Application and Research of Task Crowdsourcing Trusted Payment Based on Blockchain

Weijie Xia[1,a], Feng Zhang[1,b], Linlu Li[1,c], Shuang Liu[1,d]

xiaweijie@btpdi.com.cn[a], zhangfeng@btpdi.com.cn[b], lilinlu@btpdi.com.cn[c], liushuang@btpdi.com.cn[d]

Beijing Telecom Planning & Designing Institute Co., Ltd. Beijing, China[1]

Abstract—In order to improve the efficiency of project execution within the enterprise, prevent single point failure in the process of the project, and prevent violations in value transfer, this paper proposes a trusted payment system for task crowdsourcing based on blockchain, which realizes decentralization and ensures the security and efficiency of the system. Through the point-to-point value transfer and post-payment settlement mechanisms, the fairness and transparency of the system's value transfer can be improved.

Keywords-component; blockchain; task crowdsourcing; trusted payment

1. INTRODUCTION

In the process of the project, there are some tasks with low relevance and high professionalism, and there is a situation where the task workload cannot be quantified when the project is settled. As a result, an increasing number of organizations, institutions, and businesses, among others, have incorporated crowdsourcing into the project-planning process. Through network resources, this model can greatly match the resources of all parties, break through the original boundary between consumers and producers, reduce costs and increase efficiency for enterprises, give prominence to core competitive advantages and stimulate new innovation ability.

The traditional task crowdsourcing system is based on a centralized architecture that realizes value transfer and trusted payment between task initiators and executors through centralized nodes (i.e., incentives after the task is completed). However, centralized organizations generally have subjective attributes, which means they cannot be completely tamper-proof, open and transparent, so there are certain limitations. The three characteristics of blockchain technology, namely decentralization, tamper-proof and traceability, can reduce the centralization of traditional crowdsourcing systems and improve the opacity of payment in traditional crowdsourcing systems. Therefore, the task crowdsourcing trusted payment system based on blockchain can greatly ensure that the value transfer in the task crowdsourcing process is open and transparent, and the incentive payment has high credibility.

ICEMME 2022, November 18-20, Nanjing, People's Republic of China

DOI 10.4108/eai.18-11-2022.2326928

Gems, a foreign blockchain crowdsourcing platform, aims to solve the micro-task crowdsourcing protocol in the field of artificial intelligence, that is, requiring human participation but relatively simple task crowdsourcing, such as clicking links, entering web pages, labeling images, etc. The platform is a public chain organization form based on the mining mechanism. Since Gems can issue coins independently, there are certain compliance risks in China. At the same time, there are also two task distribution platforms based on blockchain in China: Weike Chain and Nework, both of which adopt a public chain structure. Weike Chain is a DAPP based on Ethereum, and Nework is a blockchain platform independently developed based on the Ethereum platform. Both of them have independent coin issuing behaviors and face compliance risks in China. Weike Chain and Nework are both forms of public chains, consensus on the chain needs to be achieved by mining. Moreover, the organizational form of the public chain is not friendly to enterprise users, which makes it easy to expose the internal information of the enterprise and cause unnecessary losses.

Based on the above, this paper uses the decentralized characteristics of blockchain technology and integrates the task crowdsourcing model to design a blockchain-based task crowdsourcing trusted payment system [1]. It uses the alliance chain as the organizational form and does not adopt the form of blockchain mining to reach consensus. There is no additional currency issuance, so there is no compliance risk. At the same time, the system can clarify the subject of the project, quantify the content of the work, integrate and efficiently use human resources within the company, and achieve the cost reduction and efficiency increase of the company's project, increasing the profit. During project settlement, credible payment is realized through a point-to-point value transfer and a post-payment settlement mechanism. It can ensure that the value flow is open and transparent, cannot be tampered with, and prevent violations of rewards and punishments, thereby forming a more efficient cooperation model and production relationship.

2. BLOCKCHAIN TECHNOLOGY

Blockchain technology, a new distributed infrastructure and computing paradigm , uses block chain data structures to verify and store data, uses a distributed node consensus algorithm to generate and update data, uses cryptography to ensure the security of data transmission and access, and uses smart contracts composed of automatic script code to program and operate data[2]. It has the characteristics of decentralization, tamper-proof, and traceability. The four core technologies of the blockchain: distributed ledger, consensus mechanism, cryptography, and smart contracts, play the roles of data storage, data processing, data security, and data application in the blockchain.

2.1 Distributed ledger

Distributed ledger is a data storage technology. It is a decentralized distributed database. Distributed ledger can share transaction information on a network composed of multiple entities, different geographic locations, and different institutions. Every participant in this network can obtain a true and unique copy of the information[3]. At the same time, in the ledger, the security of the stored data is achieved through the use of public and private keys and signatures to control the access rights of the ledger, thereby achieving encryption protection.

2.2 Consensus mechanism

In the blockchain system, during information transmission and value transfer, the consensus mechanism solves and ensures the consistency and correctness of each transaction on all accounting nodes. Based on this consensus mechanism, the blockchain system can complete large-scale and efficient cooperation without relying on a centralized organization. At present, there are three mainstream consensus mechanisms on the public chain, namely PoW, PoS and DPoS. On the alliance chain, election consensus algorithms such as PTFT or RAFT are usually used to improve efficiency.

2.3 Cryptography

Through the hash function in cryptography, it is processed into a chain structure. The latter block contains the hash value of the previous block[4]. Because the hash algorithm is unidirectional and resistant to tampering, once data is chained in the blockchain network, it cannot be tampered with and can be traced back.

2.4 Smart contracts

On the basis of distributed ledgers, smart contracts are built at the application level. When we want to solve some trust problems, we can use smart contracts to make the agreement between users in the form of code, list the conditions clearly, and execute them through programs, and the data in the blockchain can be called up through smart contracts[5].

3. TASK CROWDSOURCING SYSTEM

In order to improve the overall work efficiency, solve the problems of information and resource asymmetry in project collaboration, clarify the tasks of all parties and allocate the workload in the most efficient manner possible in the process of the project, this paper designs a task crowdsourcing trusted payment system based on blockchain, as shown in figure 1. Centralized institutions generally have subjective properties and cannot be completely tamper-proof, open and transparent. Different from traditional crowdsourcing systems that rely on the credibility of centralized institutions, this system utilizes the decentralized characteristics of blockchain technology to upload project reviews, task releases, applications, user value transfers, and other content on the chain and encrypt user data through SM3 and SM2 to form a data summary, ensuring user privacy with maximum assurance[6].

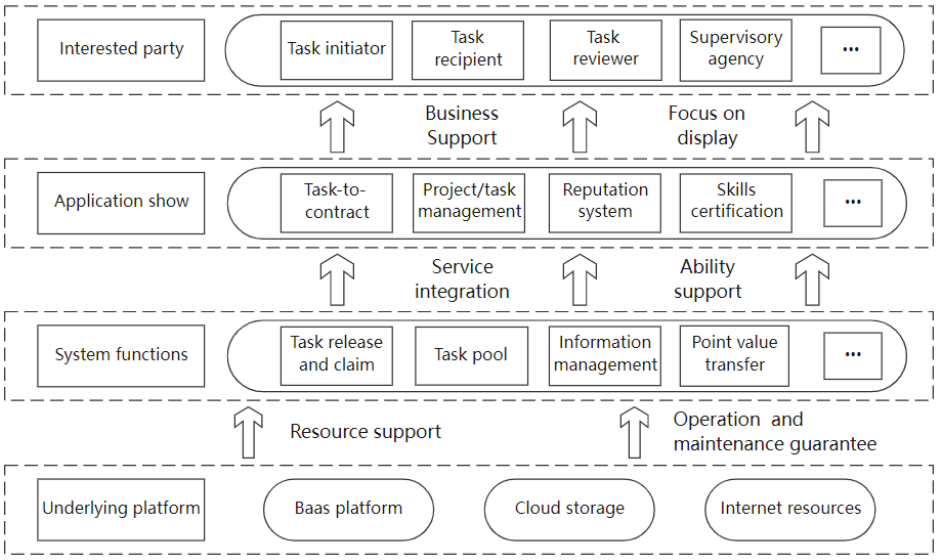

Figure 1. Blockchain-based task crowdsourcing trusted payment system architecture

4. VALUE TRANSFER SYSTEM OF TRUSTED PAYMENT

The value transfer system of trusted payment in the task crowdsourcing trusted payment system based on blockchain is mainly to store the value transfer situations of users. It puts all system operations on the chain to ensure that the value transfer process is open, transparent, and tamper-proof, and to prevent violations of rewards and punishments. As a quantitative incentive form, system value can be used to ask for help in publishing tasks in the system, and it can also be used to apply for reward redemption in the system.

4.1 Value Transfer State Tree

Since the task distribution process has to go through the steps of project review, task release and application, contribution settlement, etc., each link is highly coupled. In order to better manage the system data, this paper proposes a value transfer state tree database for the value transfer of distribution systems, as shown in figure 2, which manages the relevant basic data of the underlying value transfer in a centralized and efficient way.

The value transfer process is as follows：

- Contract confirmation: The task initiator uses the existing valuable points in the account as an incentive to release the task. After the initiator selects the appropriate claimant, the task will be converted to a contract.
- Task Acceptance: The executor submits an acceptance application after completing the task, and the initiator will perform the acceptance inspection based on the contract content. If the task is passed, the system will transfer value according to the transaction

mode of the contract. If the task is not passed, it will be rejected and the applicant will continue to perform the task.

- Value transfer: After the task is successfully accepted, the system will automatically perform value transfer operations. For each value transfer operation, a string of information such as the initiator ID, executor ID, value points, and electronic signature will be hashed and encrypted. Then the calculation result data is stored in child nodes. Each transfer operation will be stamped with a timestamp to ensure the traceability of the whole process.

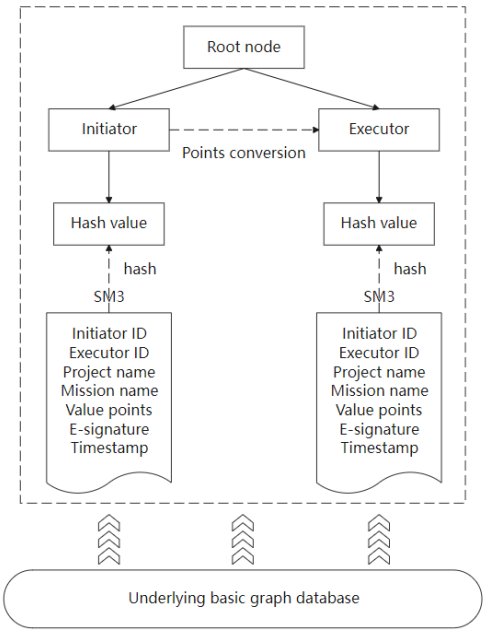

Figure 2. value transfer state tree

4.2 Point-to-Point Value Transfer Mechanism

In the traditional crowdsourcing platform, in order to protect the interests of both parties, the task initiator and the executor will realize the value transfer through an intermediary role. For example, when the task is released, the value incentives paid by the initiator will be delivered to the intermediate layer for notarization and custody. After the task is completed and confirmed by the initiator, the value incentive will be transferred to the executor’s account through the intermediate layer. If the task fails, the value may be refunded directly from the intermediate layer to the initiator's account. Therefore, the traditional value transfer is a tripartite transfer.

This introduces blockchain technology into this system, which completely removes centralization and does not require a third-party notary to be stored in it, realizing point-to-point value transfer through smart contracts. After the task is confirmed by both of the two parties, all the transfer terms will be written in the smart contract. That is, the task will be converted into a contract, and the transfer operation will be automatically executed in accordance with the

contract. When both parties confirm that the task is successfully completed at the same time, the system automatically transfers the initiator's value incentive points to the executor's account, and the reputation value of both accounts increases accordingly. At the same time, the entire process will generate corresponding transfer records on the blockchain. If the task fails, the value incentive points of the accounts of both parties remain unchanged, and the smart contract will deduct the corresponding reputation value of the responsible parties based on the reason for the failure of the task. Only the process is recorded in the blockchain, and the value in the accounts of both parties does not change. That is, no transfer is made.

The point-to-point value transfer mechanism is shown in Algorithm 1.

Algorithm 1: Point-to-Point Value Transfer

Data: $Task_{info}$:task completion; $Task_{requi}$:task requirement; P_{incent}:value incentive points; P_{credit}:credit value points; $Account_{in}$:initiator account; $Account_{re}$:recipient account

Result: Point-to-Point Value Transfer

initialization;
while *Recipient submits the task* **do**
  if $Task_{info} = Task_{requi}$ **then**
    $Account_{in} = Account_{in}$ - P_{incent} + P_{credit};
    $Account_{re} = Account_{re}$ + P_{incent} + P_{credit};
  else
    $Account_{re} = Account_{re}$ - P_{credit};
  end
end

4.3 Post-payment Settlement Mechanism

Since the project is a long-term process, the workload of the tasks attached to the project varies. Therefore, the schedules are also inconsistent. From a practical point of view, the final value transfer is usually completed only after the project is completed, and the workload and rewards are divided according to the final degree of contribution. However, there may be a situation in the actual process where it is not easy to evaluate the final quantitative rewards for each task before the project is completed. Based on this, this paper designs a post-payment settlement mechanism from the perspective of actual project operations. The post-payment settlement process is shown in Figure 3

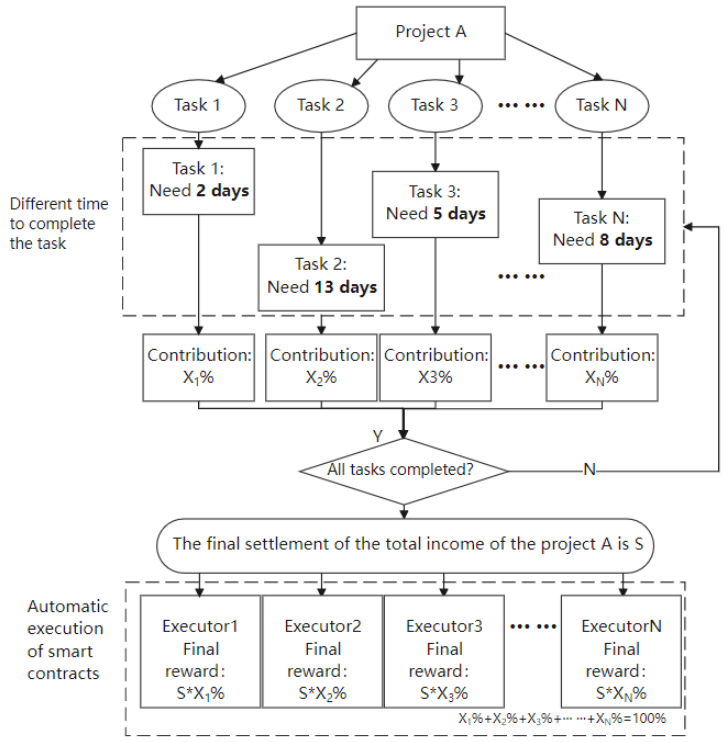

Figure 3. Flow chart of post-payment settlement mechanism

The post-payment settlement mechanism, that is, settlement after the task acceptance is achieved, because it is not easy to quantify the reward value of the task in advance, only a contribution ratio can be determined according to the importance of the task to the project. After the final project reward is confirmed at the end of the project, value rewards will be issued in proportion to the contribution. Therefore, for this task, the executor cannot get the corresponding value points the first time. In order to protect the rights and interests of the task executor, the post-payment terms will be directly written in the contract when the task is transferred to the contract. Without relying on centralized roles, the technology itself guarantees that a task executor can ultimately obtain application rewards. When the project is completed, based on the terms of the smart contract, the system automatically transfers the value from the initiator's account to the executor's account and completes the value post-payment operation.

5. EXPERIMENT ANALYSIS

The bottom layer of this experiment is based on the Fabric Hyper ledger framework[7], and the upper layer implements various functional applications of task crowdsourcing services. The test environment is shown in TABLE I

TABLE I. SYSTEM TESTING ENVIRONMENT

Node Number	***Node Configuration***	***Network Bandwidth***	***Programming Language***
22 platform	24C 128G	10 Thousand Mb	Python

A stress test was carried out for the throughput of the system in the case of setting 4, 8, or 16 formula nodes based on the test environment. The system continues to send transactions at a high frequency (unprocessed transactions remain above 1,000 for one hour). Under the test conditions, the system's transaction processing success rate is 100%. The overall test result is shown in Figure 4

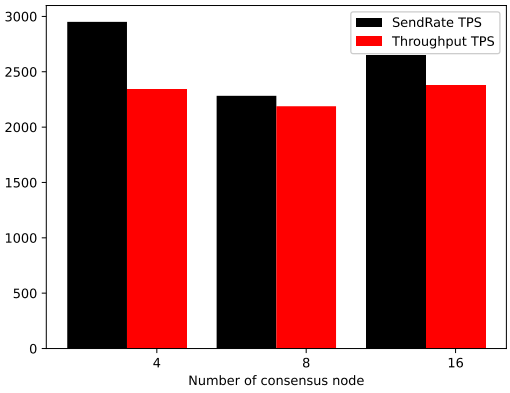

Figure 4. Stress test results

The test environment for the data structure of the value transfer state tree is shown in TABLE II

TABLE II. COMPUTER TESTING ENVIRONMENT

CPU	***Memory***	***Language***
8G	16G	Python

This paper conducts comparative experiments on the traditional flattening naming storage method (FN), the hierarchical named storage method (HN), and VTST. The query efficiency of the three data structures was tested on a scale of 1 million to 10 million data nodes. The experimental results are shown in Figure 5The final experiment shows that compared with the traditional HN and FN, the data storage method in this paper can achieve nearly a hundred times the performance advantage.

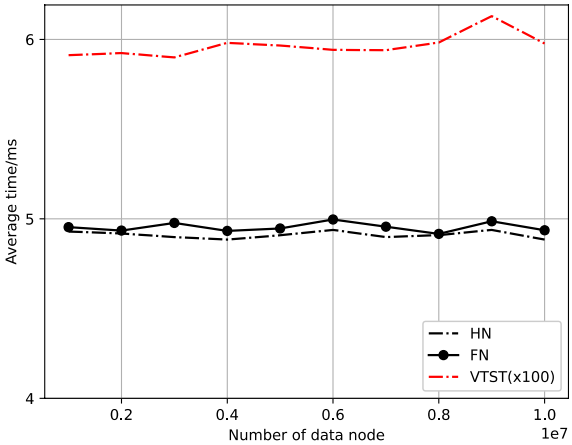

Figure 5. VTST test results

6. CONCLUSION

This paper proposes a trusted payment system based on blockchain by integrating the application of a task crowdsourcing system. With the help of the decentralized characteristics of blockchain technology, a point-to-point value transfer mechanism and a post-payment settlement mechanism in the task crowdsourcing system are presented. At the same time, all operations are on the chain, which greatly improves the transparency and fairness of the value transfer in the crowdsourcing system. In addition, experimental tests have also proved that the VTST has nearly a hundred times the performance advantage compared with the traditional storage method. Comprehensive performance meets the needs of practical applications and can basically reach the level of large-scale application promotion.

REFERENCES

[1] C. Tongran, “Study on quality problems and management measures during construction process of steel structure”, School of Civil Engineering Southeast University, 2019.

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”, Manubot, 2019.

[3] Z. Feng, J. Wenbao, S. Boxuan, “TAC: A unified trust anchor framework based on consortium blockchain”, Journal of Physics: Conference Series. IOP Publishing, 2020, 1544(1): 012181.

[4] Z. Feng, S. Boxuan, J. Wenbao. “Review of key technology and its application of blockchain”, Chinese Journal of Network and Information Security. 2018.

[5] G. Wood. A. Ethereum, “A secure decentralised generalised transaction ledger”, Ethereum Project Yellow Paper, 2014.

[6] D. Larimer, Delegated proof-of-stake (dpos), Bitshare whitepaper, 2014.

[7] J. Bonneau, J. Clark, S. Goldfeder, “On Bitcoin as a public randomness source”, IACR Cryptology ePrint Archive, 2015.