Scientific Research Publishing

Advances in Internet of Things, 2022, 12, 19-34
https://www.scirp.org/journal/ait
ISSN Online: 2161-6825
ISSN Print: 2161-6817

CrowdIoT: The Crowd-Sourcing Test System for IoT Devices Based on Blockchain

Yifan Lin*, Zhiji Li, Wenbo Yue, Jinghang Wen

Jinan University, Guangzhou, China
Email: *linyifan19970218@163.com

How to cite this paper: Lin, Y.F., Li, Z.J., Yue, W.B. and Wen, J.H. (2022) CrowdIoT: The Crowd-Sourcing Test System for IoT Devices Based on Blockchain. *Advances in Internet of Things*, **12**, 19-34.
https://doi.org/10.4236/ait.2022.122003

Received: January 19, 2022
Accepted: March 5, 2022
Published: March 8, 2022

Abstract

In view of some problems existing in traditional software crowdsourcing tests and Internet of Things device tests, we developed a CrowdIoT crowdsourcing test system for the Internet of Things devices based on a block chain. CrowdIoT uses the core technology of blockchain to focus its testing on physical devices on the Internet of Things. CrowdIoT uses two different testing methods for different testing needs: online testing and offline testing. Online remote testing is our key function and research object. By opening the testing interface of Internet of Things devices to testers, testers can test the devices in the CrowdIoT system interface without having to get the hardware. At the same time, CrowdIoT introduced multi-threaded parallel testing technology to solve the conflict problem of multiple testers competing for hardware resources in online testing. Offline testing, as a supplement to online testing, is to send Internet of Things devices to testers with high credibility in deposit guarantee, so that testers can fully test the hardware devices and dig out as many vulnerabilities of the devices as possible. CrowdIoT has its own complete and scientific credibility system, combined with relevant incentive mechanism, consensus mechanism and connection mechanism, which not only effectively solves the centralization problem existing in traditional crowdsourcing testing platforms, but also solves the pain point of the lack of remote testing of Internet of Things devices in the market. Then it solves the problems of equipment limitation and testing cost limits in the field of Internet of Things equipment testing, and provides a platform for security testing and use for the Internet of Things participants.

Keywords

Blockchain, IoT, Crowdsourcing, Blockchain Application

1. Introduction

In recent years, with the official commercialization of China's fifth-generation mobile communication technology, driven by both policy and market, China's IoT industry has entered a new round of innovation and development period, and the number of youth terminals has shown explosive growth. The number of youth terminals is exploding. The number of terminal devices with testing requirements is also increasing, and new devices must generate a large and complex testing requirement. However, the traditional IoT device testing environment has problems such as high testing cost, insufficient testing equipment and lack of qualified testers, which can easily lead to inadequate testing and thus bring great threats to IoT security. The increasing frequency of its endpoint security incidents also poses a huge challenge to this emerging industry. In order to solve the above problems, we innovatively combine IoT device testing with a blockchain crowdsourcing platform to create a blockchain technology-based IoT device crowdsourcing testing system—CrowdIoT.

Throughout recent years, the blockchain crowdsourcing platform is gradually emerging and the application of IoT on blockchain is developing rapidly, but there are few studies combining block chain, crowdsourcing testing and IoT, and the few studies are simple models. Therefore, the CrowdIoT designed in this paper provides a new design idea and solves the pain point problems brought by traditional testing, with the following contributions.

With CrowdIoT, IoT device manufacturers can safely and conveniently publish test tasks and hand them over to a considerable number of professional testers in the form of crowdsourcing. The problems exist in the platform. Credit provides a safe and reliable cooperation platform for both vendors and testers. By building CrowdIoT own credibility system, incentive mechanism and consensus mechanism, it solves the centralization problems of traditional crowdsourcing testing platforms. Through a scientific connection mechanism, it solves the pain points of remote testing of IoT devices on the market, which in turn solves the problems of equipment limitation and testing cost limits in the field of youth device testing.

Credit is committed to providing a secure testing and usage platform for youth participants. A safer and more reliable IoT ecosystem will allow more IoT devices to be fully and completely tested for security, allowing vendors and testers to achieve a win-win situation and ultimately promoting the sustainable and healthy development of the entire IoT industry. Throughout the field of IoT security testing, CrowdIoT is highly forward-looking and innovative.

In the other sections of this paper, the structure is as follows: Section 1 introduces the technical, theoretical foundation involved in credit; in Section 2 we introduce the current status of research related to blockchain technology in IoT and crowdsourcing mode and analyze its technical features; Section 3 describes the specific design details of the system scheme; Section 4 goes through the internship of the system model and conducts experimental testing and analysis on

it. The conclusion is described in Section 5.

2. Background of Technology

2.1. Crowdsourcing Strategy

Crowdsourcing, is both the outsourcing of tasks to non-specific, large mass networks on a voluntary basis. It requires the distribution of tasks down in the form of outsourcing, with multiple tasks and multiple users dovetailing, either one-to-one or one-to-many, resulting in a distributed logical relationship. With the increasing demand for testing work on its devices from its participants, coupled with the quarantine policy brought about by the recent epidemic has expanded the demand for online testing. The adoption of a crowdsourcing model to outsource testing tasks to users and thus increase the testing base has become the choice of most companies.

2.2. Blockchain

Due to the decentralized nature, the system needs to adopt a distributed system structure, and blockchain is a very popular technical means at present. Since Satoshi Nakamoto proposed the idea of Bitcoin, a distributed transaction system, and put it into practical application in 2008, the enthusiasm for research and application of its underlying technology, blockchain, began to rise. As shown in Figure 1, a blockchain can be understood as a distributed ledger, where a block contains two parts: a block header and a block body. 18 A block contains transaction data, a timestamp, and a cryptographic hash of the previous block. The legitimacy of each block is verified by the participants, while newly created blocks are broadcast to all nodes of the network, requiring a consensus of the majority of the network. Modifying the data in a block requires a very difficult task for all its subsequent blocks. Blockchain also has the advantages of good tamper resistance, irreversibility and decentralization in terms of security.

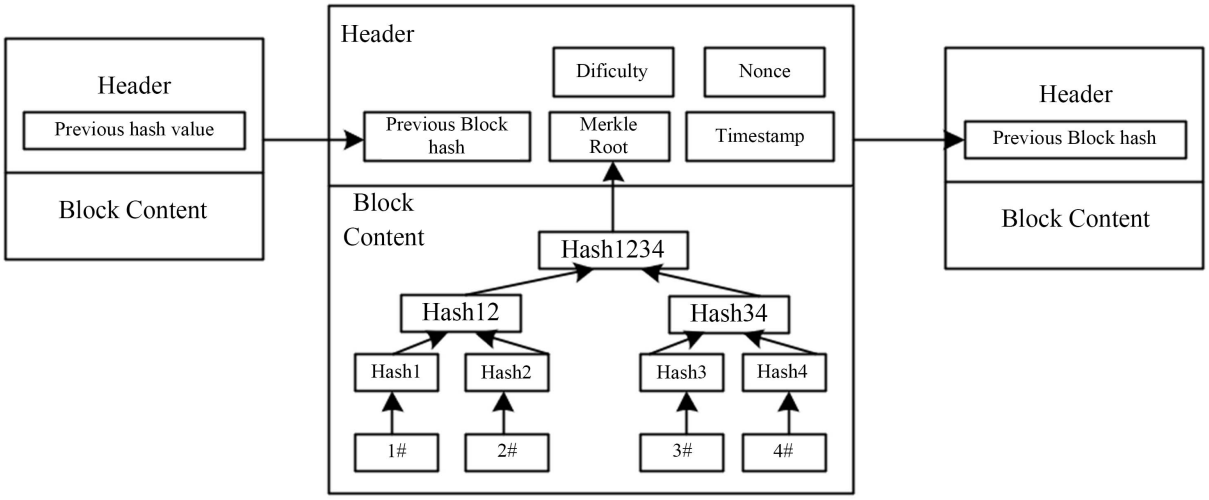

Figure 1. The structure of block.

2.3. Related Work

Currently, its systems in blockchain applications have been widely noticed. Both it and blockchain each have more mature systems, but the research and application of the integration of both are in the development stage. The crowdsourcing model is widely used in testing, but the combination with blockchain technology is relatively new. At the same time, its devices on the market have the demand for crowdsourcing testing. Crowdsourced testing systems require automated and decentralized control and management of large amounts of data from IoT devices.

K. Christidis and M. Devetsikiotis [1] provide an extensive description of the basics of blockchain and smart contracts and propose a solution for blockchain with an overview of its application and deployment. However, it does not delve into the characteristics of the ideal blockchain and its architecture or the possible optimizations to be made to create the system. In Aymen Boudguiga, *et al.* [2], a blockchain-based out update solution is proposed to build an infrastructure with better availability and accountability. Also, an evaluation of the system is proposed and they analyze the evaluation of the IoT system in some of its systems using block chain. In contrast to the previously mentioned, both M. Conoscenti [3] and J. Yli-Huumo [4] propose a holistic approach to blockchain for IoT scenarios, including not only the basics of blockchain-based IoT applications, but also a comprehensive analysis of the most relevant aspects related to its development, deployment and optimization. This work also aims to foresee the various potential contributions of blockchain in driving change in the IoT industry and in addressing today's challenges.

The upstream and downstream chain of data in blockchain has also been a key part of the research. For IoT security, Bo Wu *et al.* proposed RFL [5] and PPV [6], which can be used to ensure secure packet transmission between IoT devices. Yuan Tian *et al.* [7] proposed an IoT application security technique, called SmartAuth, with user-centric authorization, which ensures consistency between the functionality of its applications and actual authentication. However, these approaches rely on centralized permissions, where the security and capabilities of third parties can seriously affect the effectiveness of vulnerability detection. To avoid centralization and use blockchain technology for investigation, Jing Chen *et al.* [8] proposed a blockchain-driven, decentralized security audit scheme for TLS connections that relies on a consensus protocol based on distributed reliability levels to avoid centralization. Bo Wu *et al.* [9] also introduced a decentralized incentive mechanism for the traceability detection of it systems—Ahmed Kosba [10] proposed a blockchain-based framework that ensures privacy protection in smart contracts, which does not store financial transactions in plain text format on the block chain. Subdividing into IoT devices on the chain, S. Huh, S. Cho and S. Kim S. Huh, S. Cho and S. Kim [11] proposed to directly use the Ethereum to edit smart contracts directly on the chain, but there are cases where cryptographic storage requires the use of a third party. Hossein

Shafagh *et al.* [12] used virtual chains for this case in terms of storage H. Al-Breiki [13] also used a prophecy machine to complete the on-chain and off-chain process, providing a trusted source of data. In terms of practical case applications, Deng *et al.* [14] designed a food traceability system based on blockchain and RFID technology, and studied the combination of the Internet of things equipment and blockchain in the field of RF technology. A. Dorri [15] designed a lightweight blockchain-based smart home framework that uses high-resource devices to handle communication requests and a blockchain to control and audit the communication to ensure security. Although the concept of crowdsourcing is missing, this is a mature and complete its device-blockchain system and introduces the concept of decentralized management, which is of significant help to our study.

For the research on the application of crowdsourcing model on blockchain, Bo Wu *et al.* [16] elaborated the design of the incentive mechanism in the crowdsourcing testing process and proposed the SmartCrowd system and its operation process. Yang Zhen, Huang Song, Zheng Changyou, *et al.* [17] proposed a framework for blockchain-based crowdsourced testing of intellectual property and designed a model to be put into use, and the article contains unique analysis and insights on the up and down chains in the crowdsourcing model. In the article, Yu Li *et al.* [18] and others provide an overview of the use of blockchain in the crowdsourcing model, presenting the dangers that traditional centralized crowdsourcing platforms can encounter and giving a distributed solution to the problem.

3. Program Analysis

3.1. Architecture

Credit is a distributed system that can automate docking and has an incentive mechanism, and has the ability to test IoT devices online by multiple users in crowdsourcing mode. As shown in **Figure 2**, CrowdIoT services are provided to IoT vendors and crowdsourced testing users, both of whom form a close interaction with the system. The system provides online or offline service testing, and according to specific needs, IoT vendors will provide IoT device testing interfaces to the system. The vendor also needs to record the rewards into the block chain, and the block chain automatically issues the rewards after the user receives the task in the system and completes it. Through the block chain platform and smart contracts, the system can achieve the automation of the whole process and maintain the overall decentralization.

In this system, as a decentralized architecture system, it combines blockchain technology to provide task publishing, task query, and task receiving functions for task publishers and receivers. As shown in **Figure 3**, the design of this system is divided into a four-layer structure: application layer, blockchain layer, data storage layer, and IoT device layer. Each layer is structured as follows.

The application layer directly faces users and provides interfaces for their op-

erations, and contains three main parts: user information management, task management, and device connection. The user layer receives input information from users, and then transmits the input information to the block chain layer for processing.

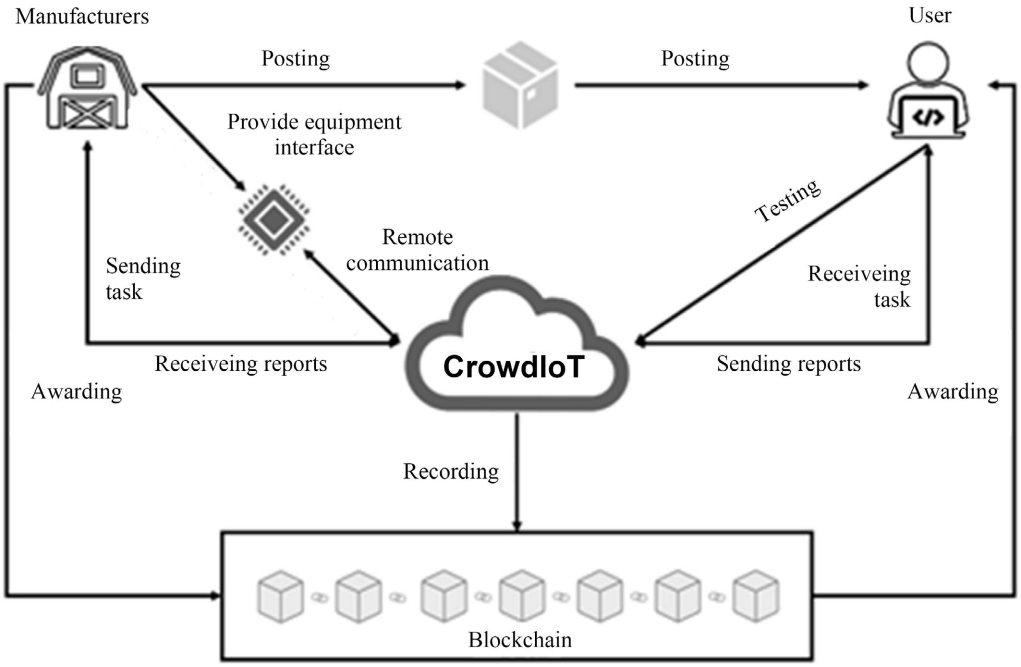

Figure 2. The overview of the system.

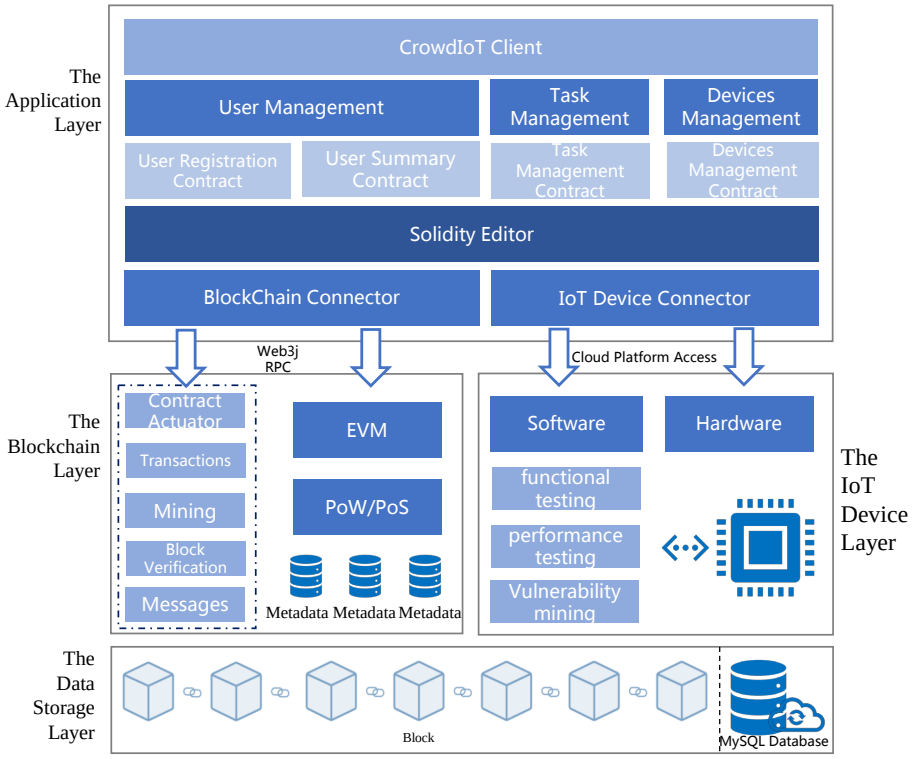

Figure 3. The general architecture of the system.

The blockchain layer uses Ethernet technology as the block chain distributed architecture. Compared with traditional crowdsourcing testing platforms, the advantages of this system are distributed crowdsourcing testing and a group, trusted collaboration mechanism in a distributed computing environment. In the block chain layer, we use Ethernet's smart contract as an implementation of consensus protocol, which can provide automatic protocol interaction based on smart contract for task publishers and receivers. Most of the business logic in the system, such as user registration, user management and task publishing, etc., are handled by smart contract. The system's smart contracts include: user registration contract, user aggregation contract, task management contract, and device management contract.

The data storage layer uses distributed cloud database to store large-capacity data such as test reports generated by users in the course of business processing, while for some blockchain metadata and key data generated by smart contracts, they are stored in the blocks of Ethernet. The combination of the two storage methods can effectively expand the storage capacity of the system and prevent key data from being tampered.

The IoT device layer is an intermediate layer between the youth devices and this system, which provides the corresponding interface for the system to test the devices and other operations. The system uses cloud platform access technology to provide key technical support for data interaction between hardware devices and the system. The tester does not need to care about the connection of hardware devices in the testing process, the IoT device layer has already provided the corresponding interface for the tester, the tester only needs to input the corresponding data to the interface according to his experience, and then generate the corresponding test report according to the feedback from the IoT device layer.

3.2. Device Parallelism Mechanism

Because of the crowdsourcing operation model, there are cases of multiple users testing the same device at the same time, which leads to such problems as access conflicts. For device security, the same port of the same device can only be invoked by one tester, and CrowdIoT designs a parallel mechanism to ensure the safe invocation of its devices in this system to avoid wasting resources. When a device is invoked by multiple users at the same time, the smart contract makes a judgment on which user will be tested first, satisfying the first-come-first-test principle for the first time and the reputation score priority principle for the second time. When the device is tested by a user, the smart contract will change the device state to occupied, and resources such as interfaces will be locked.

In Figure 4, for example, five users request to call the device at the same time for a period of time, and the contract will read the time and respective reputation score of each user's request. The contract will automatically determine the user with the highest priority to test first, *i.e.*, user #3, who is guaranteed to be the first in time and also has the highest reputation score. At this point, the re-

quest channel of other users will be closed, and the device interface will be locked after user #3 calls. We use a *k* value to represent the use of the device, after the device is invoked and used, the smart contract will give the device interface at the *k* value of 1, after which all requests to access the device will be denied. *m* value indicates how many users are waiting in line for the device, the larger the *m* the value the more people in line. When the *m* value is too large, the system will prompt and dissuade users to continue queuing for testing. As shown in Table 1, different *km* states represent different device states.

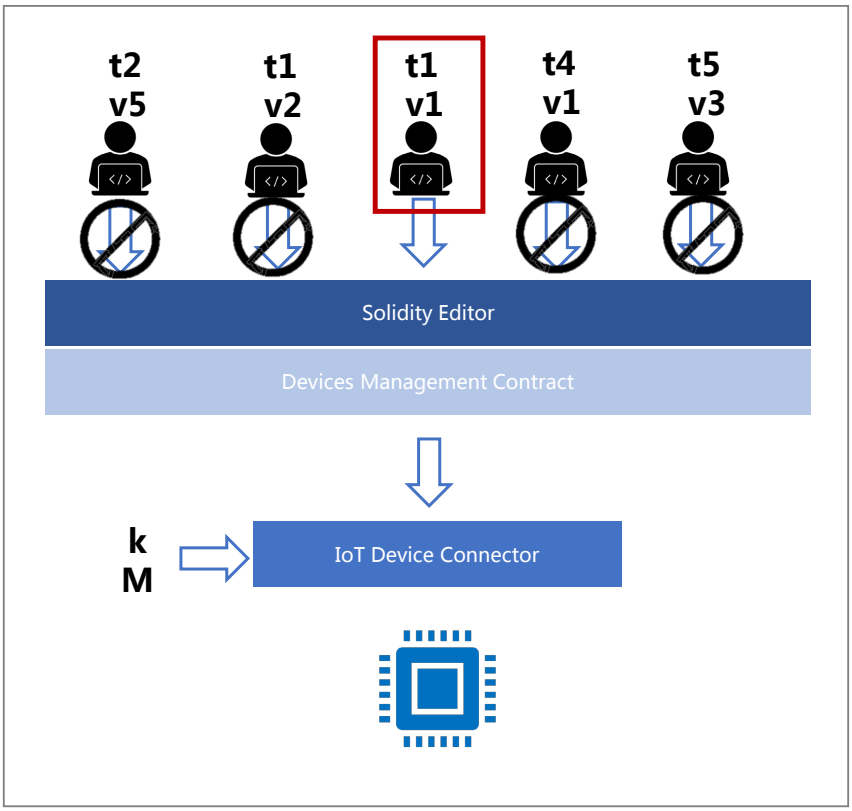

Figure 4. The schematic diagram of parallel mechanism.

Table 1. The status chart of *k* and *m*.

k	*m*	IOT device status	Next steps
1	-	Using	-
0	-	Device idle	Allow users to request a call
-	*n*	*n* users are queuing	Scheduling by priority
-	0	User has completed scheduling and there are no users in queue	Wait for release of *m* value
1	0	Device is in use and no users are queued	Open application
1	*n*	Device is in use and *n* users are queued users queued	Close system application channel when $n > 5$
0	0	Device is idle and no users are queued	Open application
0	*n*	The equipment is idle but cannot be used, resulting in queuing	The system reports errors to the administrator and closes the application channel

3.3. Incentive

In the design of the CrowdIoT incentive mechanism, a blockchain virtual currency transaction model is used. Since CrowdIoT uses Ether as the block chain platform, it uses Ether as the bonus of rewards. Through a smart contract, it is mandatory for vendors to pay a certain deposit as a subsequent bonus when posting tasks to the block chain. The deposit is also to prevent IoT vendors from maliciously releasing to cease attacks on the system. After the user completes the task and submits the test report, the system allows the IoT vendor to audit it, and the smart contract will only automatically release the bonus amount set by the IoT vendor beforehand into the user's account wallet after the audit is passed. Thus, CrowdIoT provides a fully decentralized incentive mechanism to automatically motivate its vendors and users who perform well.

3.4. Storage

As a result of the nature of blockchain, there are certain drawbacks in storage. The system adopts a set-dispersion hybrid storage method, combining IPFS distributed storage and centralized server-side storage, which plays a role in expanding capacity while being as decentralized as possible. Credit allows vendors and users to store hashes of task-related data in the block chain without having to put the data itself on the chain. That is, the specific data information is found in the off-chain IPFS based on the hash address of the task and report files on the block chain, completing the storage and fusion of information on and off the chain. The file hash address and file summary can be obtained according to user information and query conditions, which can enable users to query on-chain information. If CrowdIoT has enabled the caching mechanism, the results can be queried in the relevant cache without the next step of IPFS parsing. Not only can it save the computing pressure of the block chain, but it can also protect it effectively. However, CrowdIoT still uses a centralized server to store and manage the data generated by the system such as account information.

3.5. Workflow

The core of the overall system process is the youth participants, whose objects are mainly users and IoT vendors. As shown in **Figure 5**, the user first deploys the client program, after opening the page home page, if the user has not been registered, then refer to the user registration, management requirements for registration, and then the user to modify the information and create the corresponding publisher account and worker account. After successful registration, users can log in and enter the main menu interface. Task management mainly includes three parts: publish task, receive task, query task, submit reports and report audit. If you are a publisher, you can select the task publishing function, fill in the task information and publish it, and if you are a worker, you can operate on the receiving task interface, select the corresponding task and receive the acceptable tasks.

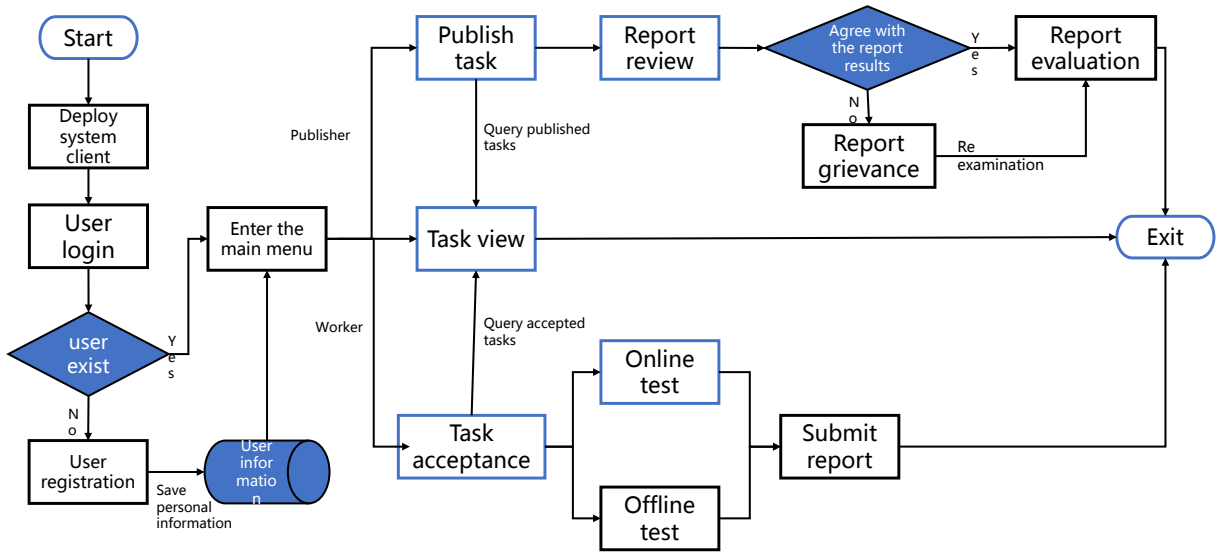

Figure 5. The system flowchart.

Secondly, after success, both publisher/workers can check the task information in the task query page. Again, after the test is completed, the worker uploads the test report in the report submission interface, and the publisher can receive the corresponding report in the report review interface and can review and rate it.

Finally, after the review is passed, it can be rated, and after the rating is completed, the corresponding reward and the withheld deposit or the reputation value will be returned to the worker's account; if the review is not passed, the publisher can apply for a second review, file a complaint, and leave it to the intelligent hardware to review the test report online and test the authenticity of the test report.

4. Model Implementation and Test Evaluation

4.1. Smart Contracts

Through smart contracts written in Solidity language, we can transfer the business logic and most of the data of CrowdIoT to the block chain without the need for a centralized management system, realizing the decentralization of the testing process and data. Credit utilizes the features of smart contracts such as non-tamper ability and electronic data commitment to transfer user management, task issuance, task reception, task evaluation, etc. are automatically executed and completed by means of smart contracts. If the customer and the worker disagree, the result can be determined by the smart contract. The user structure constructed in the smart contract is shown in Figure 6, which includes specific attributes such as user information and task reception situation.

4.2. Model Implementation

Credit is a project running environment under Windows 10, with a common

web browser on the client side, an Ethernet client geth1.9.12, an Ethernet wallet MetaMask 7.7.9 and a Mysql database 5.7.29, and a Java server Tomcat 8.5 on the server side. As shown in Figure 7, the system mainly implements functions such as user management, task management, online testing, report review and statistics management. The following is a brief description of the system.

1) Task list

As in Figure 8, system tasks will display task information based on the real time situation and can display the corresponding task list for different users. Each task has a limit on the number of people, and the limit will change after the user accepts the task.

2) Test online

As in Figure 9, users choose online remote testing; you need to click on the IoT device testing interface provided by the vendor in the task to enter the test page. After filling in the corresponding parameters according to the actual situation, the user can debug the device. The system will return the test results to the log and also display the data of the control results.

```
struct User{
    address payable addr;
    string username;
    bytes32 password;
    string profile;
    uint registerTime;
    uint processTaskNum;
    uint finishTaskNum;
    uint reputation;
    uint256[] postTaskList;
    uint256[] acceptTaskList;
}
```

Figure 6. The user structure of smart contract.

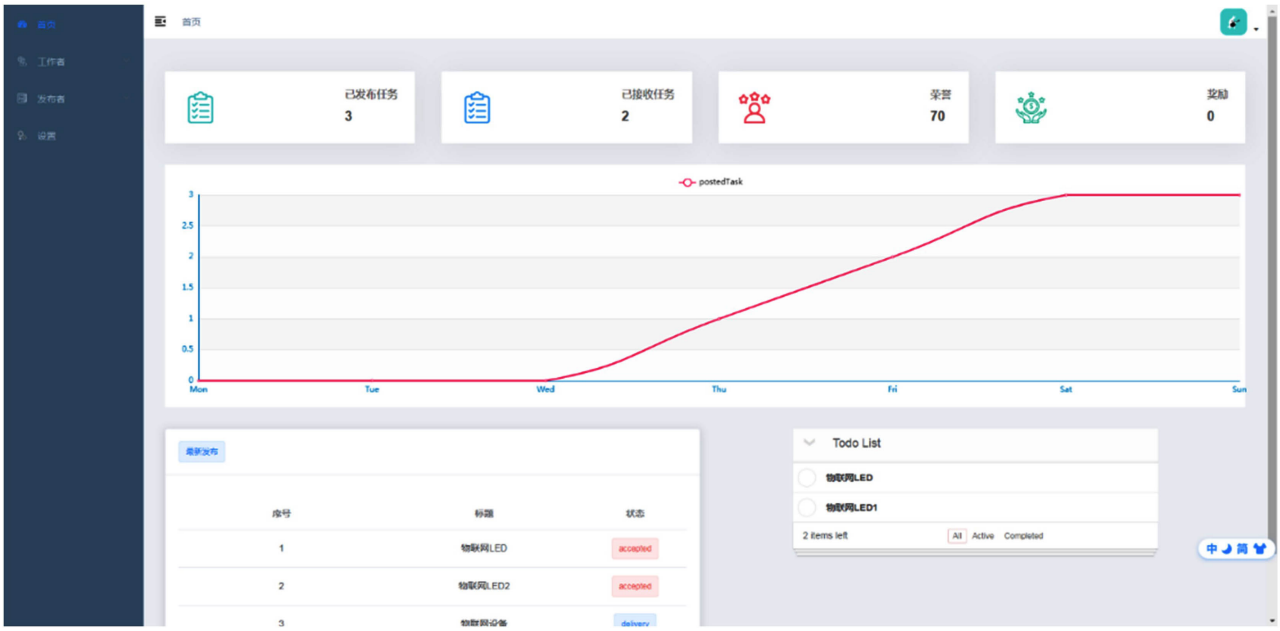

Figure 7. Screenshot of home page.

Figure 8. Screenshot of mission list.

Figure 9. Screenshot of test online.

3) Report audit

As in **Figure 10**, users need to upload the test report to the system after doing the task, and IoT vendors can find the report in their own task list and review it. The review process needs to give a rating, and the system will automatically issue a bonus to the user's wallet if the rating is qualified.

4.3. Experimental Evaluation

In the CrowdIoT system model, the basic operational performance of the system model is tested by switching multiple roles for multiple accesses, such as administrator, user, and vendor. The variables were controlled as much as possible and the system transactions were repeated five times to test the system. The CrowdIoT test model was tested to perform multiple transactions such as task reception, online testing, and report uploading excellently. As shown in **Table 2**, the Credit system model was tested for each transaction using the JMeter testing tool to record the response time. During the testing phase the system operated normally and the test cases passed with a 100% success rate. The fluctuation of the value is affected by the network condition and the data fluctuation is not significant, which proves that the system has a certain stability. Except for the uploading report, which takes more time, all other transactions can complete the response in less than 25 ms, and the system runs at a considerable speed and with certain smoothness.

Figure 11 also gives the throughput of the test system in the case of concurrent multi-transaction transactions with multiple users. The system throughput continues to rise to the number of transactions is 35, and after exceeding 35, the throughput decreases slightly and finally stays at around 30. The system stability

is quite good, but the peak throughput is small and cannot withstand the huge volume of transactions, which has a certain gap with the actual application requirements of the IoT system, and CrowdIoT still has much room for improvement.

Table 2. Time measurement of system transactions.

Number	Validate Logon	Accept Task	Dispatch Orders	Upload Report
1	15	10	20	350
2	10	15	25	367
3	9	12	15	390
4	10	13	19	388
5	9	14	20	379

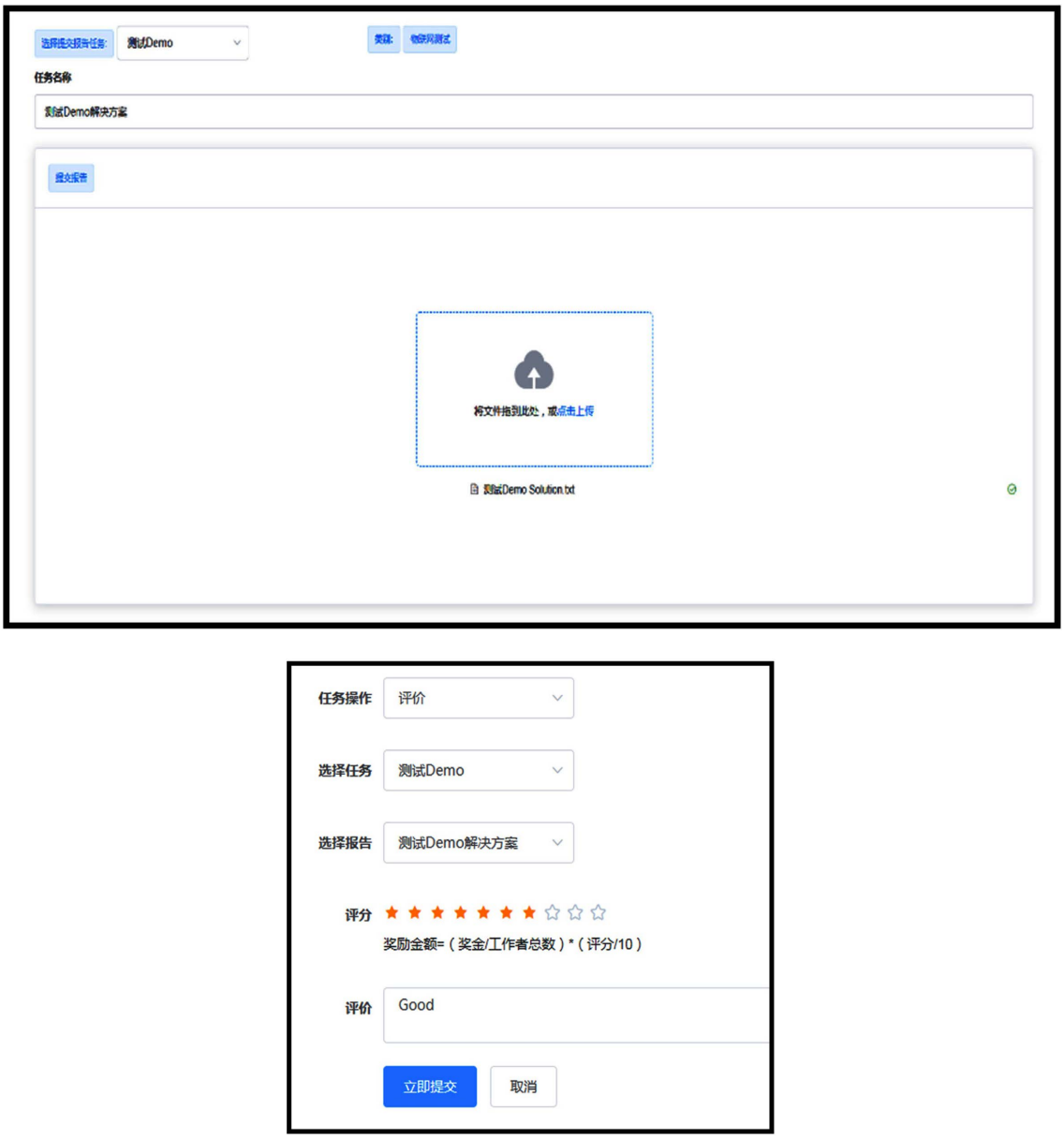

Figure 10. Screenshot of uploading and checking reports.

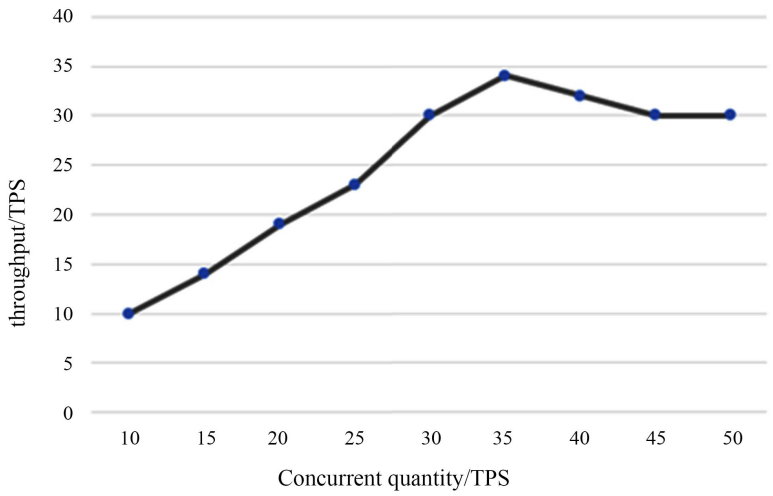

Figure 11. System throughput test results.

5. Conclusions

1) A blockchain-based crowdsourced testing system for its devices is established to achieve effective and secure management of users, tasks and test devices through smart contracts, and to significantly reduce the hidden risks brought by third parties, providing a solution for the application of IoT security construction.

2) For the working environment of blockchain and IoT devices, a parallel testing mechanism is proposed, using smart contract technology for efficient scheduling of users and devices. It ensures the security of IoT device interfaces while reducing unnecessary resource wastage. It solves the conflict problem of multiple users testing a single device.

3) The innovative combination of crowdsourcing testing model and blockchain technology is applied to the general environment of it. It simplifies the complex business process of crowdsourcing tests and increases security, thus making the testing process of its devices more systematic, planned and networked.

4) Combining the basic theory of blockchain with the actual IoT devices, the concept of online crowdsourcing testing is adopted, and CrowdIoT, a crowdsourcing testing system for its devices, is designed and developed to realize the interface between IoT device data and blockchain, which improves the completeness of crowdsourcing testing and also accelerates the pace of IoT security code verification.

Funding

National Natural Science Foundation of China (Grant No. 61932011), Guangdong Basic and Applied Basic Research Foundation (Grant No. 2019B1515120010), Guangdong KeyR&D Plan2020 (No. 2020B0101090002), National KeyR&D Plan2020 (No. 2020YFB1005600).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Christidis, K. and Devetsikiotis, M. (2016) Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, **4**, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

[2] Boudguiga, A., Bouzerna, N., Granboulan, L., Oliv-ereau, A., Quesnel, F., Roger, A. and Sirdey, R. (2017) Towards Better Availability and Accountability for Its Updates by Means of a Blockchain. *IEEE European Symposium on Security and Privacy Workshops*, 50-58. https://doi.org/10.1109/EuroSPW.2017.50

[3] Conoscenti, M., Vetrò, A. and De Martin, J.C. (2016) Blockchain for the Internet of Things: A Systematic Literature Review. *Proceedings IEEE/ACS 13th International Conference Computer Systems and Application* (*AICCSA*), Agadir, Morocco, 29 November-2 December 2016, 1-6. https://doi.org/10.1109/AICCSA.2016.7945805

[4] Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K. (2016) Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLoS ONE*, **11**, e0163477. https://doi.org/10.1371/journal.pone.0163477

[5] Wu, B., Xu, K., Li, Q. and Yang, F. (2017) Robust and Lightweight Fault Localization. *IEEE 36th International Performance Computing and Communications Conference* (*IPCCC*), San Diego, 10-12 December 2017, 1-8. https://doi.org/10.1109/PCCC.2017.8280428

[6] Wu, B., Xu, K., Li, Q., Liu, Z.T., Hu, Y.-C., Reed, M.J., Shen, M. and Yang, F. (2018) Enabling Efficient Source and Path Verification via Probabilistic Packet Marking. *IEEE/ACM 26th International Symposium on Quality of Service* (*IWQoS*), Banff, 4-6 June 2018, 1-10. https://doi.org/10.1109/IWQoS.2018.8624169

[7] Tian, Y., Zhang, N., Lin, Y.-H., Wang, X.F., Ur, B., Guo, X.Z. and Tague, P. (2017) Smartauth: User-Centered Authorization for the Internet of Things. *USENIX Security Symposium* (*USENIX Security*), Vancouver, 16-18 August 2017, 361-378.

[8] Chen, J., Yao, S.X., Yuan, Q., He, K., Ji, S.L. and Du, R.Y. (2018) Certchain: Public and Efficient Certificate Audit Based on Blockchain for TLS Connections. *IEEE Conference on Computer Communications* (*INFOCOM*), Honolulu, 15-19 April 2018, 2060-2068. https://doi.org/10.1109/INFOCOM.2018.8486344

[9] Wu, B., Li, Q., Xu, K., Li, R.Y. and Liu, Z.T. (2018) Smartretro: Blockchain-Based Incentives for Distributed IOT Retrospective Detection. *International Conference on Mobile Ad Hoc and Sensor Systems* (*MASS*), Chengdu, 9-12 October 2018, 308-316. https://doi.org/10.1109/MASS.2018.00053

[10] Kosba, A., Miller, A., Shi, E., Wen, Z.K. and Papamanthou, C. (2016) Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. *IEEE Symposium on Security and Privacy*, San Jose, 22-26 May 2016, 839-858. https://doi.org/10.1109/SP.2016.55

[11] Huh, S., Cho, S. and Kim, S. (2017) Managing IoT Devices Using Blockchain Platform. 2017 19*th International Conference on Advanced Communication Technology* (*ICACT*), PyeongChang, 16-19 February 2020, 464-467. https://doi.org/10.23919/ICACT.2017.7890132

[12] Shafagh, H., Burkhalter, L., Hithnawi, A. and Duquennoy, S. (2017) Towards Blockchain-Based Auditable Storage and Sharing of IoT Data. *Proceedings of the*

2017 *on Cloud Computing Security Workshop*, Dallas, 3 November 2017, 45-50. https://doi.org/10.1145/3140649.3140656

[13] Al-Breiki, H., Rehman, M.H.U., Salah, K. and Svetinovic, D. (2020) Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges. *IEEE Access*, **8**, 85675-85685. https://doi.org/10.1109/ACCESS.2020.2992698

[14] Deng, M. and Feng, P. (2020) A Food Traceability System Based on Blockchain and Radio Frequency Identification Technologies. *Journal of Computer and Communications*, **8**, 17-27. https://doi.org/10.4236/jcc.2020.89002

[15] Dorri, S., Kanhere, S., Jurdaak, R. and Gauravaram, P. (2017) Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. 2017 *IEEE International Conference on Pervasive Computing and Communications Workshops* (*PerCom Workshops*), Kona, 13-17 March 2017, 618-623. https://doi.org/10.1109/PERCOMW.2017.7917634

[16] Wu, B., Xu, K., Li, Q., *et al.* (2019) SmartCrowd: Decentralized and Automated Incentives for Distributed IoT System Detection. 2019 *IEEE* 39*th International Conference on Distributed Computing Systems* (*ICDCS*), Dallas, 7-10 July 2019, 1106-1116. https://doi.org/10.1109/ICDCS.2019.00113

[17] Yang, Z., Huang, S., Zheng, C. and Wang, T. (2021) Blockchain Based Crowdsourcing Testing Intellectual Property Trusted Management Framework. *Computer Applications and Software*, **38**, 27-32+99.

[18] Li, Y., Duan, H., Yin, Y. and Gao, H. (2021) Overview of Decentralized Crowdsourcing Technology Based on Blockchain. *Computer Science*, **48**, 12-27.