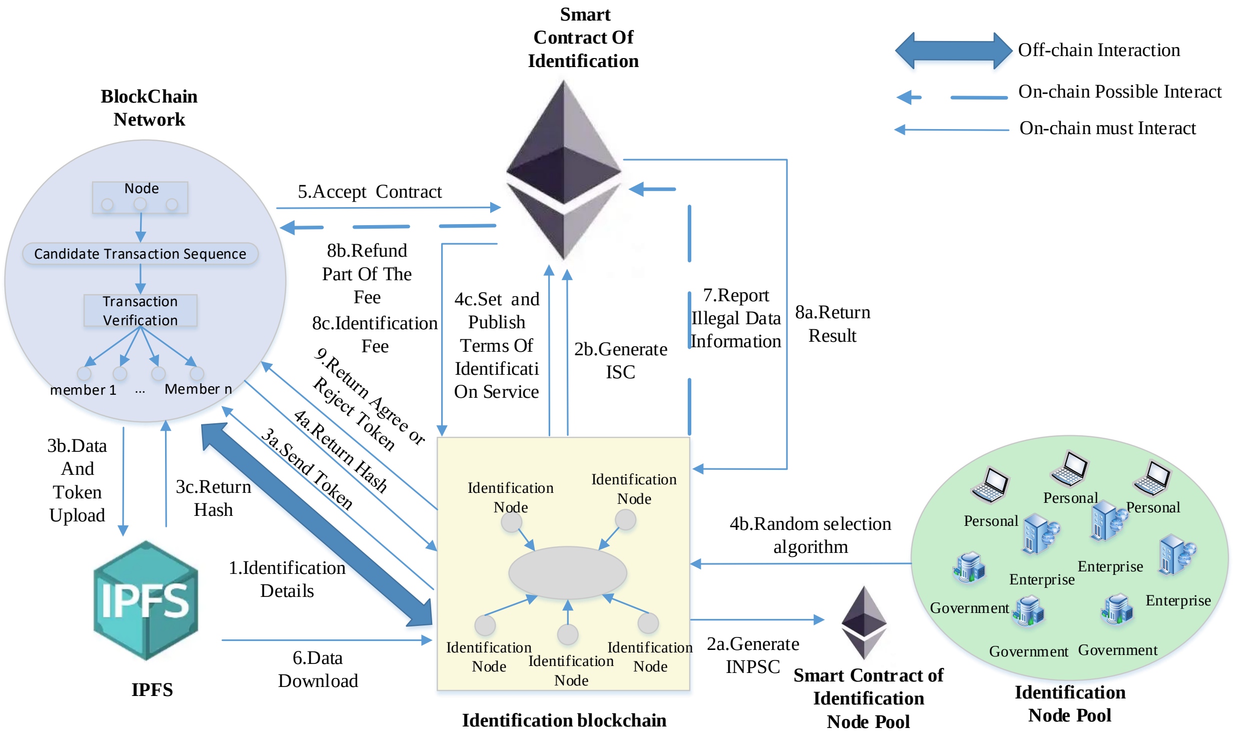


Figure 1. The overall architecture of the trust model.

ISC will start timing since the first IN report that the data is illegal, T_{Report}. During this time period, the ISC will accept reports from other INs. When the timer ends, if the ISC receives no less than $Illegal$ reports from the identification committee, the IBC will automatically confirm that the data information is illegal. Among them, $Illegal$ is also the result of negotiations between IBC and IDBC, and IBC will put $Illegal$ into ISC as an important parameter. It should be noted that $Illegal$ must be more than half of $Number$. The larger the $Illegal$, the identification result of the IBC will be more credible. For example, if there are $Number = 5$ identification nodes in the identification committee, at least $Illegal = 3$ reports are required, and IBC can confirm that the data information is illegal. It should be noted that ISC will only receive identification reports from committee members, and reports sent by non-committee nodes will be considered illegal reports and will be rejected. Meanwhile, INs cannot report multiple times within the same reporting period. In a sense, the $Number$ identification nodes constitute a $Number$ man game. In this game, each IN is eager to obtain the maximum benefit. This paper designs the incentive mechanism, as shown in Section 4.2, and uses the Nash equilibrium principle of game theory to prove why INs must be honest players in the game; that is, they must honestly report illegal data information.

Finally, the blockchain-based trust model for uploading illegal data identification will end in two cases. One case is that the identification time $T_{Identification}$ has ended, and the data information is not illegal. Another case is that the data information is illegal information. According to these different situations, IN and IDBC receive corresponding fees from the contract. Section 4.2 explains this in detail.

4. Key Technology

This section will describe in detail the key techniques in the trust model. The trust model realizes the identification of illegal data, and the identification result has high credibility. First, a reputation-based random selection algorithm is used to ensure that the majority of INs elected to the identification committee are credible and independent. On this basis, the incentive mechanism of INs is given. At the same time, through the principle of Nash equilibrium, it is proved that the INs in the identification committee must be reported honestly. Revenue can be maximized only when data information is identified fairly. Furthermore, the paper also analyzes a malicious identification node and shows that such behaviors can be avoided by the incentive mechanism.

4.1. The Detailed Design of RBRSA

In the blockchain-based trust model for uploading illegal data identification, it is very important to identify the data information from IDBC fairly and impartially; that is, IN cannot be biased towards IDBC. The paper proposes a reputation-based random selection algorithm for committee member selection, as shown in Algorithm 1. The algorithm in this paper is implemented in INPSC. Different from the selection algorithm of the paper [20], the selection algorithm is based on reputation, and the higher the reputation, the greater the probability of being selected. When the reputation value of NN is lower than 0, NN will no longer be selected as IN.

Algorithm 1 Reputation-Based Random Selection Algorithm()

```
Input: A set of Registered NN, NNAddrs, a list of addresses;
       Required number, Number, of members in a IN committee;
       The address of the IDBC;
       The address of the IBC;
Output: Selected Number IN to form a committee, INC;
assert (NNAddrs.length > 10*N) & assert (curBlockNum != 0);
Seed←0, Trust←0;
for i = 0; i<NNAddrs.length && NN.state = WState.online; i++ do
        Trust += NN.Trust;
end for
Hash =Hash(Trust, timestamp, height);
for node = 0; node < Number; node++ do
    Seed = Hash % Trust;
    reputation ← 0;
    for n = 0; n<NNAddrs.length && NN != IBC && NN != IDBC && NN.state ==WState.online; n++ do
        if InPool[NNAddrs[n]].state != WState.NNtoIN then
            reputation = reputation + NN.Trust;
            if Seed < reputation then
                NN.state = WState.NNtoIN;
                NN.confirmDeadline = now+ 5 minutes;
                NN.IdentificationContract = sender;
                onlineCounter–;
                Trust -= NN.Trust;
                INC←NN;
                Break;
            end if
        end if
    end for
    Hash = Hash(Seed, timestamp);
end for
return INC;
```

First, the trust model has a basic smart contract that manages normal nodes. INPSC provides a set of interfaces for any IBC node to join in the identification node pool. In addition, the state of the NN can be changed to “Online” or “Offline”, and only the NN that is “Online” can be selected as IN. The management of NNs state is introduced in Section 5.1. NNs in the identification node pool are managed in registration order.

INPSC is designed with two interfaces called by ISC to select *Number* INs in the identification node pool. The “Request” interface is mainly used to record some parameters necessary for selecting the algorithm. The "Sortition" interface is used to select $Number$ INs from NNs.

$$Seed = Hash(trust, block.timestamp, block.\ height) \quad (1)$$

$$Seed = Hash(Seed,\ block.timestamp) \quad (2)$$

RBRSA uses the hash value as the seed. The hash is consisting of the total reputation value in the node pool, timestamp and block height, as shown in the Formula (1). RBRSA selects NNs with high reputation value according to seeds but does not rule out selecting NNs with low reputation. In addition, every time a quasi-identification node is selected, a new seed is generated. The new seed is generated based on the previous seed and timestamp, as shown in Formula (2). Repeat this process until $Number$ quasi-identification nodes are selected. At the beginning of Algorithm 1, RBRSA will check whether the available NNs are enough. The number of NNs is much larger than INs to ensure the fairness and randomness of the algorithm output.

Considering the difficulty of using the hash value composed of the total reputation value in the node pool, timestamp, and block height as the seed and it is difficult for the outside world to know the total reputation value in the node pool. The paper can prove that the random selection algorithm based on reputation is credible. That is, IDBC cannot manipulate selection results to prevail in the identification committee.

4.2. Incentive Mechanism and Nash Equilibrium

Game theory is a mathematical theory and method to study the phenomenon of competition; it is a new branch of modern mathematics. Many scholars have made great contributions to the advancement of science and technology by combining game theory with other applications, including economics, evolutionary biology, and computer science [24]. The goal of game theory is to mathematically predict the behavior of a target. The behavior of these participants depends not only on themselves but also on the behavior of others.

One of the most common forms of game theory is the strategic form of multiplayer games. The definition consists of a set of actors (IN), a set of strategy profiles, and an incentive function. The INs constitute the basic type of dynamic game with complete information in game theory. The so-called complete information means that the incentive mechanism of each IN is known to others. The IN game is defined as follows:

Definition 1. *Identification game. This is a game of Number INs,* $(INC,\ ST,\ EX)$*.*

Where $INC = \{IN_1, IN_2, \ldots, IN_{Number}\}$ is a set with $Number$ INs. Each IN is selected through the reputation-based random selection algorithm, and these INs form an identification committee.

$ST = ST_1 \times ST_2 \times \ldots \times ST_{Number}$ is the action strategy configuration of a group of INs, where ST_h is a set of action strategies for identification node IN_h. IN_h can choose any action $AC_h \in ST_h$. Each IN may take different actions in each identification process, namely, $AC = \{AC_1, AC_2, \ldots, AC_{Number}\}$. $(h = 1, 2, \ldots, Number)$.

$EX = \{EX_1, EX_2, \ldots, EX_{Number}\}$ is a set of incentive functions. EX_h is the incentive function of identification node IN_h for specific action strategy AC_h. $EX_h = \{R_h, P_h\}$ where R_h and P_h represent reputation incentive and token incentive respectively.

In the identification process, the identification game roughly has two actions, reporting illegal data information to IBC and keeping silent, namely, $AC_h = \{AC_h^r,\ AC_h^s\}$. In the game process of $Number$ INs, the INs that report illegal data information are put into the reporting set INR, and the INs that do not report illegal data information are put into the silent set INS, where if $AC_h = AC_h^r$ then $IN_h \in INR$; If $AC_h = AC_h^s$ then $IN_h \in INS$. These operations determine whether the data information is illegal. Only when the number of elements in the INR is greater than $Illegal$ or equal to $Illegal$, the data information will be identified as illegal data. For details, refer to Definition 2. Otherwise, the IBC identifies it as normal data information. The identification is complete now.

Definition 2. *Confirmation of illegal data information.*

When $||INR|| >= Illegal$, where $1 < \frac{1}{2}Number < Illegal < Number$. That is, if there are no less than $Illegal$ INs reporting the data information, the IBC considers the data information illegal. Otherwise, IBC considers that the data information is normal.

Here $Number$ should be as large as possible, the larger the $Number$, the higher the credibility of the identification result. In addition, $Illegal < Number$ and $Illegal > 2$, in order to more fairly and credibly identify the data information. When INs identify, INs need to pay the corresponding deposit for each report to the IBC. If the data information is not identified as illegal data information, IN will not be able to recover the deposit and deduct the credit value. According to the above analysis, the detailed incentive mechanism design is shown in Definition 3.

Definition 3. *Incentive mechanism. Design the incentive mechanism according to the final identification result.*

When the identification result is that the data information is illegal as follows:

$$\forall IN_h \in INR,\ R_h(AC^r) = R_h + \mu \times (R_{MAX} - R_h) \times \frac{Correct}{Count},\ P_h(AC^r) = \frac{R_h}{R_{MAX}} \times SAL \tag{3}$$

$$\forall IN_h \in INS,\ R_h(AC^s) = R_h - \mu \times (R_h - R_{MIN}) \times \frac{Count - Correct}{Count},\ P_h(AC^s) = 0 \tag{4}$$

When the identification result is that the data information is normal as follows:

$$\forall IN_h \in INR,\ R_h(AC^r) = R_h - \mu \times (R_h - R_{MIN}) \times \frac{Count - Correct}{Count},\ P_h(AC^s) = -\frac{R_h}{R_{MAX}} \times SAL \tag{5}$$

$$\forall IN_h \in INS,\ R_h(AC^s) = R_h - \mu \times (R_{MAX} - R_h) \times \frac{Correct}{Count},\ P_h(AC^s) = \frac{R_h}{R_{MAX}} \times SAL \tag{6}$$

Equations (3) and (6) are the reputation and token reward formulas when the identification nodes successfully identify data. Equations (4) and (5) are the reputation and token penalty formulas when the identification nodes identify data incorrectly. Among them, μ is a reputation factor, which is responsible for controlling the increase and decrease speed of the reputation in different situations. μ is suggested [0.1, 0.3]. $Count$ is the times of participation and $Correct$ is the times of correct identification. It should be noted that the advantage of doing this is that INs with a high reputation can be prevented from doing evil. Because every time IN does evil, IN will reduce a large amount of reputation value, thereby reducing income. At the same time, incentive mechanisms can encourage nodes with low reputation value to identify data correctly. Because IN identifies data correctly each time, IN will gain more reputation value, thereby increasing income. According to game theory, if an IN knows what other INs will do in the future, IN will choose an action strategy that maximizes payoff based on the actions taken by other INs, which is called the optimal reaction. Therefore, the optimal reaction to IN defines is as follows.

Definition 4. *The optimal reaction of identification node IN_h.*

Let $AC_{-h} = \{AC_1,\ AC_2, \ldots,\ AC_{h-1},\ AC_{h+1}, \ldots, AC_{Number}\}$ is the set of other INs actions without IN_h. Then the optimal reaction action strategy for IN_h to other nodes is $\forall AC_h \in ST_h$, so that $EX_h(AC_h, AC_{-h}) \geq EX_h(AC_h, AC_{-h})$, so that IN_h obtains the maximum benefit.

The Nash equilibrium point can be regarded as a stable state between $Number$ identification nodes. In this state, no other action strategy will be chosen by any IN. At this point, each IN will take the best action strategy to obtain the maximum benefit.

Definition 5. *Nash equilibrium: This is a special IN action point* $AC = (AC_h,\ AC_{-h})$*. If every INs action* AC_h *is the action policy of optimal reaction to the action* AC_{-h} *of the other identification nodes. That is,* $\forall IN_h \in INC$ *and* $\forall AC_h \in ST_h$*, you can obtain* $EX_h(AC_h, AC_{-h}) \geq EX_h(AC_h, AC_{-h})$*.*

Based on the above definitions, the following theorems can be deduced:

Theorem 1. *In the node identification game, there are only two Nash equilibrium:*
$AC = (AC_1, AC_2, \ldots, AC_{Number})$, where $\forall IN_h \in INC,\ AC_h = AC_h^r$
$AC = (AC_1, AC_2, \ldots, AC_{Number})$, where $\forall IN_h \in INC,\ AC_h = AC_h^s$

Proof of Theorem 1. According to definitions 1 and 2, in a game with $Number$ INs, $Number \geq 3$, $\frac{Number}{2} < Illegal < Number$. where $Number$ and $Illegal$ are both integers. □

For the set of policy profiles $\forall IN_h \in INC, AC_h = AC_h^r$, this means $||INR|| = Number > Illegal$, so the data information is illegal. According to the incentive mechanism designed in Definition 3, $\forall IN_h,\ IN_h$ can obtain the benefit is $EX_h\left(AC_h^r, AC_{-h}\right) = (+,+)$. If an IN chooses silence instead of report. The final identification state of the data information will not be changed, because $||INR|| = Number - 1 \geq Illegal$, the income of the IN is $EX_h\left(AC_h^s, AC_{-h}\right) = (-,0) < EX_h\left(AC_h^r, AC_{-h}\right) = (+,+)$. By Definition 5, the policy configuration file is a Nash equilibrium point.

Similarly, for another set of policy configuration file $\forall IN_h \in INC,\ AC_h = AC_h^s$, this means that $||INS|| = Number > Number - Illegal \geq 2$. Therefore, the identification result of the data information is normal. By defining the incentive mechanism of 3, it can be known that $\forall IN_h, IN_h$ can obtain the benefit is $EX_h\left(AC_h^r, AC_{-h}\right) = (+,+)$. If an IN chooses another action strategy, that is reporting illegal data information, the identification result of the data information will not change. Because $||INS|| = Number - 1 > Number - Illegal - 1 \geq 2$. Then the income of the IN is $EX_h\left(AC_h^r, AC_{-h}\right) = (-,-) < EX_h\left(AC_h^s, AC_{-h}\right) = (+,+)$. By Definition 5, the action policy configuration is also a Nash equilibrium point.

Other action policies are a combination of actions, including reporting illegal data messages and silence. It means $||INR|| \neq \varnothing$ and $||INS|| \neq \varnothing$. There are two cases at this moment, the data information is illegal or normal. When the data information is illegal, $||INR|| \geq Illegal,\ \exists IN_h \in INS$, it can change the operation to report the data information. However, the identification result of this data does not change, because $||INR|| + 1 >$ Illegal, thereby increasing IN_h's income from $EX_h\left(AC_h^s, AC_{-h}\right) = (-,0)$ to $EX_h\left(AC_h^r, AC_{-h}\right) = (+,+)$. These examples show that the action policies of these INs are not the Nash equilibrium point.

Therefore, in the identification game between INs, there are only two Nash equilibrium points, namely, $AC = AC_1^r, AC_2^r, \ldots, AC_{Number}^r$ and $AC = AC_1^s, AC_2^s, \ldots, AC_{Number}^s$. Taking five identification nodes as an example, namely, $Number = 5$, according to Definition 2, $Illegal = Number/2 = 3$. Table 1 shows the incentive effects of different behaviors. The value elements in Table 1 are the vectors of the corresponding incentive mechanism, which can be expressed as $(EX_1, EX_2, EX_3, EX_4, EX_5)$. According to Theorem 1, the Nash equilibrium points of INs are $[(+,+),(+,+),(+,+),(+,+),(+,+)]$ and $[(+,+),(+,+),(+,+),(+,+),(+,+)]$.

It can be seen from the above analysis that for a rational IN who wants to obtain more benefits if the IN wants to maximize the benefits, with the least risk, the IN must perform the identification work as follows. If the data information is illegal, IN knows that most other nodes are more likely to report the data information to obtain more income. Therefore, the IN also reports that the data information is illegal. On the contrary, if the data information is normal, the node knows that other nodes will not report the data information to reduce losses because each IN has to pay a deposit for each report. It can be seen from this that when the data information is normal, all INs are more inclined to remain silent, thus achieving a Nash equilibrium that is $AC = (AC_1^r, AC_2^r, \ldots, AC_{Number}^r)$. Similarly, if the data information is illegal, the profit-seeking nature of INs will make them report the data information to reach another Nash equilibrium point, namely, $AC = (AC_1^s, AC_2^s, \ldots, AC_{Number}^s)$.

Table 1. Five-player game and incentive mechanism.

			$\boldsymbol{AC_4^r}$		$\boldsymbol{AC_4^s}$	
			$\boldsymbol{AC_5^r}$	$\boldsymbol{AC_5^s}$	$\boldsymbol{AC_5^r}$	$\boldsymbol{AC_5^s}$
AC_1^r	AC_2^r	AC_3^r	[(+,+),(+,+),(+,+),(+,+),(+,+)]	[(+,+),(+,+),(+,+),(+,+),(-,0)]	[(+,+),(+,+),(+,+),(-,0),(+,+)]	[(+,+),(+,+),(+,+),(-,0),(-,0)]
		AC_3^s	[(+,+),(+,+),(-,0),(+,+),(+,+)]	[(+,+),(+,+),(-,0),(+,+),(-,0)]	[(+,+),(+,+),(-,0),(-,0),(+,+)]	[(-,-),(-,-),(+,+),(+,+),(+,+)]
	AC_2^s	AC_3^r	[(+,+),(-,0),(+,+),(+,+),(+,+)]	[(+,+),(-,0),(+,+),(+,+),(-,0)]	[(+,+),(-,0),(+,+),(-,0),(+,+)]	[(-,-),(+,+),(-,-),(+,+),(+,+)]
		AC_3^s	[(+,+),(-,0),(-,0),(+,+),(+,+)]	[(-,-),(-,-),(+,+),(+,+),(+,+)]	[(-,-),(+,+),(+,+),(+,+),(-,-)]	[(-,-),(+,+),(+,+),(+,+),(+,+)]
AC_1^s	AC_2^r	AC_3^r	[(-,0),(+,+),(+,+),(+,+),(+,+)]	[(-,0),(+,+),(+,+),(+,+),(-,0)]	[(-,0),(+,+),(+,+),(-,0),(+,+)]	[(+,+),(-,-),(-,-),(+,+),(+,+)]
		AC_3^s	[(-,0),(+,+),(-,0),(+,+),(+,+)]	[(+,+),(-,-),(+,+),(-,-),(+,+)]	[(+,+),(-,-),(+,+),(+,+),(-,-)]	[(+,+),(-,-),(+,+),(+,+),(+,+)]
	AC_2^s	AC_3^r	[(-,0),(-,0),(+,+),(+,+),(+,+)]	[(+,+),(+,+),(-,-),(-,-),(+,+)]	[(+,+),(+,+),(-,-),(+,+),(-,-)]	[(+,+),(+,+),(-,-),(+,+),(+,+)]
		AC_3^s	[(+,+),(+,+),(+,+),(-,-),(-,-)]	[(+,+),(+,+),(+,+),(-,-),(+,+)]	[(+,+),(+,+),(+,+),(+,+),(-,-)]	[(+,+),(+,+),(+,+),(+,+),(+,+)]

It can be seen from the above analysis that in order to obtain maximum benefits, INs must choose to be honest nodes; that is, INs must identify the data information fairly and impartially.

4.3. The Analysis of the INs Uncertainty Behavior

Inspired by the uncertainty concept [25,26], this section intends to discuss and explain the uncertainty of IN behavior. Because INs are selfish and subjective, some INs may take different actions for their benefit. For example, IN knows that the data is illegal, but IN does not report it because of the benefit. The uncertainty of IN behavior will decrease the credibility of the model. Therefore, it is necessary to analyze the uncertainty of IN behavior.

- Malicious Behavior: Because nodes are selfish, some INs may engage in malicious behavior for their benefit. INs incorrectly identify data when facing benefits, leading to a decrease in the credibility of the model.

Anonymous mechanisms and voting consensus in the trust model can avoid this problem. First of all, each IN is anonymous. It is difficult for the outside world to know which NN is selected as an IN, so it is difficult for the outside world to make INs do malicious behavior through benefit. Secondly, the voting consensus of the trust model has a certain fault tolerance. The model allows some INs to identify data incorrectly. Finally, the incentive mechanism will punish the nodes who do malicious behavior. The income of malicious nodes changes from $EX_h\left(AC_h^r, AC_{-h}\right) = (+,+)$ to $EX_h\left(AC_h^s, AC_{-h}\right) = (-,0)$. The reputation value of malicious nodes decreases, which will also reduce the future benefits of nodes. Because the reward of the incentive mechanism is related to the reputation value.

- Credible Behavior: Because nodes are subjective, some INs still engage in credible behavior when facing benefits. The incentive mechanism in the trust model will reward the nodes that exhibit credible behaviors. The incentive mechanism will improve the reputation of nodes. Nodes with a high reputation will have a higher probability of participating in the identification service, so the nodes will obtain more income.
- Alliance Behavior: Some INs make the same wrong decision together, thus affecting the results of identification. The trust model has an anonymity and selection mechanism. On the one hand, anonymity can ensure that nodes cannot know the identity of other

nodes. On the other hand, the nodes selected by RBRSA are random, and the nodes cannot control the results of the selection. Therefore, the model can ensure that the INs are independent.

- Lazy Behavior: The behavior of INs does not actively work, because some INs are lazy when faced with these incentives. Regardless of whether the data information is illegal, INs do not report the data information to IBC. In this way, INs can obtain a low income.

The reputation value of the node can help the trust model better manage lazy behavior. When the data information is illegal, although the INs that fail to report the data information will not be punished by tokens, the reputation of INs will be deducted. INs who report the data information but whose final result is normal will not only be penalized tokens but also have decreased reputation value. In addition, when *Correct* remains unchanged but *Count* increases, the INs will increase less and less reputation value and will decrease more and more reputation value. At this time, the lazy node will obtain fewer and fewer incentives. When a node's reputation value is 0, the node will no longer be selected as IN. Additionally, the final incentive mechanism is also linked to the reputation value. In this way, the number of lazy IN will reduce. Each IN will be encouraged by the incentive mechanism to identify data information fairly and impartially.

5. Results and Discussion

According to the trust model for uploading illegal data identification and incentive mechanism design, we use Ethereum smart contracts to conduct related experiments. In the trust model for uploading illegal data identification, there are two types of smart contracts, including INPSC and ISC. In this part, we expound on these two kinds of contracts separately, describe the detailed functions of the interface in the smart contract, and show several states of IN. Afterward, we experimented with the transaction costs of these interfaces on the Ethereum test net.

The interfaces designed in both smart contracts are named as the text on the arrows in Figures 2 and 3, blue for ISC and yellow for INPSC. The format of the text is *role:interface*, which means that only the role or smart contract can call the interface. Smart contracts can implement specific functions for specific roles through inspection mechanisms, which is a feature of the programming language provided by Ethereum. Among them, IBC stands for the identification blockchain, and IDBC stands for the identified blockchain. IN stands for identification node, and ISC stands for the smart contract of identification. INPSC stands for the smart contract of an identification node pool.

5.1. Implementation of INPSC

This part will focus on the implementation details of the smart contract for the identification node pool, including the management of NN and the selection of IN. Figure 2 shows the four states of the node defined in the smart contract, namely, "Online", "Offline", "Quasi-IN" and "IN". The state transition mechanism of INs is as follows.

After a blockchain node is registered in INPSC, it will become a normal node in the identification node pool. NNs can choose between "Offline" or "Online" status. NNs in the "Offline" state do not participate in the selection algorithm. Only NNs in the "Online" state have the chance to be selected as "Quasi-IN" by RBRSA. At this time, NNs need to check their status on IBC at all times. Checking their status does not require any fee, which meets the requirements of NNs to frequently check their status anytime, anywhere. After the status becomes "Quasi-IN", there will be a timing window. If NN selects the "INconfirm" interface before the time ends, the status will become "IN". If the "Reject" interface is chosen, the random selection algorithm will be re-executed. After calling the interface "INconfirm" of the ISC, it represents the NN selects to become IN. Before the end of the data information identification process, IN has the right to choose "INrelease" to voluntarily withdraw from ISC. In addition, the IBC can also dissolve the identification committee through the "ResetIN" interface.

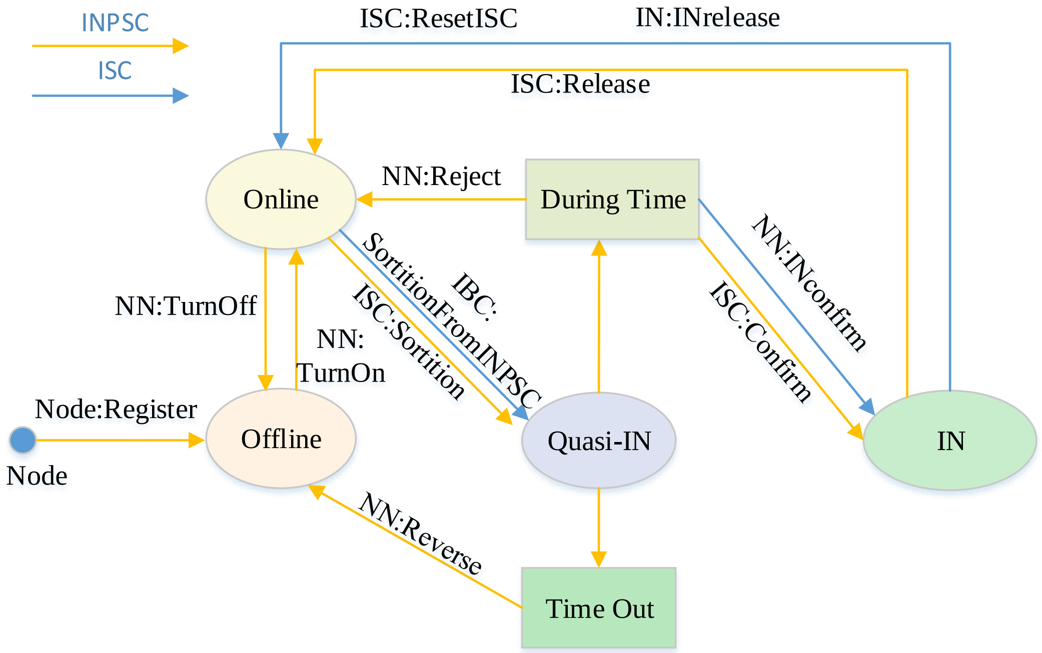


Figure 2. The transition of node states.

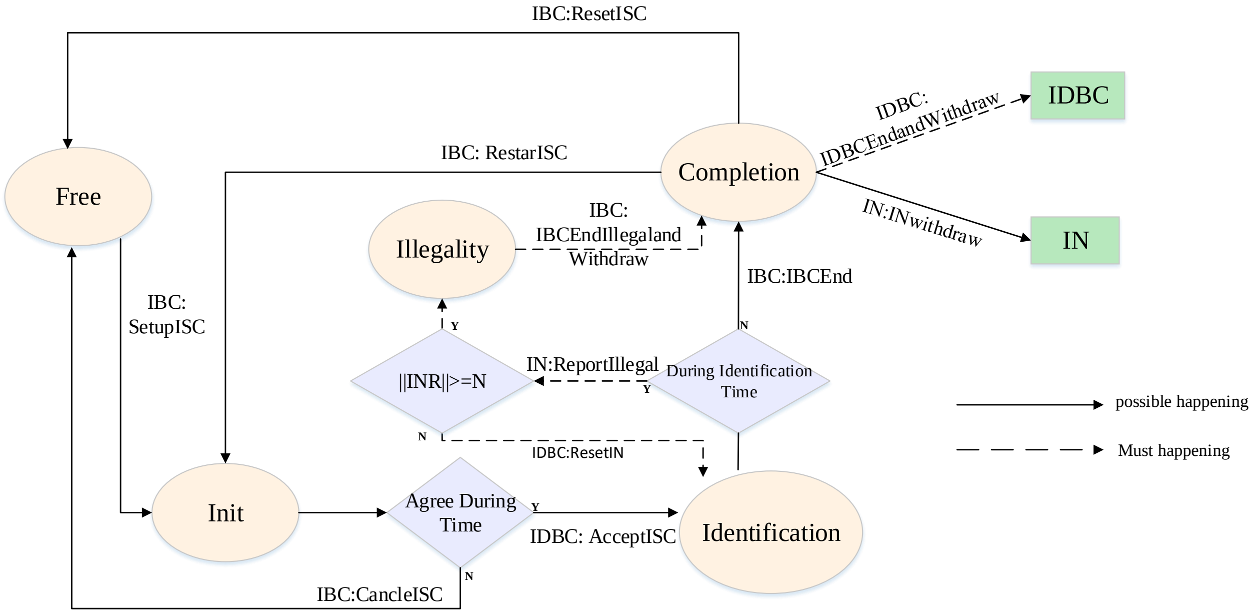


Figure 3. The transition of identification states.

To reduce malicious nodes, we set the reputation value attribute for NN to measure its behavior. Each node will be assigned an initial reputation value R_{init} when the node registers. It can be a predefined constant or a value depending on some interest relations. Here the initial value is set, $R_{init} = 50$. In addition, because some NNs do not check their status frequently when ISC selects them as candidate nodes, they cannot select and confirm to join the identification nodes within the specified time. At this point, their status changes to “Quasi-IN”. To return to the “Online” state, nodes need to use the “Reverse” interface.

5.2. Implementation of ISC

Figure 3 shows the state transition of the ISC identification result. There are the following five identification states: “Free”, “Init”, “Identification”, “Illegality”, and “Completion”. As shown by the circle in Figure 3. Arrows indicate the paths of state transition. The two squares in the figure represent the corresponding roles in the smart contract. At the end of the identification, they can withdraw the income separately.

Smart contracts on IBC cannot run on their own. State transitions must be initiated by some interfaces and need to pay the corresponding cost to run. We designed interfaces to modify the state of INs, which can be used when the state needs to be modified. For example, when the identification service ends normally, IBC can end the identification through the "IBCEnd" interface. At the same time, INs can obtain the identification fee through the incentive mechanism, and IDBC can be returned part of the fee as a reward. Similarly, when the data information is identified as illegal data information, it can end the identification through "IBCEndIllegalandWithdraw". At this time, the identification fee will be allocated to INs, and the identification state will also be converted from "Identification" to "Completion".

5.3. Trust Model Results and Analysis

In order to test the blockchain-based trust model for uploading illegal data identification, we conducted simulation experiments for smart contracts on "Rinkeby". We set up several accounts on "Rinkeby" to simulate different roles, namely, IDBC, IBC, and INs. We use the interface by "Ether" for each account and pay different fees according to the incentive mechanism. For experimentation, we first deployed the most basic INPSC and registered several accounts in the identification node pool. Then, IDBC sends the hash value returned by IPFS to IBC to start to identify the data information. After that, we test all possible scenarios to test and validate all interfaces. The results show that the trust model in this paper basically meets the identification needs.

The credibility of the trust model is proved by game theory and guaranteed by the reputation-based random selection algorithm and incentive mechanism. The credibility is supported by the technology of the blockchain itself. Therefore, we mainly analyze some performance information from experimental studies. Among them, performance refers to the complexity of each interface in the contract. It determines the fees that need to be paid by INs in IBC. Because INs need to execute certain programs defined in the method, the more complex the interface is, the higher the cost it needs to pay, that is, the higher the cost. This is measured by Ethereum's definition of "Gas". The identification fee is the product of "Gas" consumption and the price per unit. The cost is similar whether it is in the main network or in the simulation experiment. Therefore, we recorded all "Gas" consumption for each operation of the trust model.

Figure 4 shows the simulation results of the trust model. It can be seen that compared with IDBC and IN, IBC needs more cost consumption in the whole identification cycle, and IDBC and IN use less interface consumption. This is in line with the original intention of the model design. In most cases, IBC is the maker of tokens and has more tokens, and IBCs main purpose is to identify the illegal data that IDBC is about to upload to the chain. INs consume less "Gas" but obtain more "Gas". IDBC pays less "Gas", which is very small compared to the identification service fee paid. These cost expenditures can persuade INs and IDBCs to participate in the trust model. In addition, "Gas" consumptions are implemented based on smart contracts. It is possible to further optimize the complexity to reduce gas consumption.

5.4. Algorithm Results and Analysis

In the comparative experiments of random selection algorithms, different algorithms are applied in smart contracts, and the smart contracts are deployed on the Ethereum test network "Rinkeby". In this paper, five nodes are placed on the test network. These nodes are set to have the same or different reputation values. The experiments were carried out 20, 40, 60, 80, and 100 times. Experiments test the effects of different algorithms on selecting three nodes from five nodes. The experimental results are shown in Figures 5 and 6.

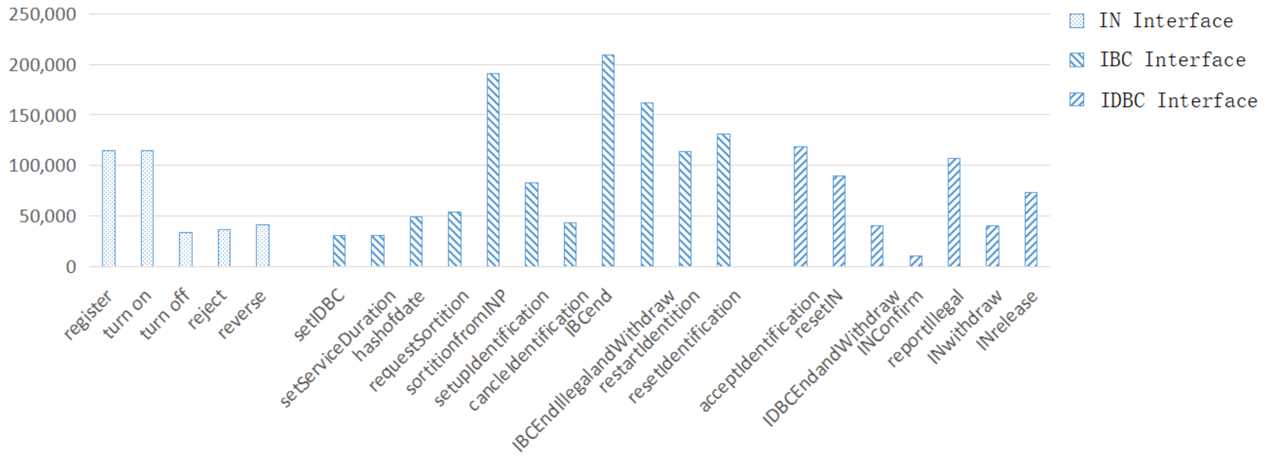
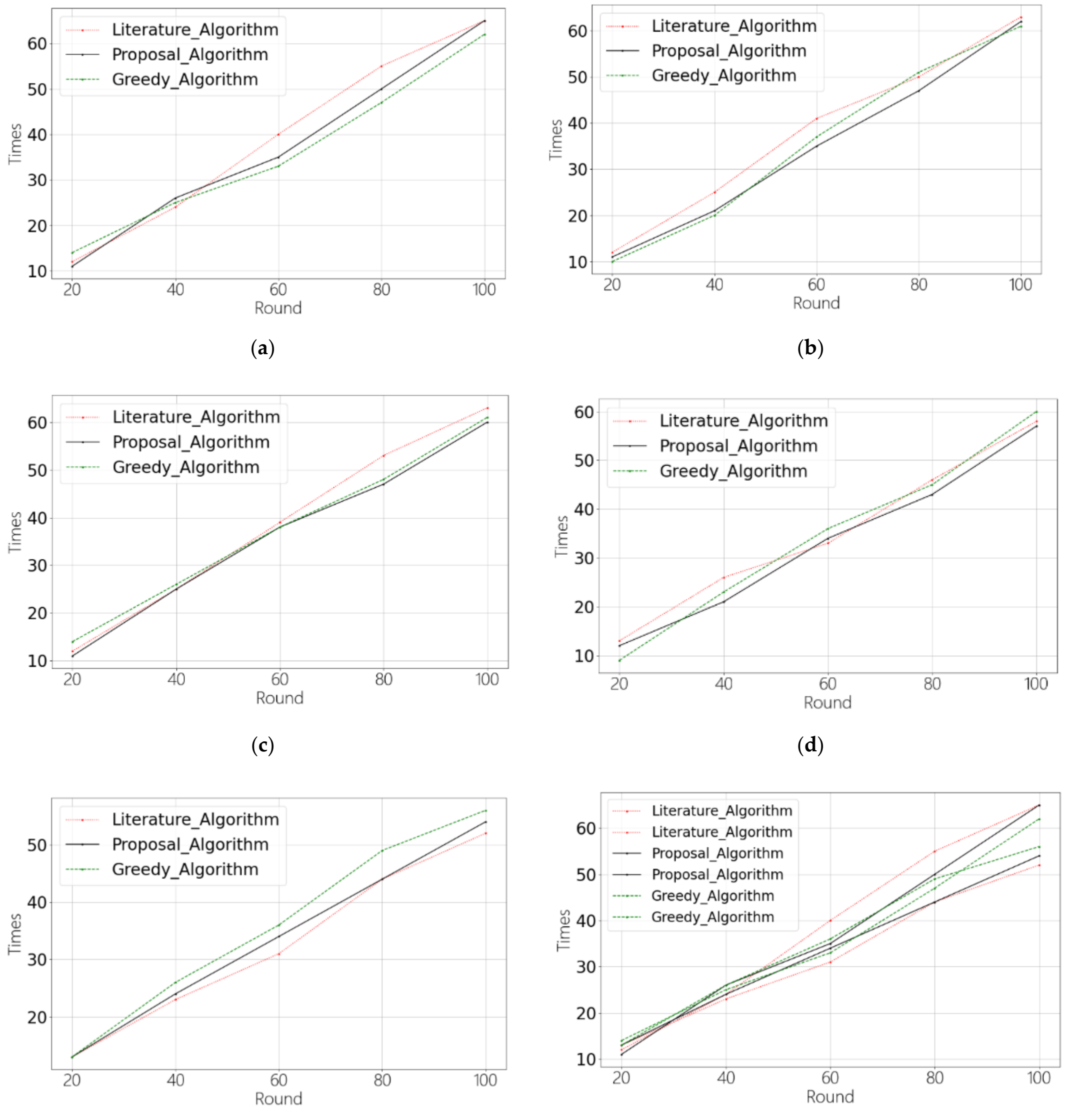


Figure 4. Gas consumption of each interface.



(**a**)

(**b**)

(**c**)

(**d**)

(**e**)

(**f**)

Figure 5. Comparison of algorithms under the same reputation values. (**a**) Node1; (**b**) Node2; (**c**) Node3; (**d**) Node4; (**e**) Node5; (**f**) comparison between the most selected nodes and the least selected nodes.

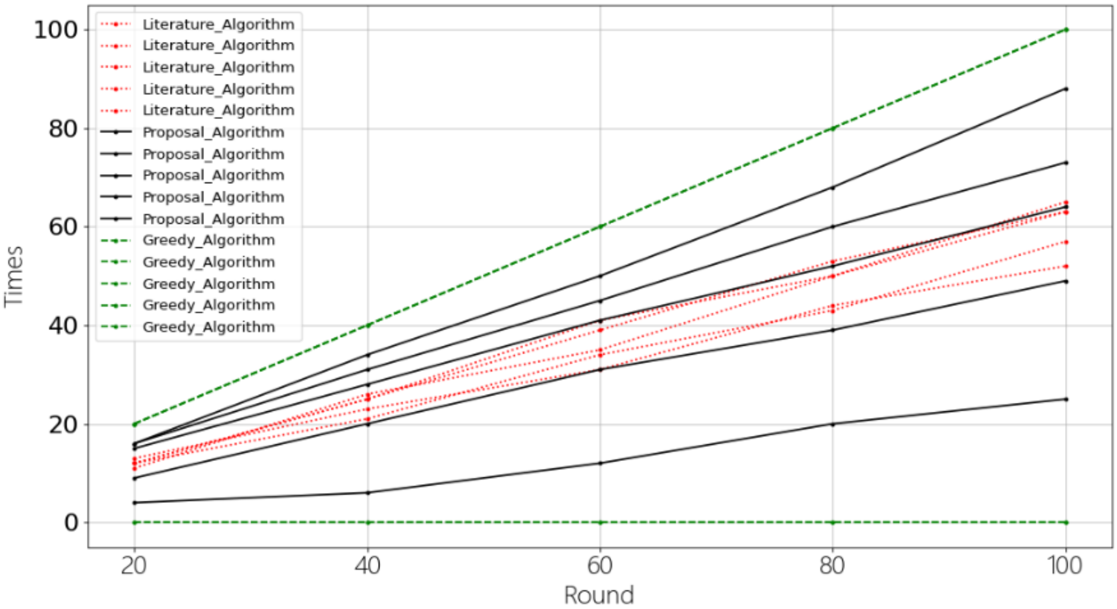


Figure 6. Comparison of algorithms under different reputation values.

Figures 5 and 6 show the comparison among the node selection algorithm proposed in this paper, the node selection algorithm in the paper [20], and the greedy algorithm. There are two cases when selecting three nodes out of five nodes. Figure 5 shows the number of times that five nodes are selected when the reputation values are the same. Figure 6 shows the number of times s that 5 nodes are selected when the reputation values are 100, 80, 60, 40, and 20. It can be seen from Figure 5 that in the case of nodes with the same reputation value, the number of times that NNs are selected as INs is roughly the same among the three algorithms. However, RBRSA is 23% and 13% higher than the algorithm [20] when the nodes have reputation values of 100 and 80. RBRSA is 11% and 27% lower than the algorithm [20] when the nodes have reputation values of 40 and 20. The number of times that the two algorithms select nodes with a reputation value of 60 is approximately the same, as shown in Figure 6. Although the greedy algorithm can select honest nodes and is better than the other two algorithms, in the face of different reputation values, the greedy algorithm will definitely select the nodes with the highest reputation value. On the one hand, nodes with low reputation value will no longer be selected, which lacks fairness. On the other hand, once nodes with high reputation values are united, the credibility of the identification model will be reduced. Therefore, compared with the other two algorithms, the nodes selected by RBRSA are more credible.

5.5. Incentive Mechanism Results and Analysis

In the experiment of the incentive mechanism, we assume that the nodes continuously correctly or incorrectly identify the data and show the effect of the incentive mechanism under different µ by controlling the parameter μ, as shown in Figures 7 and 8.

Figure 7 shows the effect of reputation increase when a node has correctly identified data 50 consecutive times. As can be seen from the figure, when the number of correct identifications increases, the reputation value also increases. However, the bigger the reputation value, the slower the reputation value increases. In addition, as the value of μ increases, the convergence of reputation value is faster. Figure 8 shows reputation decreases when a node incorrectly identifies data information 20 times in a row. As can be seen from the figure, as the number of incorrect identifications increases, the reputation value decreases. However, the lower the reputation value, the slower the reputation value decreases. In addition, as the value of μ increases, the convergence of reputation value is faster. Therefore, the incentive mechanism can reduce malicious nodes between high reputation value nodes because the incentive mechanism will make more penalties for high reputation value nodes; incentive mechanism can increase credible nodes in low reputation value nodes because the incentive mechanism will reward low reputation value more.

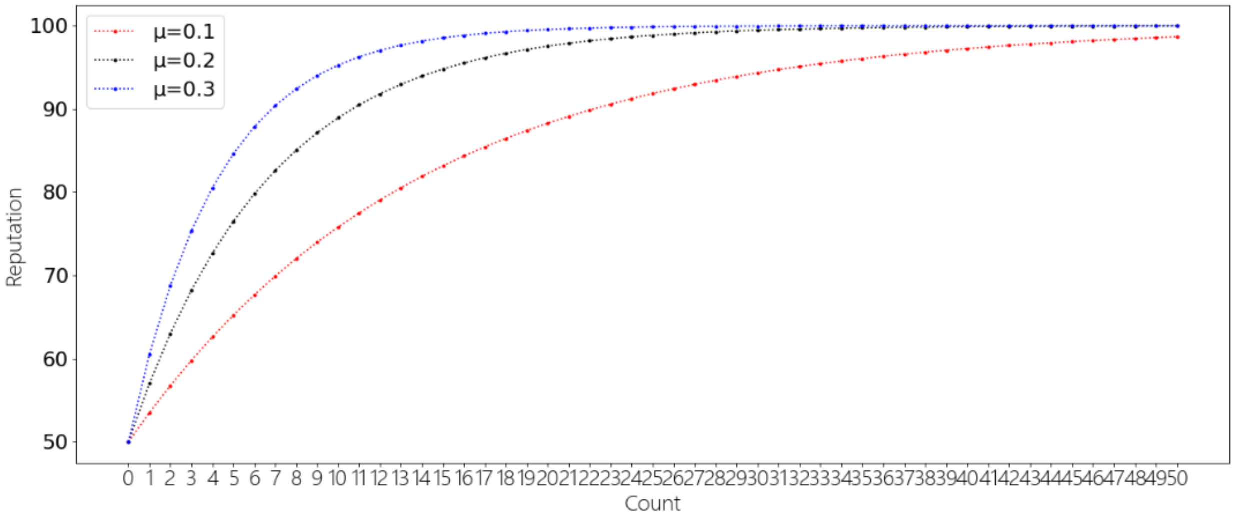


Figure 7. The increase in reputation under different μ.

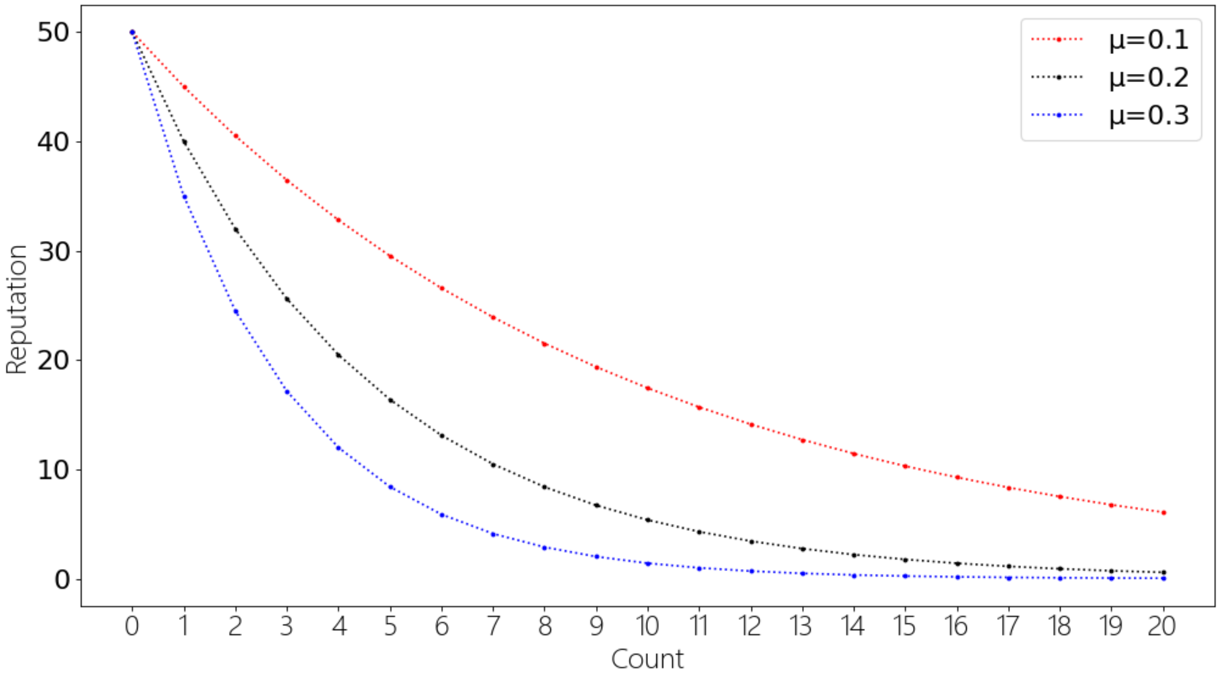


Figure 8. The decrease in reputation under different μ.

6. Conclusions

Aiming at the credibility problems of existing models, this paper proposes a blockchain-based trust model for uploading illegal data identification. Firstly, the paper proposes a trusted model for uploading illegal data identification. The trust model identifies the illegal data by means up decentralized voting. The model improves credibility through RBRA and incentive mechanisms. Secondly, the paper proposes a reputation-based random selection algorithm. The algorithm will bias toward the nodes with high reputation values, but it does not exclude the selection of nodes with low reputation values, so as to ensure the randomness and credibility of the identification nodes. Finally, the paper analyzes the model in terms of game theory and Nash equilibrium and proposes an incentive mechanism. Although nodes with high reputation value increase less in reputation value, they can obtain higher token income. The nodes with low reputation value can obtain more reputation value, but the income is less. We experimented with the model of the Ethereum smart contract. The results show that RBRSA can select credible nodes and that incentive mechanisms can encourage nodes to make credible identification. Therefore, the model in this paper is more credible than other models. Although RBRSA and the incentive mechanism improve the credibility of the model, a single reputation value cannot accurately describe the credibility of nodes, and the consensus efficiency among nodes is also low. Therefore, in future work, we will further study the attributes of nodes and consensus among nodes to improve the credibility and efficiency of the model.

Author Contributions: Conceptualization, J.C., Y.L., Y.Y. and X.X.; methodology, J.C., Y.L., B.Z. and X.X.; writing, Y.L., J.C., B.Z. and Y.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the Key Research and Development Program of Hainan Province (Grant Nos. ZDYF2021GXJS003, ZDYF2020040), Major science and technology project of Hainan Province (Grant No. ZDKJ2020012), National Natural Science Foundation of China (NSFC) (Grant Nos. 62162022, 62162024), Hainan Provincial Natural Science Foundation of China (Grant No. 620MS021).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ren, Y.; Guan, H.P.; Zhao, Q.X.; Yi, Z.X. Blockchain-Based Proof of Retrievability Scheme. *Secur. Commun. Netw.* **2022**, *2022*, 3186112. [CrossRef]
2. Mendi, A.F. Blockchain for Food Tracking. *Electronics* **2022**, *11*, 2491. [CrossRef]
3. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857. [CrossRef]
4. Lone, A.H.; Naaz, R. Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review. *Comput. Sci. Rev.* **2021**, *39*, 100360. [CrossRef]
5. Kumar, R.L.; Khan, F.; Kadry, S.; Rho, S. A Survey on blockchain for industrial Internet of Things. *Alex. Eng. J.* **2022**, *61*, 6001–6022. [CrossRef]
6. Guo, H.Q.; Yu, X.J. A Survey on Blockchain Technology and its security. *Blockchain Res. Appl.* **2022**, *3*, 100067. [CrossRef]
7. Wang, Y.; Gou, G.P.; Liu, C. Survey of security supervision on blockchain from the perspective of technology. *J. Inf. Secur. Appl.* **2021**, *60*, 102859. [CrossRef]
8. Spagnuolo, M.; Maggi, F.; Zanero, S. Bitiodine: Extracting intelligence from the bitcoin network. In *International Conference on Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 457–468.
9. Matzutt, R.; Hohlfeld, O.; Henze, M.; Rawiel, R.; Ziegeldorf, J.H. Poster: I don't want that content! on the risks of exploiting bitcoin's blockchain as a content store. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; Association for Computing Machinery, ACM: New York, NY, USA, 2016; pp. 1769–1771.
10. Matzutt, R.; Hiller, J.; Henze, M.; Ziegeldorf, J.H.; Mullmann, D.; Hohlfeld, D.; Wehrle, K. A quantitative analysis of the impact of arbitrary blockchain content on bitcoin. In *International Conference on Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 420–438.
11. Goldsmith, D.; Grauer, K.; Shmalo, Y. Analyzing hack subnetworks in the bitcoin transaction graph. *Appl. Netw. Sci.* **2020**, *5*, 1–20. [CrossRef]
12. Reijers, W.; Wuisman, I.; Mannan, M.; Filippi, P.D.; Raelooi, V.; Velez, A.C.; Orgad, L. Now the code runs itself: On-chain and off-chain governance of blockchain technologies. *Topoi* **2021**, *40*, 821–831. [CrossRef]
13. Bitcoin Improvement Proposals. 2021. Available online: https://github.com/bitcoin/bips (accessed on 13 March 2022).
14. Ethereum Improvement Proposals. 2021. Available online: https://eips.ethereum.org (accessed on 13 February 2022).
15. Subramanian, H. Decentralized blockchain-based electronic marketplaces. *Commun. ACM* **2017**, *61*, 78–84. [CrossRef]
16. Li, X.; Wu, L.; Zhao, R.; Lu, W.S.; Xue, F. Two-layer Adaptive Blockchain-based Supervision model for off-site modular housing production. *Comput. Ind.* **2021**, *128*, 103437. [CrossRef]

17. Yong, B.B.; Shen, J.; Liu, X.; Li, F.C.; Chen, H.M.; Zhou, Q.G. An intelligent blockchain-based system for safe vaccine supply and supervision. *Int. J. Inf. Manag.* **2020**, *52*, 102024. [CrossRef]
18. Omar, I.A.; Debe, M.; Jayaraman, R.; Salah, K.; Omar, M.; Arshad, J. Blockchain-based Supply Chain Traceability for COVID-19 personal protective equipment. *Comput. Ind. Eng.* **2022**, *167*, 107995. [CrossRef] [PubMed]
19. Zhu, P.; Hu, J.; Zhang, Y.; Li, X.T. Enhancing Traceability of Infectious Diseases: A Blockchain-Based Approach. *Inf. Process. Manag.* **2021**, *58*, 102570. [CrossRef] [PubMed]
20. Zhou, H.; Ouyang, X.; Ren, Z.J.; Su, J.S.; Laat, C.D.; Zhao, Z.M. A blockchain based witness model for trustworthy cloud service level agreement enforcement. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1567–1575.
21. Dursun, T.; Ustundag, B.B. A novel framework for policy based on-chain governance of blockchain networks. *Inf. Process. Manag.* **2021**, *58*, 102556. [CrossRef]
22. Bao, Z.S.; Wang, K.X.; Zhang, W.B. An Auditable and Secure Model for Permissioned Blockchain. In Proceedings of the 2019 International Electronics Communication Conference, Okinawa, Japan, 7–9 July 2019; ACM: New York, NY, USA, 2019.
23. Fan, X.X.; Chai, Q.; Zhong, Z. Multav: A multi-chain token backed voting framework for decentralized blockchain governance. In *International Conference on Blockchain*; Springer: Cham, Switzerland, 2020; pp. 33–47.
24. Liu, Y.; Yao, R.; Jia, S.; Wang, F.; Wang, R.; Ma, R.; Qi, L. A label noise filtering and label missing supplement framework based on game theory. *Digit. Commun. Netw.* 2022; *in press*. [CrossRef]
25. Mohamed, M.A.; Mirjalili, S.; Dampage, U.; Salmen, S.H.; Obaid, S.A.; Annuk, A. A Cost-Efficient-Based Cooperative Allocation of Mining Devices and Renewable Resources Enhancing Blockchain Architecture. *Sustainability* **2021**, *13*, 10382. [CrossRef]
26. Almalaq, A.; Albadran, S.; Mohamed, M.A. Deep Machine Learning Model-Based Cyber-Attacks Detection in Smart Power Systems. *Mathematics* **2022**, *10*, 2574. [CrossRef]