

# Intellectual Property Management and Legal Protection Mechanism of Blockchain-based Crowdsourced Testing

Cheng-Yong Liu<sup>1</sup>, Cheng Chen<sup>2\*</sup>

<sup>1</sup> College of Marine Culture and Law, Jimei University, China

<sup>2</sup> Law School, Fuzhou University, China  
cy.liu@jmu.edu.cn, chengchen\_cy@yeah.net

## Abstract

While promoting the vigorous development of crowdsourced testing services, Internet technology has also generated problems such as non-standard intellectual property management, unclear ownership of rights, and lack of trustworthiness. Based on the characteristics of being decentralized, traceable and tamper-proof of blockchain, IPFS, SHA256 algorithm, and digital certificate technology, this paper puts forward a new intellectual property management framework for crowdsourced testing to meet the requirements of intellectual property traceability of crowdsourced testing, right confirmation and query, and proposes the idea of applying on the chain and off chain decomposition and integration technology to address the storage performance bottleneck problem caused by data expansion on the chain, thus realizing a trusted intellectual property management system of crowdsourced testing. Meanwhile, this paper puts that the intellectual property of crowdsourced testing cannot be fully maintained only by technical means, and corresponding legal support means should be supplemented, including improving the laws and regulations on judicial and administrative protection of intellectual property, and properly handling the legal risk control of intellectual property of crowdsourced testing.

**Keywords:** Blockchain, Crowdsourced testing, Intellectual property management, Legal protection introduction

## 1 Introduction

With the rapid development of Internet technology, such as Internet of Things, cloud platform and communication technology [1-3], crowdsourced testing technology has been increasingly widely used. "Crowdsourcing" is a new distributed problem-solving model based on the combination of human and machine computing, involving such subjects as the employer, the crowdsourced testing platform, and the contractor. [4] The so-called "crowdsourced testing" refers to applying crowdsourcing technology to the software testing field, which is a new software testing method derived from the new generation of Internet technology. Based on new transmission technology [5], it has changed the traditional testing service model, and organized production in a

distributed and collaborative way based on the characteristics of the sharing economy, and collaborated with testing requirements and testing resources, thereby aggregating to form economies of scale. [6] The specific process of crowdsourced testing is shown in Figure 1.

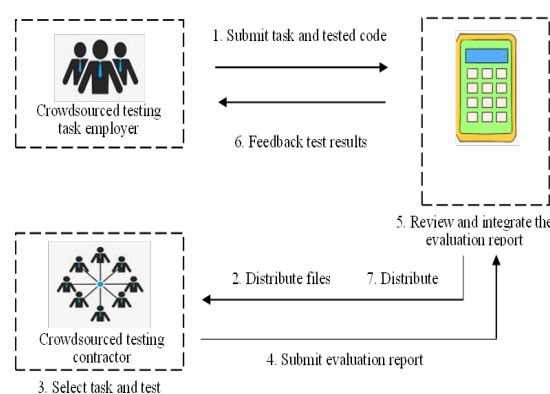


Figure 1. Process of crowd sourced testing

Traditional crowdsourced testing generally adopts the mode of integrating "manual operation" and "central organization management", which, however, poses a major threat to security and intellectual property. Feng et al. held that the current crowdsourcing lacks the protection of data security and privacy and has a risk of data disclosure, thus greatly limiting the availability of crowdsourced testing. [7] Wan believed that the intellectual property problems of crowdsourcing platforms mainly result from crowdsourcing platform management, intellectual trading characteristics, and the intellectual property environment of crowdsourcing platforms. [8] Li et al. established an intellectual property risk evaluation model for the crowdsourcing platform and analyzed the current intellectual property dilemma faced by China's crowdsourcing model from multiple perspectives. [9] According to the above research, in the field of crowdsourced testing, the testing tasks, tested code and the evaluation report of the contractor of the crowdsourced task all involve the level of intellectual property. However, because of the openness of the crowdsourcing platform, any user can freely obtain the testing tasks and tested code through the Internet access platform, leading to a serious risk of intellectual property disclosure. In addition, the crowdsourced testing

platform usually uses a centralized database to store workers' evaluation reports. Due to trust problems resulting from the easy falsification of the reports, this method cannot identify the source of intellectual property and may easily lead to property rights disputes. Therefore, in the current crowdsourced testing industry, it is important to adopt a new crowdsourced testing mode to protect the security and privacy of tasks and codes, the tamper resistance of the crowdsourced testing report, and the clarification of the ownership of rights.

In view of the above problems, studies have been conducted on intellectual property protection technologies in different scenarios at home and abroad, mainly focusing on digital watermarking [10], encryption [11] and digital rights management system [12]. Huang and others proposed a digital intellectual property protection scheme based on algorithms such as attribute-based encryption to protect digital content and user privacy. [13] Chen et al. designed a copyright management scheme by combining blockchain with digital watermarking, interstellar file system (IPFS) and other technologies, but this scheme is only applicable to the copyright management of digital images. [14] Burstall and others pointed out that blockchain can be used to register and cancel intellectual property, control and track its distribution in intellectual property intensive industries. [15] However, there is no special research on the management and protection of intellectual property issues in the field of crowdsourced testing, such as the evaluation report submitted by the crowdsourced testing contractor, the testing code, and the report on the results of crowdsourced testing issued by the crowdsourced testing platform. Especially for the open characteristics of the crowdsourced testing platform, it is currently necessary to explore a management framework that conforms to the characteristics of crowdsourced testing intellectual property and the corresponding legal protection mechanism. To this end, based on such characteristics of blockchain as decentralization, traceability, and tamper resistance, as well as IPFS, SHA256 algorithm, and digital signature technology, this paper proposes a new intellectual property management framework for blockchain-based crowdsourced testing, and legal support mechanism to assist the successful implementation of the management system.

## 2 Existing Problems and Technical Background

Despite the booming prospects of China's current crowdsourced testing, there has been a frequent occurrence of infringement of intellectual property. It is obvious that the traditional intellectual property management model and legal protection cannot meet the needs of the current crowdsourced testing industry, requiring the urgency to make breakthroughs.

### 2.1 Intellectual Property Dilemma of Crowdsourced Testing

Based on the open Internet, the crowdsourcing model relies on third-party platforms to release projects, and completes tasks by gathering public knowledge, skills

and creativity. In order to obtain technical support more effectively, the employer needs to publish the creative scheme, business plan and important data of technical parameters on the platform. On the other hand, owing to the online openness and object-oriented popularity of the platform, it is difficult to completely eliminate the risk of "collective wisdom" being usurped due to interests, thus leading to frequent plagiarism in the crowdsourced field, which will inevitably reduce innovation momentum and hinder the development of crowdsourcing model. Concerning crowdsourced testing, the intellectual property dilemma it faces is as follows.

First of all, in the dynamic service process of crowdsourced testing, after the intellectual property of crowdsourced testing (such as the evaluation report provided by the contractor) is submitted to the crowdsourcing platform, there should be a series of processing before it is delivered to the employer. Since the process is not transparent, intellectual property cannot be traced and confirmed, and the authenticity and reliability of the data cannot be ensured. If the intellectual property data is tampered with by malicious users, or the data is changed due to the error of the staff of the crowdsourced testing platform, the data will not be traced.

Secondly, in the software testing stage and the awarding stage, the testing code of the crowdsourced testing contractor is easy to be plagiarized, and a copy of the testing code may be plagiarized and submitted repeatedly, thus receiving multiple awards. In case of economic dispute, the source of the testing code of the contractor cannot be confirmed because the testing code has not been stored, and the problem cannot be properly solved. The above status quo infringes the intellectual property of the crowdsourced testing contractor, damages the economic interests of the crowdsourced testing employer and the crowdsourced testing platform, hindering the development of crowdsourced testing. Therefore, it is urgently imperative to build a credible intellectual property management mechanism for crowdsourced testing.

### 2.2 Blockchain Technology Concept

Blockchain is essentially a recorded distributed database, or a distributed ledger technology for all transactions or digital events that have been executed and shared among participants. The characteristics of blockchain technology are tamper-proof, counterfeit-proof, and traceability; Blockchain records all transaction information, with efficient and transparent process and highly secure data; Blockchain technology can be applied to all application fields that need justice, fairness and honesty. [16]

The application of blockchain technology can effectively meet the requirements of crowdsourced testing intellectual property management: (1) The blockchain can not only record the ownership information of the crowdsourced intellectual property, but also record the time when each intellectual property was put on the chain by stamping a timestamp, which cannot be tampered with and help the crowdsourcing platform effectively trace the source of intellectual property. (2) By adopting data encryption technology and digital certificate technology, the blockchain can ensure that irrelevant people cannot know the content of the accessed data. (3) Smart contracts can be used to

execute the automatic process of authorization without the participation of intermediaries. Consensus algorithms are used to ensure the consistency of data at each node. After the application, intellectual property is automatically incorporated into the system and ownership is obtained [17]. The above three aspects jointly ensure that under blockchain management, the ownership of the crowdsourced testing intellectual property can be confirmed for the first time, and the intellectual property can also be safeguarded.

### 2.3 Insufficient Legal Safeguards for Intellectual Property Protection of Crowdsourced Testing

China's intellectual property protection relies too passively on administrative and judicial forces and has always relied only on the government and judicial authorities to safeguard their rights. However, the current legal norms cannot meet the intellectual property management needs of crowdsourced testing. China's intellectual property law system is composed of the Patent Law of the People's Republic of China, the Trademark Law of the People's Republic of China, the Copyright Law of the People's Republic of China, and the Regulation on Computers Software Protection. Although this legal system is also applicable to Internet enterprises, it cannot meet the actual needs because it fails to take into account the particularity and new development of the Internet, still requiring the supplement of the rules formulated by the industry itself; The intellectual property protection of crowdsourced testing is a typical example. For example, the crowdsourcing platform ZBJ.COM has established an integrity committee to formulate the ZBJ.COM Service Rules to regulate the industry's service behavior. At present, the intellectual property protection measures of crowdsourced testing standardized by the platform operators themselves have been confronted with the problem of running their own affairs, lacking authority, and difficulty of forming a systematic mechanism, resulting in insufficient legal means to safeguard intellectual property. Hence, it is urgent to resolve this problem.

## 3 Intellectual Property Management Framework for Blockchain-Based Crowdsourced Testing

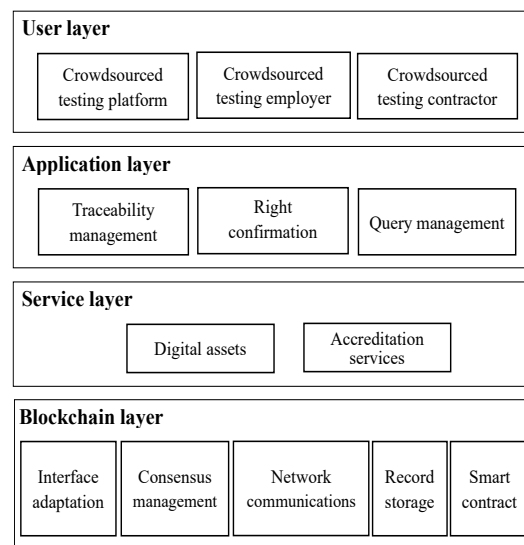
The application of blockchain technology to the management of the crowdsourced testing intellectual property is to use blockchain instead of a centralized database to store intellectual property data. The recorded data is transparent, traceable and unchangeable. The open and transparent smart contract is used to achieve the management of intellectual property and ensure the credibility and security of intellectual property data.

Figure 2 shows the intellectual property management framework for blockchain-based crowdsourced testing, which is divided into the blockchain layer, service layer, application layer and user layer. The next layer provides services for the upper layer through API interfaces. The testing code, evaluation report and other information are only circulated among the participants of the crowdsourced testing, and are

not disclosed to the outside world, and the participants are in a cooperative relationship. Therefore, the framework adopts an alliance chain structure.

### 3.1 Blockchain Layer

The blockchain layer is at the bottom of the whole framework, which provides the basic services of the blockchain for the service layer. The basic services of the blockchain layer are deployed on all nodes to verify whether the business request is valid. The specific instructions are as follows: (1) Interface adaptation: After data analysis and authentication of the request information, each participating node verifies it according to the consensus mechanism, and then stores it completely on the shared ledger. (2) Consensus management: Consensus is made by using an efficient and error-tolerant PBFT algorithm. (3) Network communication: P2P technology is mainly used for networking between nodes and data transmission of the business part. (4) Record storage: Blockchain storage structure is fully adopted, and any historical data can be found by the self-verification program after being tampered with, and real-time warning and automatic modification of its data can be carried out. (5) Smart contract: It registers and issues contracts, defines the format of uplink information, and specifies the triggering conditions of contracts and the business execution process after triggering contracts.



**Figure 2.** Intellectual property management mode for blockchain-based crowdsourced testing

### 3.2 Service Layer

In this framework, the service layer is responsible for establishing blockchain application service infrastructure products, including digital assets, authentication services and other application fields, which will help to quickly complete the construction of upper blockchain service applications, as described below.

(1) Digital assets: The online digital assets can help all participants in the crowdsourced testing complete the asset conversion from offline to online, making the crowdsourced testing transaction more transparent. After the digital assets

are put on the chain, transaction related operations such as asset transfer and cash withdrawal will have digital signature verification and leave tamper-proof records, which is helpful for the trusted management of the capital circulation in the crowdsourced testing service process and reduces the disputes over money transactions.

(2) Authentication service: in the field of intellectual property, blockchain has the ability to be indelible and publicized. In this case, all participants in the crowdsourced testing can publish intellectual property information on the blockchain through a simple interface, and other nodes in the system can provide authentication.

### 3.3 Application Layer

The application layer provides safe and reliable applications for all participants in the user layer’s crowdsourced testing. The main activities involved in the whole life cycle of trusted management of crowdsourced testing intellectual property are intellectual property control, intellectual property ownership and intellectual property query. Therefore, this framework has designed three application modules: traceability management, authority confirmation management and query management, as shown in Figure 3.

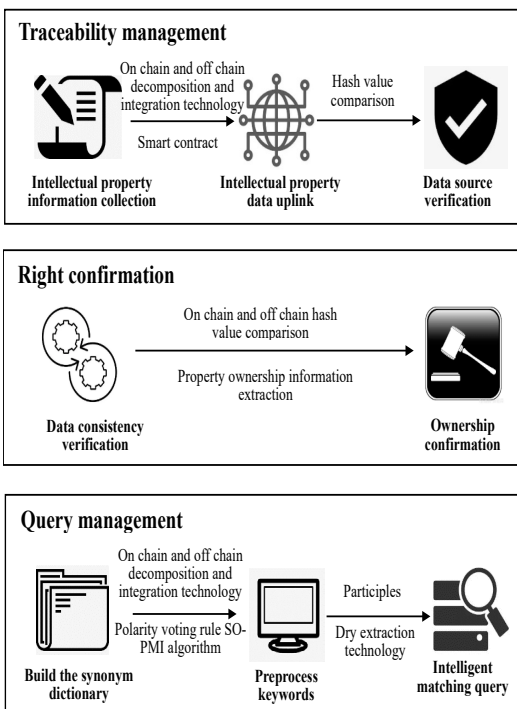


Figure 3. Three application modules

#### 3.3.1 Traceability Management

Traceability management refers to tracing the source and creation process of data through certain technologies. [18] In crowdsourced testing intellectual property management activities, a series of stages are required in the whole process of the testing project. Due to the lack of transparency in the intermediate stage, it is difficult for users to judge the source of data and whether the data is credible. Traceability

management can realize reliable traceability verification on the chain of crowdsourced testing intellectual property data by tracing the data source and conversion process and can ensure the authenticity of data.

The implementation scheme of traceability management is as follows: (i) Intellectual property information collection and storage. The system collects intellectual property data, uses encryption algorithms to convert it into hash values, and then digitally signs the hash values, uploading complete intellectual property information such as intellectual property file entities, digital signatures, provider information, and digital certificates to IPFS. [19] Subsequently, IPFS blocks, encrypts and stores the data, and calculates the unique corresponding file hash address according to the data content. According to the file hash address, users can download and save the file in the IPFS network. Once the data is stored in IPFS, it will be permanently stored in IPFS and cannot be deleted. (ii) Encrypt the complete information of the intellectual property and convert it into a unique hash value, that is, file summary. The system will form a traceability data model with data ID, file summary, file hash address, data source information, timestamp and data processing information to facilitate subsequent data traceability. (iii) Intellectual property data uplink. The data uplink process is completed by the smart contract. All nodes in the alliance chain network participate in the consensus verification of the transaction, which is transparent and traceable. [20] Traceability data is jointly maintained by all nodes to provide trust endorsement and enhance the credibility of the system. (iv) Data traceability verification. Each participant can view the intellectual property information through the unique data ID, verify the authenticity of the data, clarify the ownership of the crowdsourced testing intellectual property, protect the rights and interests of the crowdsourced testing intellectual property owners, and solve the problems in a timely manner in case of disputes.

#### 3.3.2 Right Confirmation Management

Right confirmation management means that the system uses the tamper-proof feature of the blockchain to verify whether the intellectual property data under the chain has been tampered with. The implementation method is as follows: (i) Data consistency verification. The intellectual property right confirmation function verifies the consistency between the offline intellectual property and the hash value of the file content. In order to make the data inside the system anti-attack and confidential, the SHA256 algorithm is used to encrypt the crowdsourced testing intellectual property that needs to be verified offline, [21] get the hash value A, then find the corresponding complete information of intellectual property in IPFS according to the file hash address on the blockchain, decrypt the digital signature with the public key provided by the digital certificate, and get the hash value B of the original intellectual property file content, compare it with the hash value A to see whether it is consistent, so as to verify whether the crowdsourced testing intellectual property has been tampered with. (ii) Ownership confirmation. After performing the verification, digital certificates, provider information, etc. can be obtained from the complete

information on intellectual property to clarify the owner and ownership of the intellectual property.

### 3.3.3 Query Management

Query management means that the user selects all or part of the intellectual property data from the system for browsing by setting certain query conditions. The implementation steps are as follows: (i) Build a synonym dictionary. In the retrieval process, the synonym dictionary is used to find the word information data related to the selected query word. The constructed synonym dictionary library should contain important words related to intellectual property, and should also record the associations between synonyms. Specifically, the PolarityRank rule, [22] and the Semantic Orientation Pointwise Mutual Information (SO-PMI), [23] can be used jointly to build a synonymous dictionary of intellectual property. During the construction of a synonymous dictionary, the hash address of the dictionary is recorded in the blockchain and the dictionary is recorded in IPFS. (ii) Keyword preprocessing. The words extracted from user requirements are processed by word segmentation, and character matching, understanding and statistics are combined to improve the accuracy of word segmentation results. For the segmentation results, stop words are deleted to reduce the index space and the impact of common words on retrieval effectiveness. In the meantime, for the English words extracted according to the user's needs, stem extraction technology is used to convert gerunds, negative forms, etc. into stems, replacing all morphisms. (iii) Intelligent matching search. Calculate the Word Mover's Distance (WMD) between the user requirement stemming set and each intellectual property managed by the platform. [24] The smaller the distance value is, the closer the user needs intellectual property. Therefore, the platform will display the search results in descending order of distance.

### 3.4 User Layer

The user layer indicates that all participants can directly access the application system. In the intellectual property management framework for crowdsourced testing, the user layer refers to the crowdsourced testing platform, the crowdsourced testing employer and the crowdsourced testing contractor. The crowdsourced testing employer is the person who submits testing requirements and software to be tested on the crowdsourced testing platform; The crowdsourced testing contractor is the one who completes the crowdsourced testing task on the crowdsourced testing platform; As a third party, the crowdsourced testing platform provides online systems for the crowdsourced testing employer and the crowdsourced testing contractor.

## 4 On Chain and Off Chain Decomposition and Integration Technology of Crowdsourced Testing Assets

Since the blockchain system requires each node to store ledger information, due to the persistence of blockchain data, using blockchain to record large-scale data will inevitably

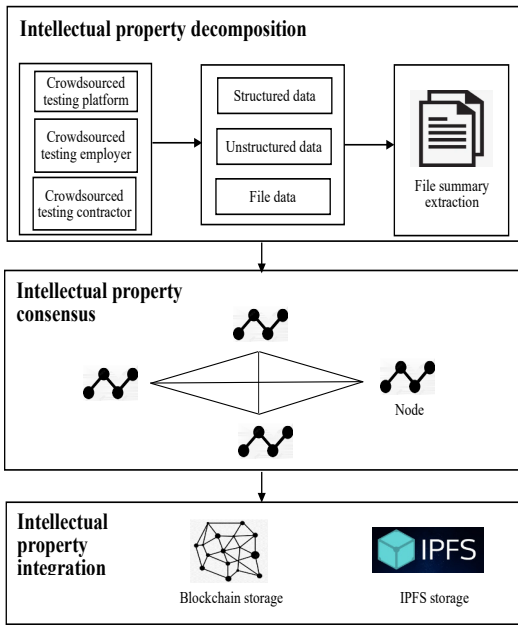
lead to data inflation and bring severe challenges to the storage performance of the system. Therefore, it is necessary to study the on chain and off chain decomposition and integration technology of crowdsourced testing assets to ensure the integrity of intellectual property data and reduce the storage pressure of the system on the chain.

In the intellectual property management framework for blockchain-based crowdsourced testing mentioned above in this article, the traceability management and right confirmation management modules need to use the online and offline decomposition and integration technology of the crowdsourced testing asset chain. On chain and off chain decomposition and integration technology of crowdsourced testing asset chains is an important foundation of the new framework used to solve the problems of high cost and small capacity of blockchain storage data. As shown in Figure 4, it is necessary to maintain a large number of structured data (such as intellectual property attribute information), unstructured data (such as testing code), and file data (such as evaluation reports and crowdsourced testing result reports). It can be seen that the management of the crowdsourced testing intellectual property has typical characteristics of multi-source, heterogeneity and large-scale. Based on the on chain and off chain decomposition and integration technology, for the new intellectual property, the file summary and intellectual property files can be saved in the alliance chain and IPFS respectively after they are signed.

As shown in Figure 4, the technology realization process is divided into three stages: intellectual property decomposition, intellectual property consensus and intellectual property integration.

### 4.1 Intellectual Property Decomposition

The intellectual property decomposition refers to the decomposition of the real entity of intellectual property into two parts: file summary and intellectual property file. Using digital signature technology can ensure the reliability and authenticity of data sources. In this step, the intellectual property entity mapping is transformed into a unique file summary, which stores the digital signature, provider, digital certificate and other information generated by the user's private key encryption. In the process of intellectual property management, file summary is used to replace the flow of crowdsourced testing intellectual property files in the intellectual property management system, and encryption certificates are used to verify the authenticity and tamper-proof of intellectual property. Specifically, firstly, the SHA256 algorithm is used to encrypt the intellectual property file  $d$  to generate the hash value  $R(d)$  of the intellectual property file content; Encrypt the hash value of intellectual property content through RSA, and generate a digital signature  $S(R(d))$ ; Again, SHA256 is used to encrypt the complete information  $t$  of intellectual property, such as intellectual property file entity  $d$ , digital signature  $S(R(d))$ , provider, and digital certificate, to obtain the hash value  $R(t)$  of the final linked intellectual property file, that is, the file summary.



**Figure 4.** On chain and off chain decomposition and integration technology of crowdsourced testing asset chain

#### 4.2 Intellectual Property Consensus

In the blockchain system, only authorized nodes can be included in the blockchain, and the consensus is completed by multiple parties rather than authorized nodes alone. Digital signature and other technologies are used to decompose structured data, unstructured data and file data generated by all parties into file summaries and intellectual property entity files. In the process of ledger consensus recording, due to the limited storage space on the blockchain, in order to reduce the storage burden of the blockchain, only file summary information is saved on the blockchain, while the managed intellectual property entities are stored in the IPFS network. Specifically, the complete intellectual property information is uploaded to IPFS to obtain the file hash address  $A(t)$ , and then the data ID, file abstract  $R(t)$ , file hash address  $A(t)$ , data source information, timestamp, data processing information, etc. are uploaded to the alliance chain. All participants jointly complete the intellectual property consensus and use the robust Hyperledger Fabric scheme to build the alliance architecture; The PBFT algorithm with high efficiency and high fault tolerance is used for consensus.

#### 4.3 Intellectual Property Integration

Intellectual property integration refers to finding specific data information in the offline IPFS according to the file hash address on the blockchain, and completing the integration of information on and off the chain. When the user queries the information on the chain, the file hash address and file summary can be obtained according to the user information and query conditions. The intellectual property entities under the chain can be searched according to the file hash address. If the results are queried in the relevant cache, it is unnecessary to further query IPFS and parse files. After the query and analysis are completed, the comparison between the file summary and the intellectual property entity information can verify that the intellectual property referred

to on the chain and off the chain is the same intellectual property, and complete the integration of the intellectual property information on the chain and off the chain.

## 5 Legal Guarantee Mechanism of the New Management Model

Blockchain technology provides a new solution for intellectual property management of crowdsourced testing, breaking through the limitations of the traditional management mode of combining manual work with central institutions. However, technical means are always mechanical and rigid, and the above-mentioned new model still needs to be supported and improved by the rule of law. Therefore, this paper proposes the following legal guarantee mechanism.

### 5.1 Improve Laws and Regulations on Judicial and Administrative Protection of Intellectual Property

The existing intellectual property law system in China does not specifically regulate the laws of Internet enterprises, making it very difficult to protect the intellectual property of crowdsourcing enterprises. It is urgent to improve relevant laws and regulations: (1) Promote judicial protection of intellectual property in crowdsourcing mode, including improving intellectual property legislation, building judicial protection institutions, and training more high-level intellectual property professionals. (2) Strengthen the administrative protection of intellectual property in crowdsourcing mode, including promoting the establishment and improvement of administrative law enforcement agencies, carrying out publicity activities to improve the awareness of intellectual property, establishing universal education on intellectual property, strengthening theoretical research on intellectual property protection, and building a public service system for intellectual property.

### 5.2 Legal Risk Control of Intellectual Property of Crowdsourced Testing

When the legal norms are insufficient and the protection of intellectual property for crowdsourced testing is regulated by the crowdsourcing platform itself, to effectively control risks and achieve the balance of interests of all participants, the autonomy rules of the crowdsourcing platform should reflect the following points and be specified in the crowdsourced service contract.

#### 5.2.1 Employer Level

First of all, if the crowdsourced testing task involves trade secrets (especially technical secrets), there is an essential conflict between the confidentiality of the task with the openness of the crowdsourcing model itself and the unspecific nature of the subject. For the protection of the intellectual property of the employer, the task containing confidential information is not suitable for crowdsourcing, and should be regarded as a prohibited crowdsourced task or the part of the task that may leak secrets should be separated. Secondly, if the crowdsourced testing task is not confidential, the employer should pay attention to the confirmation of intellectual property in the process of signing a contract with the contractor to agree on specific rights and obligations;

When the nature of the task requires, the employer shall enter into an intellectual property transfer agreement with the contractor, otherwise the employer can cancel the contractor's qualification of "winning the bid" and require him to return the reward, and the contractor will be punished accordingly by the crowdsourced testing platform.

### 5.2.2 Contractor Level

Regarding the ownership of intellectual property, the intellectual achievements provided by the contractor on the crowdsourced testing platform are at risk of unclear ownership. In practice, with regard to intellectual property issues, the employer and the contractor will make a separate agreement on the ownership of rights by concluding an intellectual property agreement; However, not every pair of the employer and the contractor can conclude an intellectual property agreement in a timely manner. The contractor's lack of awareness of its own intellectual property and the employer's neglect of reasonable and legal access to rights easily lead to ownership disputes between the employer and the contractor after the end of the crowdsourced testing process and the termination of the crowdsourced testing contract relationship. In the absence of agreement on the crowdsourced testing subject, the ownership of intellectual property is completely in accordance with the law; Generally speaking, when the task involves the creation of a work, the copyright of the completed work belongs to the trustee, that is, the contractor; When the task involves patent research and development, in the entrusted development, the right to apply for a patent belongs to the researcher and developer, namely, the contractor. The client, namely, the employer, can obtain the priority to execute the patent right and patent transfer free of charge, while in cooperative development, the patent belongs to both the employer and the contractor.

### 5.2.3 Crowdsourced Testing Platform

As a broker, the crowdsourced testing platform's legal risk control of its intellectual property is mainly reflected in whether its autonomous rules can balance the interests of all parties in the crowdsourced testing relationship.

First, as a neutral broker, the crowdsourced testing platform cannot be involved in disputes, so it should have reasonable specific rules for the design of the whole process of crowdsourced testing based on good faith and the crowdsourced method selected by the platform; Collect and keep confidential the true personal information of the contractor and the employer; Set up rules for the settlement of intellectual property disputes, and a neutral and fair online dispute resolution mechanism, so as to give consideration to the interests of all parties when intellectual property disputes arise.

Second, the crowdsourced testing platform should establish an intellectual property protection mechanism. At present, the crowdsourcing mode generally selected by the employer or the crowdsourced testing platform is a one to many integrated crowdsourcing modes, and a pricing and trading mechanism in which a single "winning bidder" gets paid. As a result, before entering into a specific contract with the employer, the contractor must put its intellectual achievements on the crowdsourced testing platform to compete with other contractors participating

in the crowdsourced testing. Accordingly, the intellectual achievements of the contractor may be infringed in the process of competition for "winning the bid", which may lead to intellectual property infringement disputes such as unilateral plagiarism and mutual plagiarism of the contractor, and even drag the employer into the vortex of infringement. Therefore, the crowdsourced testing platform should put an end to such situations in the autonomous rules, and set corresponding penalties for violators. For example, in the autonomous rules, the crowdsourced testing platform should require all contractors to initially describe their knowledge structure and innovation intention, sign a letter of guarantee without infringement of intellectual property, and submit a deposit. Those who violate the commitment should be confiscated of the deposit, temporarily prohibited or permanently deprived of the opportunity to participate.

Third, the crowdsourced testing platform should establish a multilateral mutual evaluation credit evaluation mechanism. In order to reduce the risk faced by crowdsourced testing, the platform should have a credit evaluation mechanism for all participants, and participants with low credit scores will be automatically eliminated by the market. The main evaluation connotation is as follows: review the contractor's understanding of the task, innovative ideas, participation attitude, whether there are complaints about infringement of intellectual property and other matters before evaluation; Review the difficulty of the employer's task, the size of the amount of crowdsourced testing, the fairness of the report, whether there is a fraud, and the payment speed of the cost of crowdsourced testing; After reviewing the service efficiency, the rationality of rules, difficulty in finding innovative projects, convenience in submitting crowdsourced testing reports, and perfection of the intellectual property dispute resolution mechanism of the "crowdsourced testing platform", the evaluation will be conducted.

## 6 Conclusion

To address the problems such as the lack of credibility of the current crowdsourced testing service model, insufficient standardization of crowdsourced testing intellectual property management, the inability to trace and confirm the source, and the inability to verify the authenticity and reliability of data, this paper proposes a trusted intellectual property management framework for blockchain-based crowdsourced testing based on the decentralization, traceability, tamper-proof and other characteristics of the blockchain, as well as IPFS, SHA256, and digital signature technology, to store the crowdsourced testing intellectual property data on the blockchain to ensure the security, reliability, tamper-proof and traceability of data resources. Moreover, technology is only a means to society, and any new technology means has both advantages and disadvantages. Mechanized technology alone cannot fully safeguard the intellectual property of crowdsourced testing, and a legal guarantee mechanism should be established to assist the operation of the new management model.

## Acknowledgements

This research was supported by Social Science Foundation of Fujian Province, China (Grant No. FJ2021B059) (Topic: Legalization of Credit Management of Cross-Strait, Hong Kong and Macao); Educational Commission of Fujian Province, China (Grant No. JAS21106); and Research Foundation of Jimei University (Grant No. Q202112).

## References

- [1] D.-J. Deng, K.-C. Chen, R.-S. Cheng, IEEE 802.11ax: Next generation wireless local area networks, *10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QShine)*, Rhodes, Greece, 2014, pp. 77-82.
- [2] D.-J. Deng, Y.-P. Lin, X. Yang, J. Zhu, Y.-B. Li, J. Luo, K.-C. Chen, IEEE 802.11ax: highly efficient WLANs for intelligent information infrastructure, *IEEE Communications Magazine*, Vol. 55, No. 12, pp. 52-59, December, 2017.
- [3] D.-J. Deng, C.-H. Ke, H.-H. Chen, Y.-M. Huang, Contention window optimization for IEEE 802.11 DCF access control, *IEEE Transactions on Wireless Communications*, Vol. 7, No. 12, pp. 5129-5135, December, 2008.
- [4] J. Howe, The Rise of Crowdsourcing, *Wired Magazine*, Vol. 14, No. 6, pp. 1-4, June, 2006.
- [5] D.-J. Deng, R.-S. Chang, A Priority Scheme for IEEE 802.11 DCF Access Method, *IEICE Transactions on Communications*, Vol. E82-B, No. 1, pp. 96-102, January, 1999.
- [6] A. Choudhary, M.-C. Govil, G. Singh, L.-K. Awasthi, E.-S. Pilli, D. Kapil, A Critical Survey of Live Virtual Machine Migration Techniques, *Journal of Cloud Computing*, Vol. 6, No. 1, pp. 1-41, November, 2017.
- [7] J.-H. Feng, G.-L. Li, J.-H. Feng, A Survey on Crowdsourcing, *Chinese Journal of Computers*, Vol. 38, No. 9, pp. 1713-1726, September, 2015.
- [8] D. Wan, Developing a New Model of "Four Crowds" and Promoting Talent Entrepreneurship and Innovation in Qiannan Prefecture, *China International Business*, Vol. 2017, No. 6, pp. 36-37, March, 2017.
- [9] E. Li, Z. Zhang, Research on Assessment of Intellectual Property Risk of Crowdsourcing Platform, *Science & Technology Progress and Policy*, Vol. 34, No. 12, pp. 112-119, June, 2017.
- [10] Y. Nagai, Y. Uchida, S. Sakazawa, S. Satoh, Digital Watermarking for Deep Neural Networks, *International Journal of Multimedia Information Retrieval*, Vol. 7, No. 1, pp. 3-16, February, 2018.
- [11] Z. Sun, Y. Wang, Z. Cai, T. Liu, X. Tong, N. Jiang, A Two-Stage Privacy Protection Mechanism Based on Blockchain in Mobile Crowdsourcing, *International Journal of Intelligent Systems*, Vol. 36, No. 5, pp. 2058-2080, January, 2021.
- [12] J. Guo, C. Li, G. Zhang, Y. Sun, R. Bie, Blockchain-enabled Digital Rights Management for Multimedia Resources of Online Education, *Multimedia Tools and Applications*, Vol. 79, No. 15-16, pp. 9735-9755, April, 2020.
- [13] Q.-L. Huang, Z.-F. Ma, J.-Y. Fu, Y.-X. Yang, X.-X. Niu, Privacy-preserving Digital Rights Management Scheme in Cloud Computing, *Journal on Communications*, Vol. 35, No. 2, pp. 95-103, February, 2014.
- [14] Y. Chen, H. Li, K. Li, J. Zhang, An Improved P2P File System Scheme Based on IPFS and Blockchain, *IEEE International Conference on Big Data*, Boston, MA, USA, 2017, pp. 2652-2657.
- [15] R. Burstall, B. Clark, Blockchain, IP and the fashion industry, *Managing Intellectual Property*, 23 March 2017, <https://www.managingip.com/article/2a5c1r9eduy7gz8d4xkw0/blockchain-ip-and-the-fashion-industry>
- [16] W.-T. Tsai, L. Yu, R. Wang, N. Liu, E.-Y. Deng, Blockchain Application Development Techniques, *Journal of Software*, Vol. 28, No. 6, pp. 1474-1487, June, 2017.
- [17] V. Gramoli, From Blockchain Consensus Back to Byzantine Consensus, *Future Generation Computer Systems*, Vol. 107, pp. 760-769, June, 2020.
- [18] P. Buneman, S. Khanna, W.-C. Tan, Why and Where: A Characterization of Data Provenance, *International Conference on Database Theory*, London, UK, 2001, pp. 316-330.
- [19] S.-K. Dwivedi, R. Amin, S. Vollala, Blockchain-based Secured IPFS-Enable Event Storage Technique with Authentication Protocol in VANET, *IEEE/CAA Journal of Automatica Sinica*, Vol. 8, No. 12, pp. 1913-1922, December, 2021.
- [20] Y. Li, Y. Chen, T. Li, X. Ren, A Regulatable Data Privacy Protection Scheme for Energy Transactions Based on Consortium Blockchain, *Security and Communication Networks*, Vol. 2021, pp. 1-11, December, 2021.
- [21] D. Zhang, H. Jiang, Z. Liu, SHA-256-based Trusted Boot Integrity Verification Program Design and Verification, *Network Security Technology & Application*, Vol. 2022, No. 3, pp. 49-51, March, 2022. DOI: 10.3969/j.issn.1009-6833.2022.03.028
- [22] F.-L. Cruz, C.-G. Vallejo, F. Enriquez, J.-A. Troyano, PolarityRank: Finding an Equilibrium Between Followers and Contraries in a Network, *Information Processing & Management*, Vol. 48, No. 2, pp. 271-282, March, 2012.
- [23] R. Du, Y. Zhu, H. Tian, J. Liu, J. Ma, Research on Construction of Microblog Sentiment Lexicon Based on the Smooth SO-PMI Algorithm, *Journal of Hunan University of Technology*, Vol. 29, No. 5, pp. 77-81, September, 2015.
- [24] M.-J. Kusner, Y. Sun, N.-I. Kolkin, K.-Q. Weinberger, From Word Embeddings to Document Distances, *International Conference on Machine Learning*, Lille, France, 2015, pp. 957-966.



## Biographies



**Cheng-Yong Liu** was born in New Taipei City, in 1978. He received the Ph. D. degree in Law. Now, he is an associate professor at School of Marine Culture and Law, Jimei University. His research interests include legal issues of Fintech, Blockchain and artificial intelligence.  
E-mail: [cy.liu@jmu.edu.cn](mailto:cy.liu@jmu.edu.cn)



**Cheng-Chen** was born in 1984. She received the Master degree in Law. Now, she is a doctoral candidate at the Law School of Fuzhou University. Her research interests include environmental protection theory and international environmental protection law.  
E-mail: [chengchen\\_cy@yeah.net](mailto:chengchen_cy@yeah.net)