# Research on Online Quiz Scheme Based on Double-layer Consortium Blockchain

Haojian Shen
School of Information Engineering Wuhan University of Technology
Wuhan, China
e-mail: shenghaojian@ whut.edu.cn

Youan Xiao
School of Information Engineering Wuhan University of Technology
Wuhan, China
e-mail: youan@whut.edu.cn

*Abstract*—**The students' online quiz is a way to realize the informatization and modernization of higher education. To solve the problem that the scoring process is non-transparent, injustice and the final results are easy to be changed, an online quiz scheme based on Double-layer Consortium Blockchain is proposed. The scheme achieves the public verification of students' answers and the answer records cannot be tampered with but can be traced. Besides, group signature is used to solve the problem of anonymous abuse in blockchain applications. In addition, the storage pressure of sub-chains' nodes can be further reduced by adding the prime-chain's index to the sub-chains.**

***Keywords- online quiz; Consortium Blockchain; Double-layer chain; group signature***

## I. INTRODUCTION

Along with the idea of "Internet +" being raised, most universities have begun to pay attention to realizing the informatization and modernization of higher education by combining education with Internet Technology. An important part of higher education is to understand students' learning status. Experiment is a very effective way to check out the students' learning status. But there are problems in the evaluation of the experiments that scoring process is non-transparent, injustice and the grades can be changed easily. Under the background of the informatization and modernization of higher education, experiments can also be carried out through online quiz. However, the current online quiz and online examination systems mostly adopt the B/S or C/S structure [1][2], and the students' answers are verified centrally. And it is still unable to solve the above problems.

With the extensive research and application of blockchain in the financial industry, commerce, service industry and other fields, the application in education is still in its infancy. In spite of this, the blockchain serving as a public distributed account is more transparent and reliable in recording students' academic performance. The University of Nicosia in Cyprus launched a master's degree in blockchain development and application and started using blockchain to record students' learning processes and results. However, this kind of blockchain application mainly plays the role of a public account and does not record how students obtain their grades. This paper will combine the traditional online quiz, online examination systems and blockchain technology to achieve the public verification of students' answers and record the answer records in the blockchain to realize that the answer records cannot be falsified but can be traced.

There are the following problems and corresponding solutions in applying blockchain to online quiz.

*a)* Anonymous Abuse Problem

Users in blockchain use the public key as a pseudonym to conduct transactions, which protects users' privacy [3]. However, users' privacy protection and dispute resolution mechanism are not perfect, which can cause anonymous abuse. When a student's score is questioned, we need to uncover the student's anonymity and get the mapping relations between student's pseudonym and his real identity.

Group signature [4][5] resolves two seemingly contradictory security properties: anonymity and traceability. The correspondence between entities and their roles in group is shown in Table I. A course corresponds to a course group. The group manager is the teacher of the course and the group members are the students who have selected the course. Group manager can uncover group members' anonymities when necessary.

TABLE I. CORRESPONDENCE BETWEEN ENTITIES AND THE ROLES IN GROUP

| Entity | Roles in Group | Describe |
|---|---|---|
| Course | Course Group | A course corresponds to a Course Group. |
| Teacher | Group Manager | A teacher can be the Group Manager of several Course Groups. |
| Students | Group Members | A student can be the Group Member of several Course Groups. |

*b)* Transaction Throughput and Storage Capacity Problem [6].

Every full node in blockchain must maintain the entire state of the system and process every transaction, which greatly reduces the transaction throughput. And each node theoretically needs to synchronize all the blockchain data, which greatly increases the storage pressure of nodes.

Vitalik Buterin proposed using sharding to solve above problems in the Ethereum 2.0 mauve paper [7] at the Community Ethereum Development Conference in 2016. Ethereum divides the entire network into a number of relatively independent shards, each of which maintains an independent sub-chain. Each node chooses to join one or more shards based on its own computing power and storage capacity, and processes and stores the transactions on these

2474-3828/18/$31.00 ©2018 IEEE
DOI 10.1109/ITME.2018.00213

IEEE computer society

shards. The entire network can process and store different transaction data in parallel, and a single node does not need to process and store all the data. The first double-layer blockchain—LightChain [8] came online On January 9, 2018. The double-layer structure is composed of a prime-chain and numerous sub-chains. The prime-chain is the mother chain, and there is only one prime-chain. Sub-chains are independent from each other, and the number of sub-chains can be expanded when necessary. The transaction is verified by the sub-chain nodes and regularly synchronized with the prime-chain to ensure that the prime-chain has the complete transaction records of the entire network.

In this paper, a course group is taken as a shard of consortium blockchain and maintains a sub-chain. The prime-chain records the answer records of all course groups. The storage pressure of sub-chains' nodes can be further reduced by adding the prime-chain's indexes to the sub-chains. We call it Double-layer Consortium Blockchain.

## II. OVERALL INTRODUCTION OF THE SCHEME

### A. The Basic Process of a Single Quiz

The process of a single quiz in the scheme is shown in Figure 1.

*a)* The group manager of a course group issues questions to its group members.

*b)* Group members answer the questions. And the answers need to be the publicly verified by the other members.

*c)* Group manager signs the answer record which has been verified publicly.

*d)* Group manager sends the signed answer record to the full nodes, and the full nodes verify the signature and add it to the prime-chain.

*e)* When the prime-chain adds a new block, update the corresponding sub-chains.

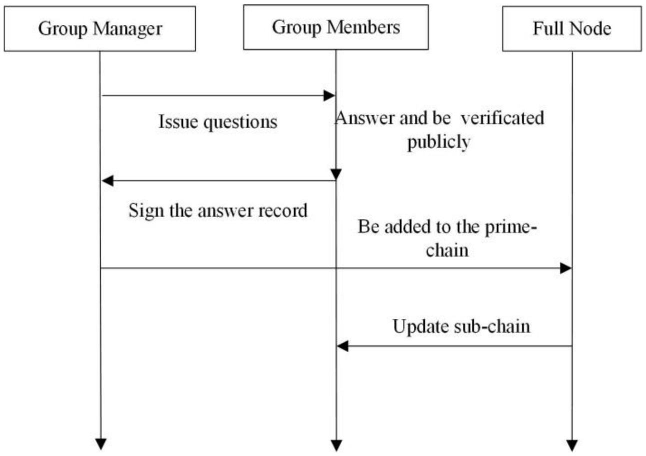

Figure 1. Quiz Process

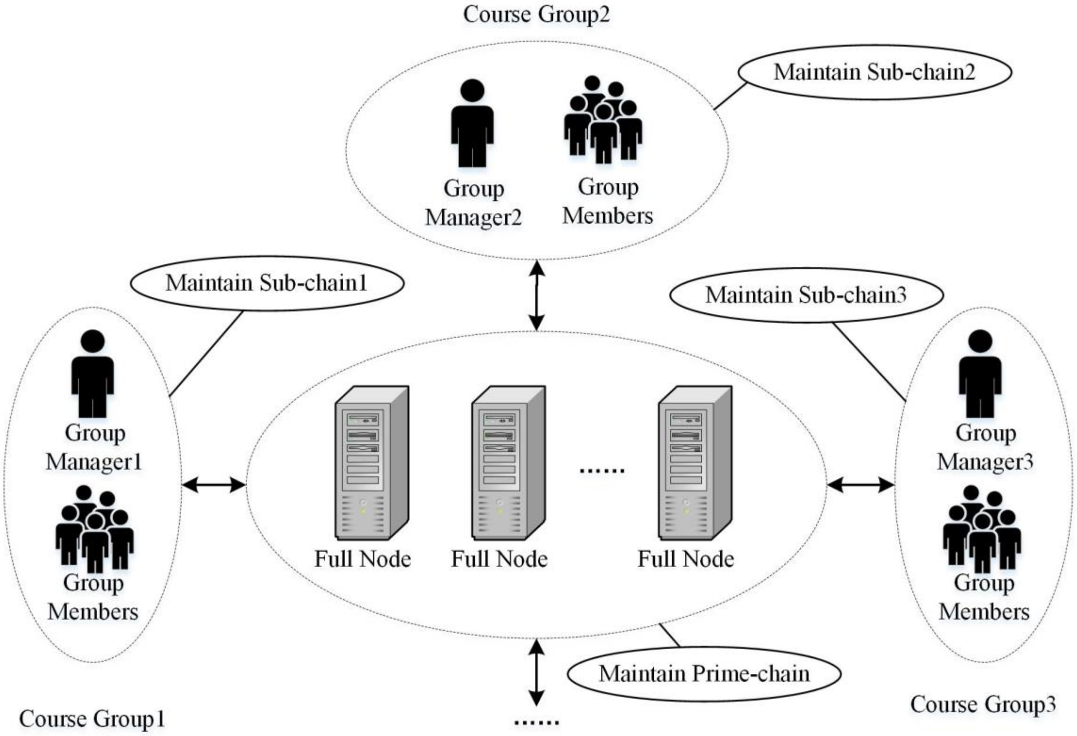

Figure 2. Network Structure of Consortium Blockchain

### B. *Scheme Model*

The network structure of consortium blockchain is shown in Figure 2. A course group consists of a group manager and group members. The group manager is responsible for issuing questions and managing group members. The group manager also needs to sign the answer records which are verified publicly by group members and send them to the full nodes. The group members answer the questions and the answer records need to be verified by the other group members.

The prime-chain is maintained by the full nodes. Answer records in all course groups are sent to the full nodes after being signed by the group managers. The full nodes verify the signatures and add the answer records to the prime-chain. The group members collectively maintain the sub-chain, which records the answer records in its own course group.

### C. *Online Quiz Scheme*

The online quiz scheme is divided into three stages, namely group manager initialization and group members' registration, quiz stage and tracking stage.

*1) Group manager initialization and group members' registration:*

Let $p$ and $q$ be a large prime number, $g$ be a generator of $\mathbb{Z}^*_p$ and $h$ be a generator of a finite cyclic group $\mathbb{C}$ of order $q$. The group manager $GM_i$ selects his private key $SK_i$ and sends his public key $PK_{GMi} = g^{SKi}$ $(mod\ p)$ to the full nodes.

Group member $j$ selects his private key $x_j$ and sends his public key $y_j=g^{xj}$ $(mod\ p)$ to the group manager $GM_i$. $GM_i$ selects a random number $n_j \in_R \mathbb{Z}^*_p$ for $j$ and adds the public key $PK_j=y_jn_j$ $(mod\ p)$ to the group member list. The Group member $j$ uses $SK_j=x_jn_j$ $(mod\ p\text{-}1)$ as his private key and the public key $PK_j$ as his pseudonym.

*2) quiz stage:*

The quiz stage uses different quiz schemes to achieve public verification according to the type of questions.

If the question is an objective question, the group manager $GM_i$ needs to publish the score and the quiz deadline $t$. If the correct answer is *results*, $GM_i$ should also publish $y=h^x \in \mathbb{C}$ where $x=hash(results) \in \mathbb{Z}_q$. The group member who obtains the correct answer before the deadline will get the score. If the group member $PK_j$ gets the $x$, he need to prove it to other members through a zero-knowledge proof. The specific process is as follows:

*a)* $PK_j$ randomly selects $r \leftarrow_R \mathbb{Z}^*_q$, calculates and publishes $t=h^r \in \mathbb{C}$.

*b)* For different $t$, the group manager $GM_i$ randomly selects and publishes different $c \leftarrow_R \mathbb{Z}^*_q$.

*c)* $PK_j$ calculates and publishes $s \equiv xc+r$ $(mod\ q)$.

*d)* All members of the group first check whether the time exceeds the quiz deadline. If it does not exceeds the deadline, continue to prove, otherwise refuse. Then check whether $PK_j$ is in the group member list. If $PK_j$ is in the group member list, continue to prove, otherwise refuse. Then check whether the local answer records already contain the answer record. If the answer record has not been recorded, continue to prove, otherwise refuse. Finally check whether $h^s=y^ct$ is valid. If it is valid, record the answer record locally. The group manager will sign the record and send it to the full nodes.

If the question is a subjective question, the group manager $GM_i$ needs to publish the score and the quiz deadline $t$. The group member $PK_j$ answers the question and sends the answer to the group manager with his own signature. The quiz is stopped when the quiz deadline arrives. The group manager publishes the reference answer and the answers submitted by all group members. All group members conduct mutual evaluation and the group manager gives scores based on the results of the mutual evaluation. Finally, the answer records are signed and sent to the full nodes by the group manager.

The full nodes verify all the answer records from each group by using public keys of the group managers. If the verification passes, the records will be added to the prime-chain. Whenever a new block is added to the prime-chain, the sub- chains will record the index which is the location of the answers of its course group in the prime-chain.

The structures of prime-chain and sub-chain are shown in Figure 3. A block consists of block header and block body. The block header consists of an index, a timestamp, a merkle root and the previous hash which is the hash value of the previous block. The block body stores a merkle tree. Each node on the merkle tree is a hash value. Each leaf node of the prime-chain corresponds to a hash of an answer record. For example, the Tx0, which is an answer record in prime-chain, consists of course name, teacher name, student pseudonym, answer time and score. Each leaf node of the sub-chains corresponds to a hash of a brief answer record. For example, the Tx0' consists of student pseudonym, score and its index in the prime-chain. Every non-leaf node is labelled with the hash of the labels of its child nodes. With the merkle root, any data tampering will be detected to ensure the integrity of the data. After the prime-chain block is generated, each group member searches for the prime-chain according to all his own local answer records to obtain the indexes which are the locations of the local answer records in the prime-chain, and adds it to the sub-chain. All group members delete the local answer records which has been synchronized.

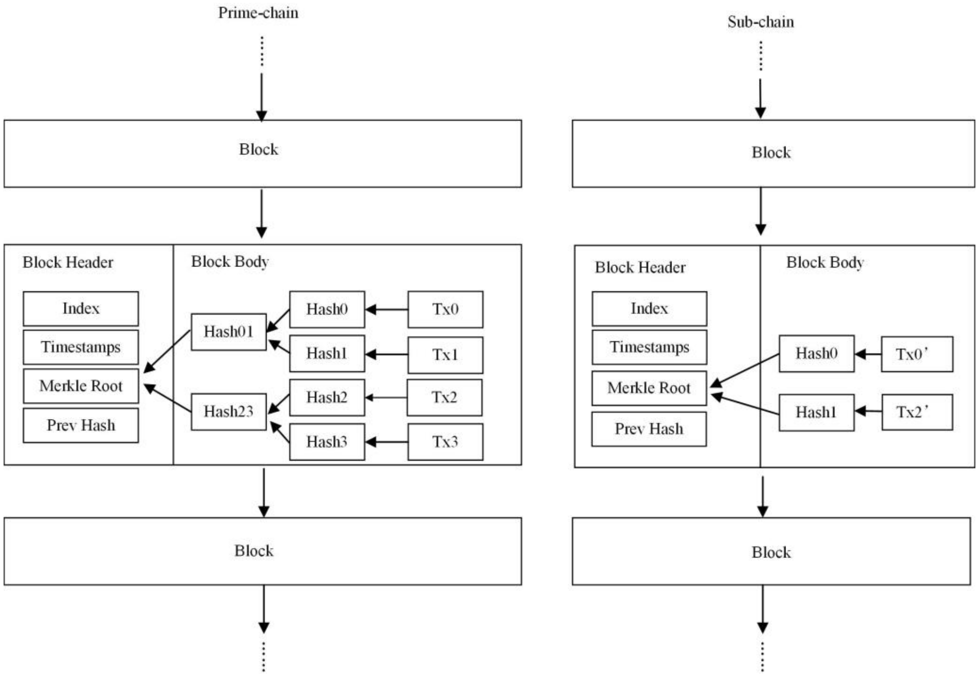

Figure 3. The structure of prime-chain and sub-chain

*3) tracking stage:*

When a group member A questions the score of a group member B, A can track all the answer records of B by the following two ways to prove the correctness of B's score:

Method 1: Since the group manager knows the mapping relations between group members' pseudonym and their real identities, A can ask the group manager about B's pseudonym and the group manager can tell A B's pseudonym after obtaining the consent of B. Then A can query all the answer records of B on the prime-chain or the sub-chain.

Method 2: B can prove its pseudonym $PK_B$ to A through a zero-knowledge proof. And A can prove the correctness of B's score by querying all the answer records of $PK_B$. The proof process is as follows:

*a)* B randomly selects $r \leftarrow_R \mathbb{Z}^*_p$, calculates and sends $t=g^r \in \mathbb{Z}^*_p$ to A.

*b)* A randomly selects and sends $c \leftarrow_R \mathbb{Z}_p$ to B.

*c)* B calculates and sends $s \equiv SK_B c+r \ (mod\ p)$ to A.

*d)* A checks whether $g^s=PK_B{}^c t$ is valid or not. If it is valid, it will prove that $PK_B$ is B's pseudonym.

## III. SECURITY AND PERFORMANCE ANALYSIS

### A. Security Analysis

*1) The scheme has anonymity.*

After registration, a group member $j$ uses his public key $PK_j$ as his pseudonym. Other members of the same group or other groups cannot get his real identity through $PK_j$.

*2) The scheme has traceability.*

When a group member is registered with the group manager, he will notify the group manager of his real identity and pseudonym. The group manager can restore the group member's identity based on the signature and his public key. Besides, all answer records are recorded in consortium blockchain. As a result, all answer records are traceable.

*3) The zero-knowledge proof in the scheme is zero-knowledge.*

In order to extract $x$, the extractor interacts with the group member twice. If the group member selects the same random number $r_1$, $r_2$ ($r_1=r_2$), which means $t_1=t_2$. The two responses of the extractor are taken as $c_1$, $c_2$ ($c_1 \neq c_2$), The extractor obtains the following two equations:

$$s_1 \equiv xc_1+r_1\ (mod\ q) \tag{1}$$

$$s_2 \equiv xc_2+r_2\ (mod\ q) \tag{2}$$

And the extractor can obtain $x \equiv (s_1-s_2)/(c_1-c_2)\ (mod\ q)$. But if the group member selects different random numbers $r_1$, $r_2$ ($r_1 \neq r_2$), the extractor is difficult to calculate $r_1$, $r_2$ based on $t_1$, $t_2$. So $x$ cannot be calculated.

To prove that the zero-knowledge proof is zero-knowledge, construct the following simulator S:

*a)* S randomly selects $t \in \mathbb{C}$ and publishes $t$.

*b)* After getting $c$ from the group manager, S randomly selects $s \leftarrow_R \mathbb{Z}_q$ and calculates $t=h^s/y^c$.

*c)* S publishes the new $t$.

*d)* S will get $c'$ from the group manager and still publish $s$.

Since the group manager will choose different queries $c$, $c'$ ($c' \neq c$) for different $t$, $s$ cannot satisfy the equation $h^s=y^{c'}t$. So simulator S cannot pass the verification without knowing the secret $x$.

*4) The scheme can resist malicious evaluation.*

There may be a malicious evaluation in the scoring process of the subjective questions. The group member may maliciously evaluate the answer intending to influence the final score of the answer. However, the answer record needs to be signed by the group manager before being sent to the full nodes. Group manager can filter malicious comments and notify all group members.

*5) The scheme can resist collusion attack.*

The collusion attack refers to that the malicious nodes in the consortium blockchain unite and try to change the prime-chain and sub-chains. However, the prime-chain is maintained by the full nodes, and the sub-chains are generated according to the prime-chain. Therefore, as long as the full nodes are guaranteed to be honest, the prime-chain and the sub-chains cannot be changed. So the collusion attack caused by the malicious nodes cannot succeed.

### *B. Performance Analysis*

The scheme utilizes a double-layer structure to process the answer records in the consortium blockchain. All the answer records just need to be verified by the group members not all the nodes in the consortium blockchain. And all course groups can verify answer records in their own groups at the same time. It greatly increases the throughput of the consortium blockchain.

In addition, the double-layer structure makes it unnecessary for all nodes in the consortium blockchain to record all answer records. The nodes only need to record the answer records of its own course group. And the storage pressure of sub-chains' nodes can be further reduced by adding the prime-chain's index to the sub-chains. For example, a complete answer record consists of course name, teacher name, student pseudonym, quiz time and score. And a record of sub-chain consists of student pseudonym, score, and its index in the prime-chain, which is similar to the summary of the complete answer record. In Ethereum [7] and LightChain [8], the nodes in the sub-chains need to record the complete answer records. But in this paper, the sub-chains' nodes just need to record the summary of the complete answer records. And the complete answer records are recorded in the prime-chain which is maintained by the full nodes. So the storage pressure of sub-chains' nodes can be effectively reduced.

## IV. Conclusion

In this paper, aiming at the problem that the scoring process is non-transparent, injustice and the final results are easy to be changed, an online quiz scheme based on Double-lay Consortium Blockchain is proposed. The scheme achieves public verification of students' answer and the answer records are recorded in the consortium blockchain, which is public, unchangeable, and traceable. At the same time, group signature is used to protect students' privacy and make the answer records can be traced. In addition, the storage pressure of sub-chains' nodes are effectively reduced by adding the prime-chain's index to the sub-chains.

## Acknowledgment

This work was supported by the Teaching and Research Project of Wuhan University of Technology and the Online Course Construction Project of Wuhan University of Technology.

## References

[1] Wang Chao. Design and Implementation of Young Employees Online Examination System [D]. University of Electronic Science and Technology of China,2016.

[2] Li Yiqiao. Design and Implementation 0f Online Examination System for Bank 0f Jinhua [D]. University of Electronic Science and Technology of China,2016.

[3] Zhu Liehuang, Gao Feng, Shen Meng. Survey on Privacy Preserving Techniques for Blockchain Technology[J]. Journal of Computer Research and Development, 2017,54(10):2170-2186.

[4] Chaum D, Van Heyst E. Group signatures[C]//Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1991: 257-265.

[5] Xie Run. Research on Group Signatures and Their Applications [D]. University of Electronic Science and Technology of China,2016.

[6] Yuan Yong, Wang Feiyue. Blockchain: The State of the Art and Future Trends[J]. Acta Automatica Sinica,2016,42(04):481-494.

[7] Vitalik Buterin. Ethereum 2.0 mauve paper. https://cdn.hackaday.io/files/10879465447136/Mauve%20Paper%20 Vitalik.pdf, 2016.

[8] Jason Jia, Steven Erh, Franklin Weldon. LightChain White Paper. http://www.lightchain.one/pdf/LIGHT_wp_v1.01_en_001.pdf.