ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20201224085501
Original scientific paper

A Ring Signature Trust Model for Project Review Based on Blockchain Smart Contract

Hao FU*, Wenhai NIE, Li LIU

Abstract: The traditional offline review model of grid projects has the problems of high cost, high risk and low efficiency, making the project review insecure and inefficient. What is worse, the review data of a grid project are generally stored in a central database, which is vulnerable to attacks and not highly trustable. To solve the problems, this paper proposes a ring signature trust model based on smart contract, an important blockchain technology, for project review. The blockchain technology was introduced to build an online review platform for grid projects, greatly saving human and financial resources. Then, the consensus efficiency was improved with a trust-based node consensus mechanism. Besides, the ring signature was integrated with smart contract to allow review experts to submit their results anonymously, ensuring the fairness and impartiality of grid project review. On this basis, an efficient review system was established for grid projects, and a secure review environment was created, so that the review results will not be tampered with. The case analysis proves that the proposed method can effectively solve the problems of traditional grid project review, making the review system more secure and efficient. The research findings provide decision and theoretical supports for grid project review.

Keywords: blockchain; grid project review; ring signature; smart contract

1 INTRODUCTION

With the rapid development of social economy and new energies (e.g. wind power and solar energy), the upsurge in the number of grid projects is a drain on review resources, such as review time, technicians, designers, and project managers. The current review model poses a serious challenge to the quality and efficiency of grid project review [1, 2]. The review of grid projects is critical to the development of power companies. Concerning grid project management, good review rules and strategies can create an objective and fair environment with benign competition, which effectively promotes grid construction and grid project quality. The review of grid projects in an important node in the closed-loop management of power companies. The grid projects can be greatly enhanced in output benefits and research efficiency through scientific review [3, 4]. Therefore, the development of grid companies hinges on the design of an efficient system for grid project review.

Safety, fairness, and efficiency are the keys to building a grid project review system. Offline review, which is adopted for most grid projects, wastes human and financial resources, and easily causes corruption. Online review, which is adopted for a few grid projects, also faces some problems. For instance, the applicant of a grid project might distrust the results of online review, and demand reevaluation of the project based on relevant data, thereby disrupting the normal progress of the project. Moreover, the review data of a grid project are generally stored in a central database. The data are prone to leakage and tampering, whenever the central database is under malicious attacks. This greatly challenges maintenance of the transaction system [5]. Facing the rapid expansion of power companies and the sheer number of grid projects pending review, the traditional strategies for grid project review have three main problems: (1) The numerous offline project reviews push up the cost and decision time of the review center, reducing its operating efficiency; (2) The project applicants do not really trust the review center; (3) The massive amount of review results stored in the central database are insecure, as they are vulnerable to malicious attacks.

The blockchain provides a decentralized, trust-free, and traceable solution to the high cost and high risk in the traditional review strategies of grid projects [6, 7]. So far, fruitful results have been achieved in both blockchain and grid project review. Li and Gong [8] researched how the US and China manage the science and technology (S & T) funds, and identified the features of management institutions in the following aspects: institutional development, assessment comprehensiveness and continuity, and S & T information management. Considering the current status of the S & T evaluation system in Shenzhen, Li and Gong suggested further improving the policy and institution system for S & T evaluation, highlighting the key indices of S & T evaluation, and making S & T evaluation more comprehensive and continuous. Drawing on information economics, Pellerin and Perrier [9] developed improvement measures and suggestions to prevent adverse selection in project review. Xu and Wang [10] proposed several strategies to apply and implement blockchain technology for trust building in academic publishing, namely, opening research process, promoting data autonomy, and optimizing peer review. Drobny [11] studied the application of blockchain technology in the peer review of scientific journals, and reconstructed an equal, transparent, and interactive relationship between editors, authors, readers, and experts, from such three levels as status relationship, information relationship, and evaluation relationship. To sum up, the relevant studies face two common defects: (1) Few have integrated blockchain with grid project review; (2) Most studies, which are merely theoretical interpretations, fail to clarify the process or develop a plan for project review based on smart contract, an important blockchain technology.

Through the above analysis, this paper puts forward a grid project review strategy based on smart contract, aiming to satisfy the growing demand for grid project review. The main contributions of this research are as follows: (1) offline review was converted into online review through blockchain technology, saving lots of human and financial resources; (2) the consensus efficiency was improved with a trust-based node consensus mechanism; (3) the traditional digital signature was

replaced with ring signature to keep the review experts anonymous, preventing malicious users from offering or taking bribes; (4) a decentralized and trust-free system was set up for grid project review based on smart contract, ensuring the operating efficiency of project review. The case analysis shows that the proposed review strategy has advantages like decentralization and high efficiency, providing a good reference for grid project review.

2 ARCHITECTURE OF BLOCKCHAIN-BASED GRID PROJECT REVIEW

2.1 General Guidelines

Grid project review must be guided by clear ideas. In the absence of such ideas, the technical architecture will be too weak and instable to meet the requirements of project review [12, 13]. The following are the ideas, architecture, and requirements of grid project review:

The ideas of project review should reflect fairness and impartiality. The review should adhere to the principle of the survival of the fittest. The review process must be objective and trustworthy, laying a solid basis for implementing and promoting the project in future. Moreover, the review activities must be fair enough to promote S & T development: excellent grid projects can be selected through accurate, trustworthy, and fair reviews, contributing to the S & T reserve of the country.

The traditional review model of grid projects lacks trust, due to the high concentration of review data. To solve the problem, the architecture of project review centers on blockchain technology, which ensures that the review data are authentic, reliable, safe, and traceable. Meanwhile, the review data are easy to store and analyze, thanks to the supports from techniques like cloud computing, big data, and artificial intelligence.

There are mainly two requirements on project review: First, the review standards must be uniform. Prior to the review, the relevant standards should be disclosed timely to the public, and the key contents should be clearly explained. For example, the allowable deviation between the effectiveness of the project and the review standard, the minimum standard to meet the needs of the project, and the funding limit for the implementation of the program. If the review standard is not clearly stated to all relevant parties in advance, one party may raise an objection, which will lead to the problem that the review cannot be carried out. Therefore, the clarity of the review standard is the basic requirement for project review. Second, the review process must be open and transparent.

On the basis of clear review standards, the innovative development ideas and refined review concepts are run through the project review process. At the same time, drawing lessons from the international advanced project review process to make the review process efficient. In addition, ensure that all audit data should be tracible, and the review results should be well-established.

2.2 Review Architecture

Blockchain offers a completely open, shared, transparent and decentralized platform. As a typical blockchain technology, Ethereum is a Turing-complete one-stop blockchain development platform, supporting protocol implementation with multiple programming languages [14, 15]. Smart contract is the core of the application of the Ethereum platform, which lowers the threshold for developing blockchain applications [16, 17].

According to the general guidelines of grid project review, this paper designs a 7 - layer review architecture for grid projects (Fig. 1). From bottom to top, the seven layers are infrastructure layer, data layer, network layer, consensus layer, incentive layer, smart contract layer, and application layer.

The infrastructure layer provides the basic services for grid project review. Through this layer, the virtual computing resources, storage resources, and review rules are pushed to the review users for utilization and management. There are three main functions of this layer: First, the basic information of the review project is acquired and transmitted rapidly through new generation high-speed network, 5G, and the IoT. Second, review results and relevant information are collected, stored, and distributed through secure cloud servers and high-performance storage techniques. Third, the service capabilities of the infrastructure are optimized through cluster management and automated operation & maintenance, providing a reliable guarantee for the soundness of project review.

The data layer encapsulates the chain structure of the underlying data blocks, including the public and private keys of the review users, the Hash function, and the Merkle tree. The pubic and private keys protect user privacy through asymmetric encryption and digital signature. The Hash function and Merkle tree maintain the chain structure of blocks, prevent data from being tampered with, and make block data traceable.

The network layer provides communication supports for the information exchange between nodes on the blockchain network, including the mechanisms for P2P networking, data dissemination, and data verification.

The consensus layer mainly syncs the data records of all nodes on the blockchain through the consensus mechanism, and guarantees the transparency and data sharing of the blockchain system. The consensus mechanism algorithm, as the core technology of the blockchain, determines the "bookkeeper". The bookkeeping method affects the security and reliability of the entire system. Currently, famous consensus mechanism algorithms include PoW, PoS, DPoS, and PBFT. Next, an overview of these four consensus algorithms.

Satoshi Nakamoto adopted the PoW consensus algorithm in his Bitcoin foundational paper. PoW means that one party submits a calculation result that is known to be difficult to calculate but easy to verify, and everyone else can verify this result and be sure that the submitter has completed the result. A lot of calculations. The throughput of the blockchain using the PoW consensus algorithm is limited, but the scalability is very good, and nodes can join or withdraw freely.

However, the PoW consensus algorithm consumes a lot of calculation examples. Therefore, the researchers proposed the PoS consensus algorithm, which uses proof of equity to replace the proof of work based on hash power in PoW, which is obtained by the node with the highest equity rather than the highest computing power in the system. Block bookkeeping rights, equity is reflected in the

ownership of a specific amount of currency by a node, which is called currency age. The PoS consensus algorithm is likely to cause the problem of fixing a few nodes to monopolize the bookkeeping power, which violates the decentralized nature of the blockchain.

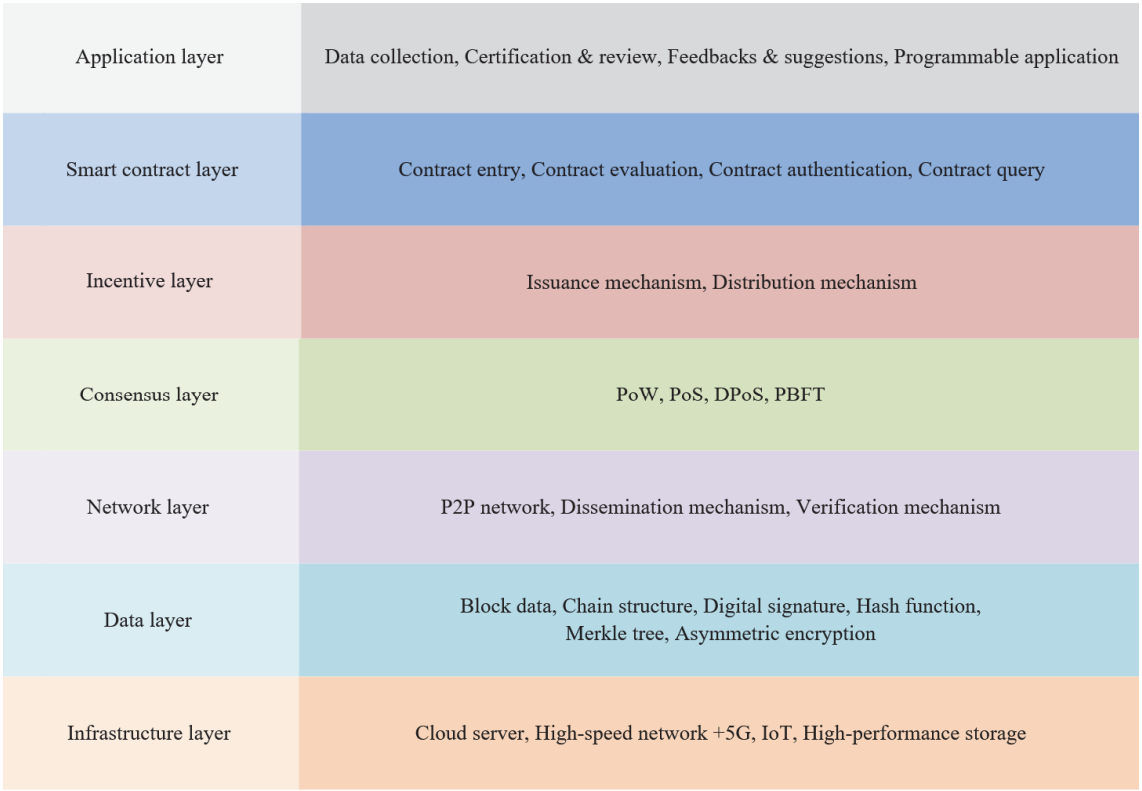

Figure 1 The architecture of grid project review based on smart contract

Note: PoW, PoS, DPoS, PBFT, P2P, 5G, and IoT are short for proof of work, proof of stake, delegated proof of stake, practical Byzantine fault tolerance, peer to peer, the fifth-generation technology standard for cellular networks, the Internet of things, respectively.

The DPoS consensus algorithm tries to solve the problems of PoW and PoS. By implementing a decentralized democratic method, each coin is equivalent to a vote. The holder of the coin can vote for several votes according to the number of coins he holds. Give yourself trustees. The system will select the N individuals with the most votes as system trustees. Their job is to sign (produce) blocks, and before each block is signed, it must first verify that the previous block has been signed by a trusted node.

The PBFT algorithm is based on the principle of state machine replication, and is mainly composed of a consistency protocol, a view switching protocol, and a checkpoint protocol. First, the master node sorts the requests, and then the nodes respond to the requests. The result that most nodes respond to is the final result.

The incentive layer integrates economic factors (e.g. the issuance and distribution of economic incentives) into the blockchain system through the issuance and distribution mechanisms. Incentive mechanism is the sum of the structure, method, relationship and evolution law of the incentive subject system in the organizational system that uses a variety of incentive methods and makes it standardized and relatively fixed, and interacts with and restricts each other. In the review of blockchain-based projects, the incentive mechanism plays an important role, the nodes that obey the bookkeeping rules are incentivized, while those that violate these rules are penalized, creating a virtuous circle for system development.

The smart contract layer further encapsulates each part of the block data encapsulated in the data layer, with the aid of smart contract (a commercial contract compiled by programming languages). Smart contract is a transaction contract trigger mechanism deployed on the blockchain. When the trigger condition is met, it can realize the automatic execution of the transaction plan and automatic settlement of cash. It conducts trusted transactions without a third party, and transactions are traceable and irreversible. For example, this layer can interpedently encapsulate the comprehensive review results of a project in a block with smart contract, such that the results cannot be tampered with or deleted. In this way, the review and supervision of the grid project is significantly simplified. Under our architecture, the smart contract layer supports the entry, evaluation, authentication, and query of contracts.

The application layer, the top layer of grid project review, mainly has three functions: the collection and entry of project information, the certification and review of grid project, and the query of review results. The review results cover the following aspects: the state of grid project (qualified or disqualified), feedbacks and suggestions on the grid project, and the improvement direction of grid project.

In summary, our smart contract-based grid project review system has three core functions. First, the system can record and store the data on review projects: the situation of each project review is recorded on a distributed ledger; the actual data of the project in daily life, as well as

the evaluation of the project by ordinary people, are collected through the IoT and big data technology. Second, the system can evaluate each project based on the actual data and agreed standards, and transmit and store the evaluation results in an encrypted manner, facilitating the query by the project leader. Third, this system takes the alliance chain as the core, which keeps the review contents private across the network, and promotes the joint governance by various relevant organizations.

3 OPERATION MECHANISM OF BLOCKCHAIN-BASED GRID PROJECT EVALUATION

3.1 Identity Management of Grid Project Review

The efficiency and accuracy of grid project review are essential to the development of power companies. Currently, most grid projects are reviewed offline in a centralized manner. The experts making the review are not anonymous. Without anonymity, it is impossible for them to be fair and impartial, leaving the door open for fraudulent practices. What is worse, the offline centralized review consumes lots of human and financial resources, which brings a high cost. Furthermore, all the review results are often stored in the database of a department. The centralized storage has high security risk, making the database prone to attacks [18].

As a decentralized and trust-free technology, the blockchain ensures that all data are open and transparent, and protects the anonymity of the review with an asymmetric encryption algorithm. The review results submitted by experts are executed automatically by the smart contract, eliminating the risk of tampering [19]. In a blockchain-based project review environment, the experts can review grid projects anonymously, without being affected by irrelevant personnel. In the meantime, the review data are kept secure, traceable, and tamper-proof, owing to the distributed storage and chain structure of the blockchain. Based on the blockchain, this paper sets up an identity management model for grid project review (Fig. 2).

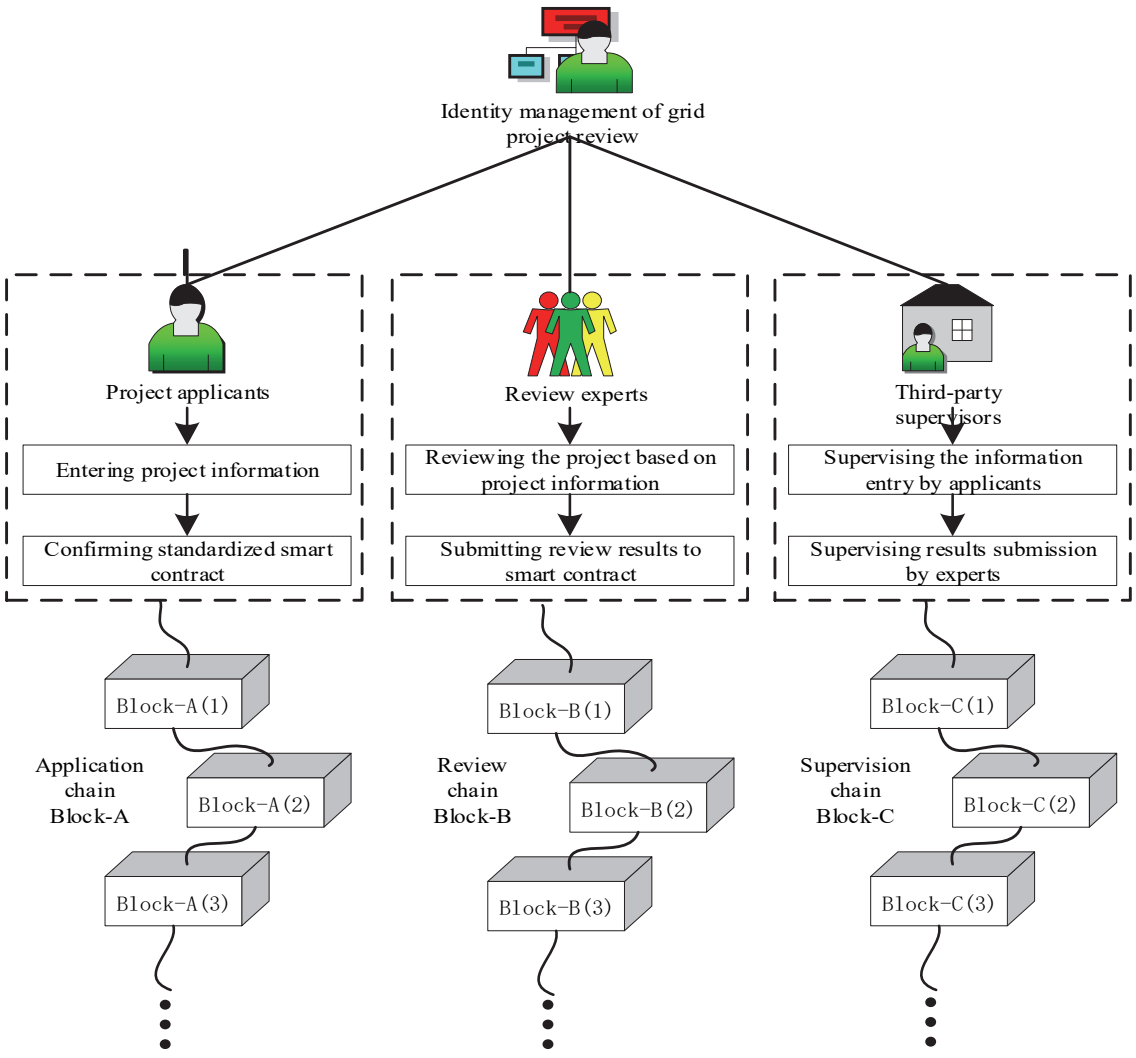

Figure 2 The blockchain-based identity management model for grid project review

As shown in Fig. 2, the personnel involved in grid project review are divided into three categories for management: project applicants, review experts, and third-party supervisors. Considering the different roles of the three kinds of personnel, our identity management model for grid project review was constructed based on the blockchain, supported by the information exchange via Internet. The model consists of three blockchains: the application chain (Block-A), the review chain (Block-B), and the supervision chain (Block-C). These three chains

are independent and coupled with each other. The review experts on the review chain need to obtain project information on the application chain to complete a reliable review. At the same time, in order to ensure the correctness of project information and the fairness of expert review, this paper proposes a supervision chain composed of third-party nodes to achieve effective supervision of information on the review chain and application chain. The details about the three blockchains are as follows:

The application chain (Block-A) is a public chain. Prior to the review, the project leader needs to enter the details of the project into the system, and fill in and confirm the agreed standardized smart contract. After passing the review of third-party supervisors, a block of project information will be produced based on the previously collected project information, and will be linked to the application chain by the agreed "bookkeeper".

The review chain (Block-B) is an alliance chain. After examining all the project information on the application chain, the review experts will make a review of the project, and submit the results to the smart contract, including the project quality and suggestions. Once the last expert submits his/her results, the smart contract will start to process the review results of all experts, and generate a block of review results. The block will be linked to the review chain by the "bookkeeper".

The supervision chain (Block-C) is an independently formed alliance chain. The third-party supervisors can be served by relevant government agencies, and participate in grid project review across the blockchain. The third-party supervisors mainly monitor whether the applicants input the correct information, and whether the experts submit review results on time. The nodes of third-party supervisors only retain the hash digest generated by the blocks in the application and review chains, and produce a digest directory tree that records the real-time review information and post-supervision information.

3.2 Node Trust-based Consensus Mechanism for Project Review

The node trust-based consensus mechanism is mainly used in the alliance blockchain network of project review. Suppose the network contains $n\left(n \in \mathbb{N}, n \geq 3\right)$ nodes. The trust degree of node *i* can be denoted as $T_i \in [0, 1]$. A high T_i value means node is very trustworthy and suitable to serve as the "bookkeeping node" in the network.

The trust degree of consensus nodes can be evaluated based on three kinds of behaviors: normal behavior, fault behavior, and malicious behavior. The trust degree of a node will vary, if the node behavior changes from one kind to another. Normal behavior will increase the trust degree, fault behavior will reduce the trust degree, and malicious behavior will set the trust degree to zero. The initial trust degree T_{i0} of a node is 0.5 by default. Once the trust degree falls below 0.1 or malicious behavior is detected, the node will be labeled as a malicious node, and excluded from the consensus process. Based on the node's trust update rules, it can be seen that if the node's trust level is lower than 0.1, it means that the four factors of the node's activities, consensus completion rate, historical influence and consensus time efficiency have not reached the standard in the process of multiple consensus, and the number of failures is equivalent *F* or malicious behavior. Therefore, the node will be marked as a malicious node and excluded from the consensus process.

3.2.1 Trust Indices

In this paper, the common indices of node trust are extracted by evaluating the previous consensus behavior of nodes, and then the trust degree of each node is derived from the values of these indices. A total of four common indices were thus extracted: activity, consensus completion rate, historical influence, and consensus time efficiency.

Definition 1 The activity refers to the frequency of a node partaking in consensus within a period, revealing the activity level of the node in the consensus network. The activity A_i of node i can be expressed as:

$$A_i = \alpha \cdot e^{-\frac{1}{n}} \tag{1}$$

where, *n* is the number of the node partaking in consensus; $\alpha\left(\alpha \geq 0\right)$ is the node activity adjustment factor, which is adjusting the growth rate. The value of A_i is proportional to that of *n*, reflecting the activity level of the node.

Definition 2 The consensus completion rate refers to the ratio of the number of a node completing the consensus to the total number of the node partaking in consensus, revealing the operating status of the node in the consensus network. The consensus completion rate P_i of node i can be expressed as:

$$P_i = \left(\frac{m}{n}\right)^{\beta} \tag{2}$$

where, *m* is the number of the node completing the consensus; *n* is the total number of the node partaking in consensus; $\beta\left(\beta \geq 1\right)$ is the adjustment factor of consensus completion rate P_i. The value of P_i is proportional to the ratio of m to n. The greater the P_i value, the more stable the node.

Definition 3 The historical influence refers to the influence degree of the historical trust degree of a node on its current trust degree, revealing the historical information of the node. The historical influence H_i of node *i* can be expressed as:

$$H_i = \frac{1}{\gamma} \cdot \left(\frac{1}{2}\right)^{\Delta t} \tag{3}$$

where, Δt is the interval between two samplings; $\gamma\left(\gamma \geq 1\right)$ is the time attenuation factor, which adjusts the influence degree of time. The value of H_i is inversely proportional to the value of Δt: the longer the time, the weaker the influence of historical trust degree on the current trust degree.

Definition 4 Consensus time efficiency refers to the efficiency of time utilization of a node partaking in consensus, revealing the ability of the node partaking in

consensus. The consensus time efficiency E_i of node i can be expressed as:

$$E_i = \eta \cdot \left(\frac{1}{2}\right)^t \cdot \frac{a}{b} \tag{4}$$

where t is the time for the node to complete consensus; a and b are the number of consensus nodes reaching an agreement and the total number of consensus nodes; η is the adjustment factor of consensus time efficiency. When most nodes have reached a consensus about the block, the efficiency of a node is negatively correlated with the time it takes to reach a consensus.This is because the premise of the completion of a task is the effective achievement of consensus of all nodes. If the node reaches a consensus for a long time, the time to complete the task is longer, which makes the node's efficiency low. Therefore, the shorter the consensus time, the higher the efficiency of the node.

3.2.2 Trust-Based Node Consensus Mechanism

After each consensus is completed, the system will evaluate the performance of each node in the consensus process. The trust degree T_i^j of node i in the j-th consensus process can be expressed as:

$$T_i^j = r_1 \cdot A_i + r_2 \cdot P_i + r_3 \cdot H_i + r_4 \cdot E_i \tag{5}$$

where, A_i, P_i, H_i, and E_i are the activity, consensus completion rate, historical influence, and consensus time efficiency of a node, respectively. These four parameters are related to each other. The higher the enthusiasm of the node to participate in the consensus, the higher the consensus completion rate, and the historical trust of the node represents the probability that the node has a good faith consensus in this cycle, which affects the consensus time efficiency. In addition, the consensus completion rate and the consensus time efficiency are key factors for evaluating the consensus results. Therefore, these four factors complement each other as the authoritative mark of the trustworthiness of nodes; r_1, r_1, r_3, and r_4 are the weight coefficients of A_i, P_i, H_i, and E_i, respectively. The sum of these four weighting coefficients is 1, and the values of these four weighting coefficients can be flexibly adjusted as needed.

Eq. (5) can accurately reflect the performance of the node in the previous consensus process. The node will be given a high trust degree, if the activity and the consensus completion rate are high, or the consensus time efficiency is high. Otherwise, the node will be given a low trust degree.After that, the trust degrees of all nodes will be updated by the following strategy. Let k be the number of consensuses completed so far, and T_i be the trust degree of node i after the k-th consensus. Then, the trust degree of node i can be updated by:

$$T_i = \begin{cases} \lambda \cdot T_i^k + \left(\sum_{j=1}^{k-1} T_i^j + T_{i0}\right), \\ \textit{if the node has not committed malicious behavior} \\ 0, \\ \textit{if otherwise} \end{cases} \tag{6}$$

where, λ is the adjustment factor of trust degree update (if the trust degree of the node is higher than the previous level, the value of λ should be properly increased; otherwise, the value of λ should be properly reduced); $\left(\sum_{j=1}^{k-1} T_i^j + T_{i0}\right)$ is the trust degree of node i after the k−1-th consensus.

The update rule (6) imposes strict restrictions on the malicious behavior of nodes. Once a node commits any malicious behavior, the node will be excluded from the following consensus. The update rule (6) proposes that the λ parameter changes dynamically with the change of the node's trust in each consensus cycle, which strictly limits the malicious consensus behavior of the node. If the node's consensus completion degree or consensus time efficiency in this consensus cycle is low, then the trust value level of this time must be lower than the previous trust degree level, which causes λ to become smaller, and the corresponding update of the node trust increment is also more efficient than others The node is small. In addition, once a node has malicious behavior, the trust of the node is immediately cleared, and the consensus contribution of the node in the past will no longer exist. In summary, this update rule can not only improve the consensus efficiency of nodes, but also strictly limit the malicious behavior of nodes.

The trust degrees of nodes can be used to make consensus. This paper adopts the PFBT consensus mechanism based on node trust. Since all the nodes partaking in consensus are trustworthy, it is very unlikely for any of them to become Byzantine node in consensus voting. In this way, our strategy greatly improves the efficiency of node consensus and the credibility of consensus results, laying a solid foundation for fair and impartial project review.

3.3 Ring Signature

Ring signature keeps the signers completely anonymous in the message. Then, a non-signer using the verification algorithm can only confirm that the signature is signed by a group formed by a list of public keys, failing to identify which user in the list is the actual signer [20, 21]. Besides ensuring user anonymity, a linkable ring signature helps to judge whether different signatures belong to the same user. This paper introduces linkable ring signature algorithm to grid project review, which ensures the authenticity of the evaluation results and the anonymity of review experts. The ring signature algorithm is implemented in five steps:

Step 1. Initialization:

Select domain Z_q, group G_1, and random numbers $t \in Z_q$ and $A \in G_1$; calculate parameters $P' = t \cdot P$ and $c_{k+1} = H_2\left(L \| m \| e(A, P) \| e(A, P)\right)$.

Step 2. Generating a ring series:

For $i = k + 1, ..., n - 1, 0, ..., k - 1$, randomly select elements R_i and T_i that belong to domain G_1, and calculate $C_{i+1} = H_2\left(L \| m \| e(R_i, P) e\left(c_i H_1(ID_i), P_{pub}\right)\right)$ $\| e(T_i, P) e\left(c_i H_1(ID_i), P'\right)$.

Step 3. Closing the ring:

Calculate $R_k = A - c_k S_{ID_k}$ and $T_k = A - c_k t H_1(ID_k)$

Step 4. Outputting signature:

Output a ring signature $\delta = (P', c_0, R_0, R_1, ..., R_{n-1}, T_0, T_1, ..., T_{n-1})$.

Step 5. Algorithm verification:

For $i = k + 1, ..., n - 1, 0, ..., k - 1$, calculate $C_{i+1} = H_2\left(L \| m \| e(R_i, P) e\left(c_i H', P_{pub}\right) \| e(T_i, P) e(c_i H_1(ID_i)), P')\right)\right)$, where $H_1: \{0,1\}^* \to G_1$ and $H_2: \{0,1\}^* \to Z_q$ are hash functions. If $c_n = c_0$ output 1, then the signature is valid; else output 0, then the signature is invalid.

3.4 Workflow of Grid Project Review Based on Smart Contract

As shown in Fig. 3, this paper splits the grid project review into three phases in time: contract formulation, contract issuance and contract execution. The smart contract-based grid project review has three defining features: (1) The review experts are anonymous to project applicants; (2) The project leader is anonymous to review experts; (3) The relevant terms in the contract are executed automatically.

During contract formulation, project applicants and review experts need to register as users of the blockchain platform. Upon registration, the blockchain platform automatically assigns public and private keys to these users. The public key of a user is his/her account address on the platform, while the private key of a user is the only password for him/her to manage and operate the account. After obtaining the public and private keys, the users start to negotiate a standardized smart contract, including the list of project materials to be provided by the applicants, the main indices of the project review, and the review process. When all the parties agree to the contract, they will leave digital signatures on the contract with their private keys, with the aim to ensure the validity of the contract. The agreed contents of the signed smart contract will be transmitted to the blockchain network.

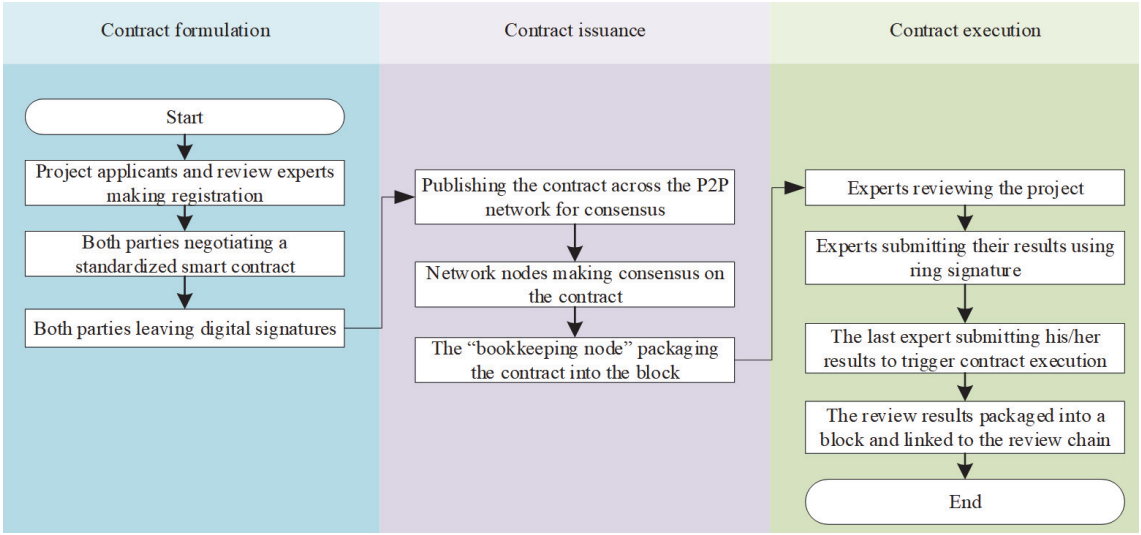

Figure 3 The workflow of grid project review based on smart contract

During contract issuance, the preliminary smart contract is published across the P2P network for consensus. The third-party supervisors, as the verification nodes, will make consensus on the published smart contract following the trust-based node consensus mechanism. If the consensus is achieved, the agreed "bookkeeping node" will package the contract into the block and link it to the blockchain platform.

Contract execution is critical to the fairness of grid project review. During contract execution, the experts review each project according to the information provided by the applicant, and the information collected by the blockchain platform. The review results are submitted anonymously with ring signature. When the last expert in the list of public keys submits his/her results, the execution conditions of smart contract will be triggered. Then, the submission channel will be closed, and the smart contract will process all the review results. After the processing, the review results will be packaged into a block, and linked into the review chain. The relevant personnel of the project can view the review results on the review chain.

After a project is successfully reviewed, the state of the smart contract will be indicated by a state indicator. When all the transactions in the contract are sequentially executed, the state indicator will mark the contract as completed. Then, the smart contract will be removed from the latest block. Otherwise, the state indicator will market the contract as in progress. In this case, the smart contract will be saved in the latest block, waiting to be handled in the next round until it is completed. All the transactions and state processing are automatically completed by the built-in smart contract system at the bottom of the blockchain. The whole process is transparent and tamper-proof.

4 SECURITY ANALYSIS AND PROOF

Theorem 1 The smart contract-based grid project review system is unforgeable.

Proof: It is assumed that the probability of malicious user A to obtain a valid signature δ from the database is k; there exists an algorithm F with probabilistic polynomial time (PPT) complexity that can query the outputs of H_1 and H_2; malicious user A has constructed a Turing machine Q

with PPT complexity that can call F to solve the discrete logarithm problem of at least one public key in the private key list L' at the probability of λ. Then, the probability for A to forge the private key x of a user is $k\lambda / n$ at the most. Next, A selects a fixed list L of public keys and a random number t', and generates a signature $\delta'\left(P', C_0', R_0', R_1', ..., R_{n-1}', T_0' ..., T_{n-1}'\right)$ by formula $P' = t'P$. The search for suitable P', t', and P is equivalent to solving a discrete logarithm problem, i.e. finding the t in $P' = tP$. If list L contains the public keys of N users, then $Q_1(k) = k\lambda / n$. Hence, the time complexity for A to forge the signature is $O(k\lambda / n)$, which is equivalent to $O(n)$. Therefore, the smart contract-based grid project review system is unforgeable. Q.E.D.

Theorem 2 The smart contract-based grid project review system is anonymous.

Proof: All review results and user signatures are open in the grid project review system. All the information can be verified on the blockchain. Suppose a malicious user A wants to attack the identity U_{ID_k} of a user U. Then, A needs to call algorithm F to solve the discrete logarithm problem of at least one public key in the private key list L at a certain probability, in order to obtain parameter t. A still needs to solve the following equations:

$$Pr(x) = \begin{cases} R_k = B - c_k U_{ID_k} \\ T_k = B - c_k t H_1(ID_k) \end{cases} \tag{7}$$

With three unknown terms, Eq. (7) are not solvable. Thus, the malicious user cannot know the identity of the signer. Therefore, the smart contract-based grid project review system is anonymous. Q.E.D.

Theorem 3 The smart contract-based grid project review system is unique.

Proof: When the list L of the public keys is determined, a digital signature can be generated by:

$$\begin{cases} h = H_2(L) \\ Y = h^{x\pi} \end{cases} \tag{8}$$

As shown in Eq. (7), one private key can only produce one Y, Y represents the unique signature corresponding to each node; $H_2(L)$ represents hashing the public key list. In the grid project review system, the review results of an expert are unique and not resubmitted, if the signature Y corresponding to the review results only appears once. Hence, the smart contract-based grid project review system is unique. Q.E.D.

5 CASE ANALYSIS

5.1 Review Platform Settings

In the lab environment, a grid review platform was simulated based on Ethereum. The platform involves five review experts and three project applicants, who apply for the same kind of projects. The simulation platform is illustrated in Fig. 4.

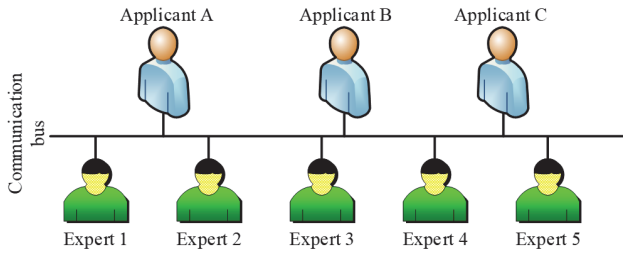

Figure 4 The simulation platform

As shown in Fig. 4, all the parties involved in project review are connected to the Ethernet communication bus to realize information exchange. In this Ethereum-based simulation platform, all the nodes are equal, and none of them is the central node.

5.2 Project Review Tests

All projects were reviewed on the simulation platform. After the three applicants submitted applications for review in turn, the review experts started to review their projects one after another. The review results are recorded in Tab. 1.

Table 1 The review results

Applicant	Expert	Anonymous application?	Time of submission	Time of contract execution	Review blockchain generated?
A	1	Yes	14:05:08	14:12:15	Yes
	2	Yes	14:10:21		
	3	Yes	14:08:32		
	4	Yes	14:12:15		
	5	Yes	14:06:03		
B	1	Yes	14:45:13	14:49:15	Yes
	2	Yes	14:42:31		
	3	Yes	14:47:22		
	4	Yes	14:49:35		
	5	Yes	14:44:01		
C	1	Yes	15:25:28	15:30:11	Yes
	2	Yes	15:27:16		
	3	Yes	15:22:39		
	4	Yes	15:28:07		
	5	Yes	15:30:11		

As shown in Tab. 1, the experts managed to review the projects in turn, after these were separately submitted by the three applicants. Under the support of ring signature and trust-based node consensus mechanism, the five experts always submitted the review results anonymously, keeping the review fair and impartial, further confirms theorem 2: The smart contract-based grid project review system is anonymous. According to the time of results submissions and contract executions, the smart contract was executed whenever the triggering conditions were satisfied, further confirms theorem 1: The smart contract-based grid project review system is unforgeable. All three reviews succeeded in generating the review block, reflecting the application value of the proposed grid project review system, further confirms theorem 3: The smart contract-based grid project review system is unique.

6 CONCLUSIONS

The traditional model of grid project review not only wastes human and financial resources, but also faces a high risk of malicious attacks on the database of the review

center, that is, the review results are easily tampered with. To solve the problems, this paper introduces the blockchain technology to build an anonymous, secure, and efficient transaction system. According to the general guidelines of grid project review, this paper designs a 7 - layer review architecture for grid projects. From bottom to top, the seven layers are infrastructure layer, data layer, network layer, consensus layer, incentive layer, smart contract layer, and application layer. After that, the identities of review personnel were managed in a unified manner, and the task of each kind of identity is detailed. Next, the ring signature and trust-based node consensus mechanism were proposed, making the consensus efficient and the submission of review results anonymous. In this way, the entire review becomes fair and impartial. On this basis, the specific steps and implementation methods were described for smart contract-based grid project review. Through case analysis, it is learned that, once the applicants file the application for review, the proposed method can ensure the anonymity of expert review, trigger the execution conditions of the smart contract, generate the review block, and link it to the blockchain network.

There are many areas worth exploring in the field of combining blockchain and grid project review: the security and economic analysis of blockchain-based grid project review, that is, how should we ensure the security and optimize the economy of project review under the decentralized and trust-free blockchain environment; improving review quality and efficiency with blockchain, facing the proliferation of online reviews. Therefore, the future research will try to build a high-quality, efficient model for blockchain-based grid project review that fully integrates the resources of all parties, and design a comprehensive three-dimensional review management model to provide technical and economic supports for power grid development.

Acknowledgements

This work is supported by National Social Science Fund Project (19BGL003).

7 REFERENCES

[1] van Dorp, J. R. (2020). A dependent project evaluation and review technique: A Bayesian network approach. *European Journal of Operational Research*, *280*(2), 689-706. https://doi.org/10.1016/j.ejor.2019.07.051

[2] Lu, M., Li, H., Zhang, Y. F., Xie, Q., & Cai, X. H. (2018). Vector control of brushless double fed generator based on control winding orientation on smooth switch from stand-alone mode to grid-tied mode. *Traitement du Signal*, *35*(1), 85-95. https://doi.org/10.3166/TS.35.85-95

[3] Groneberg, D. A., Klingelhöfer, D., Brüggmann, D., Scutaru, C., Fischer, A., & Quarcoo, D. (2019). New quality and quantity indices in science (NewQIS): Results of the first decade-project progress review. *Scientometrics*, *121*(1), 451-478. https://doi.org/10.1007/s11192-019-03188-8

[4] Koke, B. & Moehler, R. C. (2019). Earned Green Value management for project management: A systematic review. *Journal of Cleaner Production*, *230*, 180-197. https://doi.org/10.1016/j.jclepro.2019.05.079

[5] Kisely, S. & Siskind, D. (2020). Undertaking a systematic review and meta-analysis for a scholarly project: an updated practical guide. *Australasian Psychiatry*, *28*(1), 106-111. https://doi.org/10.1177/1039856219875063

[6] Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. *Journal of Industrial Information Integration*, *15*, 80-90. https://doi.org/10.1016/j.jii.2019.04.002

[7] Zeng, S. Q., Huo, R., Huang, T., Liu, J., Wang, S., & Feng, W. (2020). Overview of blockchain Technology: Principle, progress and application. *Journal of communications*, *41*(1), 134-151.

[8] Li, X. L. & Gong, Y. (2019). A study of the NIH, NSF evaluation systems in the U.S.A. and its revelation to Shenzhen. *Science Research Management*, *40*(8), 293-296.

[9] Pellerin, R. & Perrier, N. (2019). A review of methods, techniques and tools for project planning and control. *International Journal of Production Research*, *57*(7), 2160-2178. https://doi.org/10.1080/00207543.2018.1524168

[10] Xu, J. & Wang, J. Y. (2017). Build up the trust of academic publishing: Based on the technology of block chain. *Publishing Journal*, *25*(6), 19-24.

[11] Drobny, S. D., Snell, A., Morris, L., Harshbarger, C., Village, P., & Fischer, S. A. (2019). Collaborative rural nurse peer review: A quality improvement project. *Journal of Nursing Care Quality*, *34*(1), 22-27. https://doi.org/10.1097/NCQ.0000000000000331

[12] Nam, M. (2019). The review on the national project or individual paper for computer-based assessment system development. *The Journal of Educational Development*, *39*(1), 1-17. https://doi.org/10.34245/jed.39.1.1

[13] Mohagheghi, V. & Mousavi, S. M. (2019). A new framework for high-technology project evaluation and project portfolio selection based on Pythagorean fuzzy WASPAS, MOORA and mathematical modeling. *Iranian Journal of Fuzzy Systems*, *16*(6), 89-106.

[14] Hu, W., Li, H. H., Hu, Y. W., & Yao, W. H. (2019). A blockchain-based spot market transaction model for energy power supply and demand network. *European Journal of Electrical Engineering*, *21*(1), 75-83. https://doi.org/10.18280/ejee.210112

[15] Narayana, V. L., Gopi, A. P., & Chaitanya, K. (2019). Avoiding interoperability and delay in healthcare monitoring system using block chain technology. *Revue d'IntelligenceArtificielle*, *33*(1), 45-48. https://doi.org/10.18280/ria.330108

[16] Song, I. B. & Kim, Y. J. (2020). A Study on the normative recognition of blockchain smart contract. *Journal of the Korea Society of Computer and Information*, *25*(1), 187-198.

[17] Wang, Q., Lau, R. Y. K., & Mao, X. (2019). Blockchain-enabled smart contracts for enhancing distributor-to-consumer transactions. *IEEE Consumer Electronics Magazine*, *8*(6), 22-28. https://doi.org/10.1109/MCE.2019.2941346

[18] Song, K. S. (2019). A study on establishment of post-evaluation system for research support projects in humanities and social sciences. *Korean Comparative Government Review*, *23*(3): 295-321.

[19] Fan, J. L., Li, X. H., Nie, T. Z., & Yu, G. (2019).Overview of smart contract technology in blockchain system. *Computer Science*, *46*(11), 1-10.

[20] Ren, Y., Zhao, Q., Guan, H., & Lin, Z. (2020). On Design of Single-Layer and Multilayer Code-Based Linkable Ring Signatures. *IEEE Access*, *8*, 17854-17862. https://doi.org/10.1109/ACCESS.2020.2967789

[21] Assidi, H., Ayebie, E. B., & Souidi, E. M. (2019). An efficient code-based threshold ring signature scheme. *Journal of Information Security and Applications*, *45*, 52-60. https://doi.org/10.1016/j.jisa.2019.01.006

Contact information:

Hao FU
(Corresponding author)
Economic and Technical Research Institute of State Grid Jibei Electric Power Co., Ltd.,
Beijing 100038, China
E-mail: haofu_2020@sina.com

Wenhai NIE
Economic and Technical Research Institute of State Grid Jibei Electric Power Co., Ltd.,
Beijing 100038, China
E-mail: wenhainie@sina.com

Li LIU
Economic and Technical Research Institute of State Grid Jibei Electric Power Co., Ltd.,
Beijing 100038, China
E-mail: liliu_2020@163.com