Blockchain Frontier Technology (B-Front) **P-ISSN: -**
Vol. 1 No. 1 July 2021 **E-ISSN: -**

A Blockchain Based Online Business Intelligence Learning System

Untung Rahardja[1], Qurotul Aini[2], Alfiah Khoirunisa[3], Ninda Lutfiani[3], Delfi Martika Sari[3]

Faculty Science and Technology, University of Raharja[1,2,3,4,5]
Jl. Jendral Sudirman No. 40, Cikokol, Kec. Tangerang, Kota Tangerang, Banten 15117 Indonesia
e-mail: untung@raharja.info[1], aini@raharja.info[2], alfiah@raharja.info[3], ninda@raharja.info[4], delfi@raharja.info[5]

Author Notification
28 June 2021
Final Revised
02 July 2021
Published
22 July 2021

Untung Rahardja, Qurotul Aini, Alfiah Khoirunisa, Ninda Lutfiani, & Delfi Martika Sari. (2021). A Blockchain Based Online Business Intelligence Learning System. Blockchain Frontier Technology, 1(01), 87–103. Retrieved from

DOI: https://journal.pandawan.id/b-front/article/view/17

Abstract

It isn't an smooth challenge for instructors to test day by day scholar mastering assignments and deliver appropriate grades, attitudes each day. Online mastering structures are nevertheless prone and effortlessly added with the aid of using instructors and gadget managers. Blockchain offers everlasting and dependable garage offerings in addition to computerized calculation offerings. Therefore, the blockchain-primarily based totally on-line mastering gadget proposed on this paper, serves to examine the day by day lives of college students and mechanically their attitudes if you want to relieve instructors from tedious and complicated workloads and may offer sincere and accurate opinions of scholar attitudes. This article uses a qualitative method. Therefore, this text introduces the state of affairs of mastering commercial enterprise intelligence in universities and jobs associated with blockchain-primarily based totally commercial enterprise intelligence mastering structures. Then the gadget is exact withinside the shape and clever contracts.

Keywords*: Education · Blockchain · Smart Contract · Online Learning System*

1. Introduction

Currently, Business Intelligence courses at College use mostly continuous assessments rather than cumulative assessments, which provides teachers with a lot of job evaluation. In contrast to cumulative assessment which only focuses on student learning outcomes, non-stop evaluation is needed to report pupil gaining knowledge of approaches with the aid of using paying near interest to college students and looking at college students whilst they may be gaining knowledge of [1].

The authors introduces 10 non-stop school room evaluation obligations in his 14-week take a look at of the Business Intelligence route for the educational dreams of first-12 months college students [2]. Adopted getting to know portfolio (LP) as a non-stop evaluation device at Sabancı University School of Languages (SL) at Turkey [3]. At the very research screen the efficacy of non-stop evaluation in enhancing college students' abilities, achievements, and check scores. However, troubles do exist withinside the implementation. It is thought through teachers, scholars, and a few college students that it's miles unfair to decide a pupil's expert fulfillment in a very last exam. Because assessing the technique in preference to the end result is extra beneficial in encouraging pupil getting to know [4].

There are students who do their assignments with the help of others or even do plagiarism. In the process of implementing a continuous assessment of the Business

Intelligence course in Higher Education, the authors Have determined the subsequent questions that want to be resolved: . Assignments or different studying substances submitted through college students are piled up in order that they may be tough to shop and inspect; (2) At the stop of the course, a few college students will ask the trainer to extrade their grades for numerous reasons; (3) Most on-line studying structures are vulnerable [5].

As in Figure 1, the emergence of blockchain has supplied extra answers for plenty net packages which include on-line studying systems. Blockchain first existed withinside proposed Bitcoin scheme via way of means of Satoshi Nakamoto in 2008. Blockchain is split into blockchain of public, blockchain of consortium, and personal blockchain, in keeping with permit distribution. In a slender sense, blockchain is a facts shape which includes numerous blocks related via way of means of hash pointers [6].

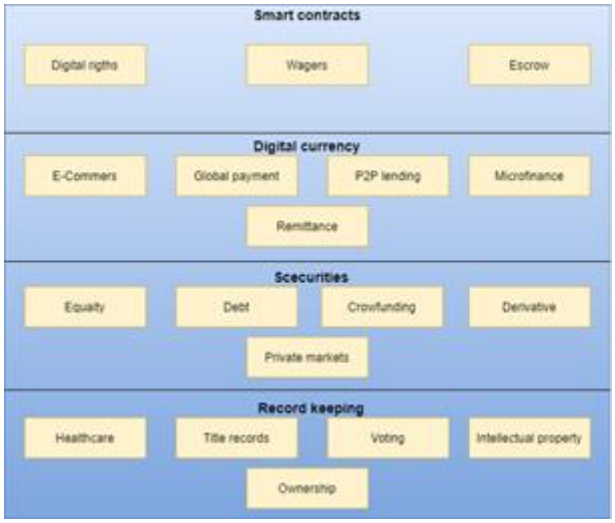

Figure 1. Blockchain applications

The public blockchain was the first blockchain to be proposed. In a public blockchain, each member has the same role as one another. They utilize P2P protocols to communicate, cryptographic strategies to make sure facts resistance to tampering, undeniability and inviolability, in addition to consensus mechanisms to make sure facts consistency [7]. Consortium blockchains are managed by multiple organizations, whereas private blockchains are managed through one organization. These 3 forms of blockchain may also fluctuate in phrases of community structure, verbal exchange protocol, get right of entry to mechanism, consensus mechanism. However the middle standards are the same, namely, statistics is maintained thru a blockchain structure, and consensus is reached amongst numerous identical organizations (besides non-public blockchains) [8]. Smart contracts are a totally essential era in brand new blockchain. A clever agreement is a hard and fast code or script that may be done robotically at the blockchain community whilst the situations are met [9].

For now, the existing online learning system is still vulnerable and easily modified by teachers and system managers [10]. Thus, this article proposes the use of a blockchain-based online learning system. This is because blockchain provides permanent and reliable storage services and automated calculation services.

2. Research Method

In this article, the author makes use of qualitative studies methods. Qualitative research method is a research method that is descriptive and tends to use analysis. This method is used to describe the current process or event that is used as the object of research.

2.1 Literature Review

In the field of education, there are now a number of blockchain-based systems. Possible directions for future deployment and improvement of clever campuses and provide beneficial guidelines. Smart campuses can use blockchain as a device to make sure transparency and security [11]. It may be concluded via way of means of researchers that blockchain may be used to manipulate instructional credentials, virtual rights, and learner results, in addition to enhance on-line studying to be interactive [12]. A complete survey of the approaches blockchain solves the hassle of consider in education, in particular in coping with pupil certification [13]. The effectiveness and significance of blockchain in comparing pupil studying results were cited via way of means of numerous researchers. Possible contribution and effect of mixing facts analytics, synthetic intelligence and blockchain in college education. What is predicted is an excellent machine model, outsourcing a part of the guides and appraisal. Blockchain is powered via way of means of studying analytics that evaluates pupil attitudes with facts evaluation and synthetic intelligence technologies, and the whole machine is powered via way of means of clever contracts from the blockchain. In particular, for a blockchain-based continuous assessment monitoring system [14]. Discusses the effectiveness and importance of implementing a system based on Ethereum [15]. Propose a blockchain-primarily based totally phrase gaining knowledge of version that stocks learner assets with nodes in a blockchain network, worthwhile college students with virtual foreign money and document of gaining knowledge of outcomes [16]. All student learning data is managed and protected easily and reliably by a management system linked to the blockchain. Learning outcomes data and learning data are stored in a management system database provided by the blockchain [17].

Students' learning motivation can improve well with the application of continuous assessment. However, teachers find it difficult to implement and monitor the learning process, especially with classes that have many students [18]. This research is about online learning system by considering continuous assessment. Therefore, a blockchain-primarily based totally on-line Business Intelligence gaining knowledge of device is proposed, which capabilities to display the every day gaining knowledge of of college students and robotically evaluates their attitudes with a view to relieve instructors from tedious and complicated workloads and might offer sincere and correct evaluations of students' attitudes. Its main contributions are:

1. First, introduce the situation and problems of the Business Intelligence learning system used by universities.
2. Second, to automatically record and evaluate student performance, A blockchain-primarily based totally on-line gaining knowledge of machine is used to attain openness, transparency, and absolute belief.
3. Third, each student is given an identity so that it can be recorded and evaluated authentically via a sure period, commonly withinside the shape of semesters, in order that plagiarism could be removed to a minimal and the load on instructors could be decreased properly.
4. Finally, this paper info the clever settlement layout and overall performance evaluation with the author's implementation.

2.2 Blockchain

Blockchain first existed withinside the Bitcoin scheme proposed via way of means of Satoshi Nakamoto in 2008. As a virtual forex with out a relied on center. Bitcoins must attain a certain state amongst nodes that each other attends. Otherwise, errors will occur in this digital currency ledger making it untrustworthy and useless. In addition, each account must be secure sufficient to shield consumer belongings and make sure transactions and messages inside this community can't be modified and refuted [19]. Therefore, P2P protocols are implemented to communicate, cryptographic strategies to make sure information resistance to tampering, no refutation and inviolability, in addition to consensus mechanisms to make sure information consistency [20]. A special blockchain structure is adopted to enhance the security of the stored data. Any modification will cause an error because the data block is concatenated with the hash pointer. It is very expensive to modify data illegally, and it can compromise now no longer handiest the goal statistics, however additionally all of the blocks that could have an effect on the goal statistics having to be modified. Moreover, with the goal statistics being sponsored up

on all nodes network, an attacker could should regulate extra than 1/2 of of the nodes for the data modifications performed on the bitcoin network to succeed. The magnitude of the cost for data modification is almost impossible [21].

It ought to be referred to that a easy script to check whether or not a transaction meets sure situations can run withinside system of bitcoin. The improvement of bitcoin drew people's interest to technology of blockchain, that could remedy the trouble of agree with withinside the network. Implementing clever contracts at the blockchain makes credible and mechanically carried out contracts a reality.

2.3 Smart Contract

Today smart contracts are a completely crucial era in blockchain. A clever settlement is a hard and fast of code or script that may be finished robotically at the blockchain community while situations are met. For a appropriate fee, builders can set up clever contracts at the Ethereum public chain. Developers also can construct non-public or shared Ethereum networks and set up clever contracts on pinnacle of them. Ethereum is one of the consultant blockchain systems with clever settlement capability withinside the public chains [22]. In the consortium chain, one in every of the maximum consultant systems is Hyperledger Fabric [23]. Smart contracts in Fabric are referred to as chaincode, and are written withinside the current Turing-whole language [24].

Chaincode gives kingdom processing good judgment primarily based totally on dispensed blockchain ledgers. In Fabric, chaincode runs at the box dock via way of means of default. Peers create and run chaincode bins via way of means of calling the Application Programming Interface (API). After the chaincode box runs, friends set up a gRPC (delivery layer protocol) connection. The chaincode box makes use of the interface supplied via way of means of the core.chaincode.shim bundle to provoke requests to Peers that are entities withinside the Fabric network [25].

2.4 Hyperledger fabric

Hyperledger Fabric includes 3 essential sorts of community entities, particularly clients, friends and orderers. In addition to those 3 member types, The Fabric community additionally has numerous specialised gear inclusive of Zookeeper and Certificate Authority (CA). ZooKeeper is a software program software that offers consensus services for disbursed application [26].

1. Clients: packages that ship transactions to the community on behalf of the user.
2. Peers: entity that transmit transactions and hold general ledger status. Committed peers receive the resulting block of transactions. To support peers generate digital signature transaction responses after verifying transactions from clients.
3. Orderers: entities that create a shared verbal exchange channel among customers and peers, and bundle blockchain transactions and ship to their colleagues.

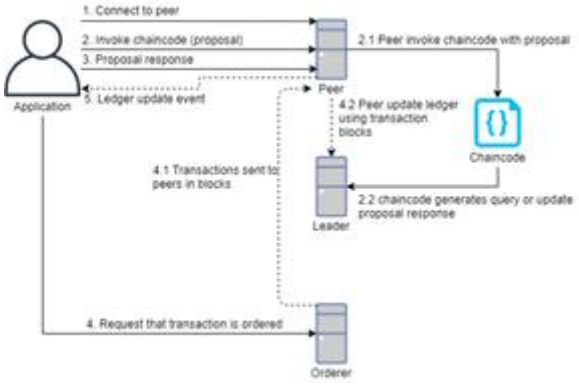

Figure 2. Fabric flowchart

Fabric executes transactions before they are sequenced, in contrast to Bitcoin and Ethereum that sort before executing the transaction. To support transactions, Fabric requires multiple nodes, which were defined in the previous support strategy. For each transaction across the network, only the predefined support nodes are required. This enables parallel processing and machine overall performance and improves scalability. Meantime, the hassle of non-deterministic transactions such as Bitcoin structures could be resolved, as inconsistent consequences will consequently be filtered earlier than being sorted [27].

Applications can be considered as clients. In Fabric applications to access ledgers and chaincode can be via peers. The SDK (Software Development Kit) supplied with the aid of using Fabric can permit packages to hook up with friends, name chaincode to generate transactions, ship transaction throughout the network, and acquire occasions generated at some stage in processing [28]. The procedure of getting access to the overall ledger thru friends is proven in Fig. 2, in which the ledger refers back to the modern grasp node at the blockchain.The strides for querying the general ledger can be explained as follows:

Stride 1: Connect the app with peers.
Stride 2: The application generates a proposal and sends it to peers.
Stride 2.1: Peers will call the appropriate chaincode to run according to the proposal.
Stride 2.2: Chaincode queries the ledger regarding suitability of the proposal
Stride 3: Return the proposal responses to the application. At this point, the general ledger query has been finished.

The asset transaction method at the blockchain wishes to replace the ledger at the blockchain. The transactions process can be seen in Fig. 2. The author will reintroduce the flow from the first stride so that users can understand the general ledger update easily. To replace the ledger, the subsequent strides want to be completed:

Stride 1: Applications begin a transaction.
Stride 2: Support peers to verify signatures and execute transactions. Peers call the appropriate chaincode to run with the proposal.
Stride 3: Supporting peers turn back “proposal responses” with their signature to the software.
Stride 4: The software verifies the signature and compares the suggestion responses to decide if the suggestion responses are the same. The software generate transaction moves primarily based totally at the outcomes lower back from the question and sends them to the order.
Stride 4.1 : Orders receive transactions from across the network, and create blocks. Then send block orders to all colleagues in the network.
Stride 4.2 : Peers validate transactions inside the block and mark transactions as legitimate or invalid. Then friends upload blocks to the chain and replace in ledger.
Stride 5: Once the ledger replace is complete, a notification is generated to inform the app that the transaction become confirmed or not.

Basically the application still makes chaincode calls through connected peers for ledger updates, unlike query ledgers, ledger updates require consensus with different friends. Therefore, the Orderer is needed to ship transaction proposals to all friends at some point of the network. Each peer will determine from his/her personal angle whether or not to just take delivery of or decline the transaction inspiration upon acquiring it. Since the entire method is time consuming, the app receives a misaligned notification while the entire method is finished [29].

In the consortium blockchain, the identification of the consumer may be identified, and now no longer counting on the mechanism of PoW, numerous low-electricity consensus mechanisms may be adopted. In particular, Fabric is enormously modular, and factor-to-factor protocols, consensus protocols, help and verification strategies, databases, and member control offerings are all interchangeable and extensible.

2.5 Proposed Framework

As Figure 3 shows, the gadget includes four layers, specifically utility layer, clever agreement layer, blockchain layer, and server layer. The utility layer encapsulates the numerous offerings supplied via way of means of the clever agreement and server layers.

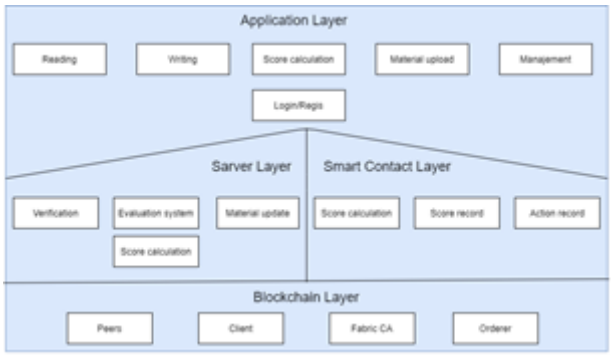

Figure 3.System overview

The services that divided by the target, in this learning system is shown in Figure 4. In addition to ask for the data, the 3 main functions of the layers of clever contract is: record student attitudes, counting the end grades, and record grades. The server layer is the primary a part of the getting to know machine and its features consist of dealing with users, verifying message signatures, dealing with getting to know materials, calculating grades, printing pupil assignments, and so on. Server layers for custom evaluation systems and learning materials management systems are not the point of this paper, so they will not be discussed in depth. Blockchain layer is a Fabric community carried out through numerous universities[30].

As shown in the flow system diagram (Fig. 5), data flows among 5 parties: students, faculty, blockchain, evaluation system, and server. Blockchain transparency can result in leakage of student privacy. To protect it, the blockchain records aliases not as student information. The main stream in the proposed system are shown in Fig. 5. Teachers need to register tags at the server side and notify students of tags in several ways,which include verbal notifications, sending emails, and so on. The gadget generates aliases primarily based totally on current pupil information. Each teaching fabric has a completely unique number. After becoming evaluated through the system, students' attitudes and learning values will now recorded on blockchain along by aliases and material numbers. The instructor can add gaining knowledge of substances to the server. The instructors and college students can look for grades or scholar mind-set statistics withinside the blockchain and instructors also can practice for scholar overall performance completion.

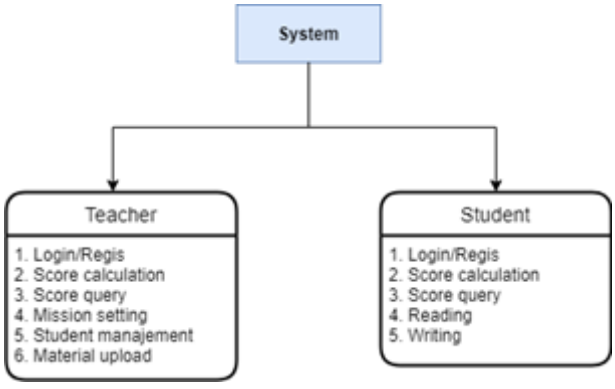

Figure 4. Requirements for roles

We can use sequence diagrams to represent flow of the system (Fig. 6), that smart contract layer, in this case system provides four functions, namely: recording student learning attitudes, calculating student final grades, recording student grades, and query scores.

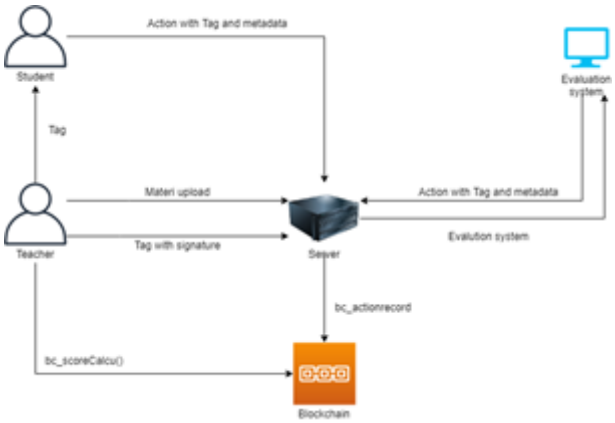

Figure 5. Flowchart

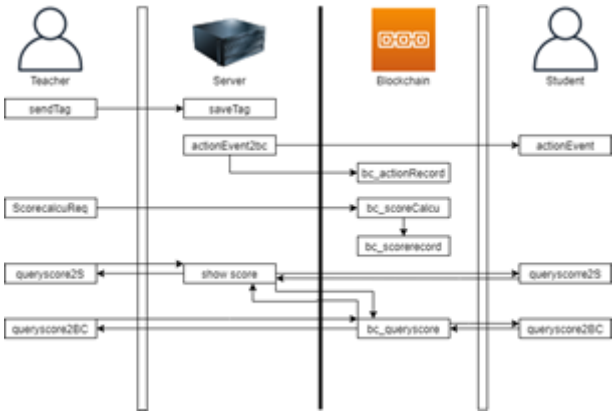

Figure 6.Sequence diagram

3. Results and Discussion

In this section, the author analyzes the profits of the proposed device in this newsletter of the system framework, privacy protection, and system security. Furthermore, the authors utilize a threat models to be analyzed student value protection and student privacy in this schema.

3.1 System Framework

The proposed gadget is split into 4 layers. The blockchain coating of this gadget is the Fabric community, and the community shape is in keeping with the needs of a couple of coaching agencies to supervise the calculation and recording of grades simultaneously. In this shape, the feature of the gadget may be stepped forward and improved properly. In particular, person management, provider provision, and task assessment on this gadget are solved through the server, and mindset logs, price calculations, and garage with agree with problems are solved through blockchain. In different words, the offerings furnished through the software layer may be effortlessly carried out on mobile, internet and different platforms, and customers do now no longer want to shop facts as blockchain members. At the identical time, person authentication and exact get entry to manage to the gadget may be carried out thru the server layer, with out including any extra overhead to the blockchain. As an impartial gadget, the assessment gadget may be connected to Artificial Intelligence (AI) furnished through different

companies, thereby lowering the problem in growing the gadget.

3.2 System Security

In phrases of blockchain community security, Fabric is a 51% attack-unfastened consistent with assignment blockchain, a couple of Byzantine fault-tolerant consensus mechanisms that may be used to resist Byzantine attacks, and a low danger of malicious amendment of community configurations or unlawful uploads of malware code.

Permitted blockchains are constructed amongst a set of known, identified, and often censored nodes. These nodes perform beneathneath a governance version and generate a sure stage of agree with. A permissioned blockchain protects inferences made via way of means of a set of entities, that have the identical aim however won't completely agree with every other. Licensed blockchains can use the Byzantine Fault Tolerance (BFT) or Crash Fault Tolerance (CFT) consensus protocols, which do now no longer require pricey mining. No mining, so no attack 51%.

The nodes understand every different and all movements are recorded at the blockchain, along with sending software transactions, converting community configurations, or imposing clever contracts. Therefore, there's a low threat of malicious amendment of the community configuration or unlawful add of malicious code.

In phrases of records security, virtual signatures make sure that messages withinside the gadget can not be tampered with, solid or rejected; the hash pointer withinside the block makes it tough to extrade the preceding content; phrase is heard, that the protocols at the Fabric community can restore defective records at the nodes. The collision-resistant hash characteristic and the hash end result can be one of a kind if the authentic textual content is changed, making it very tough to adjust the blockchain content.

In phrases of conversation security, this gadget makes use of a steady encrypted conversation protocol (HTTPS). Web security, assessment gadget security, and server security, are past the scope of this article.

The gadget proposed in this newsletter can properly remedy the demanding situations in non-stop assessment: (1) hard responsibilities are saved and checked; (2) the trainer can extrade the value; (3) the vulnerability of on line mastering systems. Responding to the 3 troubles above, this gadget has the subsequent advantages.

1. Storage and evaluation: evaluating data system sent by the students and notes the value on the blockchain from storing the student attitude data.
2. Damage check: blockchain stores student grades for every lesson attitude, calculating the end of the day grades, and shop grades, what makes it difficult for teachers or attackers to change student grades.
3. Security system: The blockchain itself makes the complete machine stronger, and the cryptographic set of rules guarantees the safety of communication, records safety, and safety of machine behavior.

3.3 Privacy Protection

The data on the blockchain must be transparent to ensure mutual control between multiple educational institutions. In this case, the privacy of students is at risk. In reaction to this contradiction, this paper developed a pseudonym mechanism, which assigns pseudonyms to users at specific points in the training process and uses pseudonyms To document person statistics withinside the blockchain. The student aliases is associated with their current instructor, and the teacher needs to provide some information to calculate the alias. Only the teacher knows the correct connection between the pseudonym of the student and his true identity. And the problematic gadget It is tough for different instructional establishments or instructors to use pseudonyms on the blockchain to discover the true identities of students.

3.4 Future Analysis

In order to higher examine the privateness protections supplied with the aid of using the

author's software and the safety of pupil grades, the authors outline a danger version and offer an evaluation of the version. The sensible assumptions of the author's danger version are as follows:

1. Both private terminal or server is not dangerous, but they can be attacked;
2. The hash function used is secure and trouble;
3. The virtual signature set of rules used is secure, and the signature can't be solid or rejected with out revealing the non-public key. In different words, the enemy can't impersonate the user;
4. The communique protocol followed is steady and might offer communique privateness protection;
5. There aren't anyt any loopholes withinside the chaincode, and the packages at the blockchain may be achieved properly.
6. Blockchain network can remain secure.

The enemy can be an arbitrary 1/3 party. Based on the assumption (2), (3) and (4), there is may be no want to fear approximately facts leakage throughout the communique process. At the equal time, there may be no want to fear that the aliases posted at the blockchain will be deciphered via way of means of adversaries seeking to get preserve of the scholar's identity. Based on assumption (5) and assumption (6), as soon as the statistics is saved at the blockchain, the statistics can't be destructed. Combining the conclusions from the above elements and the assumption (1), we will speculate that the adversary can best reap the purpose of acquiring scholar privateness statistics or changing grades via way of means of attacking servers and terminal equipment.

On change whether get a certain student's personal score, the enemy can perform the next attack

1. Attacks the server and sends mindset statistics with changed values to the blockchain.
2. Attacks the assessment machine to ship fake outcomes to the server.
3. The attacker broke into the database server and assigned aliases to the students.
4. Attack the server and get the public server and private key.
5. Attack the teacher terminal and get the instructor's public server and personal key.
6. Attackers invade The database server to reap correspondence among instructors and tags, and correspondence among college students and tags.

For attacks (1) and (2), if the enemy is currently on top of things of the server or assessment system, then best the value of the task sent in a short time may be modified, which has little impact at the very last standard score. Consequently, the effectual modification of the last value requires server control or long-range evaluation system that is illegal. In traditional online learning systems, adversaries can change user values by gaining on-the-fly authority. Long-term illegal controls are harder than short term illegal controls. Compared to conventional schemes, harder to adversaries to change values in the blockchain-based schemes proposed in this article.

The mixture of attacks (3), (4), and (6) in addition to the mixture of attacks (5) and (6) can attain the identical effect, that's to acquire a correspondence among college students and aliases. However, neither of those combos will reach acquiring the consumer's private facts or the correspondence among the pupil alias and the pupil identity, even though they are able to release a a success assault due to the fact the hash characteristic utilized by the device wishes to be dismantled. Despite the issue of the assault, enemies can certainly benefit privateness beneathneath those situations for a fee. However, maximum aliasing mechanisms can not hold to shield consumer-figuring out facts while essential public and personal keys are revealed. Therefore, if you want to hold consumer privateness, essential public and personal keys need to now no longer be leaked.

3.5 Research Implementation

In this section, the main parts of the author's system implementation will be explained. Some of the notation is sum up in Table 1. The server and user communicate using an encrypted protocol transmission, such as HyperText Transfer Protocol over Secure Socket Layer (HTTPS).

Continuous assessment usually divides academic achievement into two parts, namely very last examination ratings and each day ratings. Daily grades are obtained based on Students' overall performance in their independent learning and The great in their assignments. In the Business Intelligence course in Higher Education, students are asked to do self-study every day, in the form of reading, and writing, these two components are the basis of students' overall skills. Daily assignments can be chosen by the student.

kpb∗	Public key*
kpv∗	Private key*
ID∗	ID Participant*
aID∗	ID name*
MIDi	ID i
pMi	Property i
E∗()	Encryption*
S∗()	content*
H()	hash, H: {0, 1}∗ → Z∗q
Ack	deskripsi tindakan pembelajaran
T	timestamp

Table 1. Notations

Assignments are a few unique gaining knowledge of substances or sports of their textbooks. This article makes a speciality of non-stop recording and very last agreement of every

day values. According to the composition of every day grades, instructors need to be capable of decide positive assignments once they entire students' every day grades. When the homework fabric assigned via way of means of the instructor isn't always withinside the gaining knowledge of system, the instructor is needed to actively add gaining knowledge of substances.

In this system, all teaching substances have precise numbers and attributes. The attributes are analyzing, and writing in every day assignments, in addition to analyzing and writing given with the aid of using the teacher.

3.5.1 Aliases Creation Method

The trainer sends a sign the tag (any character string) to the server and register the tag on the server. Instructors can tell college students approximately those tags in any form, which include verbal notifications, sending emails, and so on. Students want to feature this tag to non-public records withinside the system. As gaining knowledge of progresses, gaining knowledge of records is despatched to the server along side the pupil ID, tag and signature of all messages.

After verifying the signature, the server retrieves withinside the nearby database whether or not a pupil aID that fits the hash of the pupil ID, personal server key, and tag, H(kpvserver, pupil ID, Tag), exists. If there is, the studying technique is recorded at the blockchain beneathneath this alias. If the alias does now no longer exist, the server wishes to ship an aliases registration request to the trainer that fits the tag. The aliases registration request consists of an encrypted pupil ID and tag.

Since receiving a registration request from a server alias, teachers decrypt the request to obtain the ID and tag students. Then, teachers need to re-encrypt the student ID and mark it with a private key and a public key server teacher, then send Ekpbserver (TeacherEkpv (student ID, Tag)) to the server.

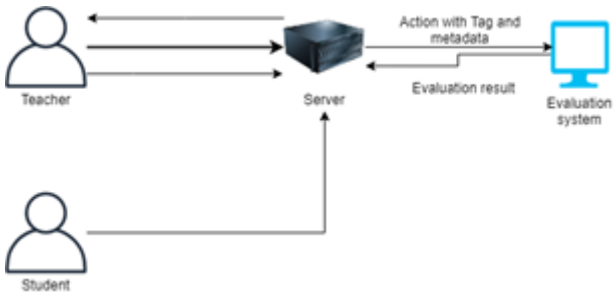

Figure 7. Flowchart of the aliases generation method

The server makes use of the personal key to decrypt the message to get the trainer Exp(Student ID, Tag). The server makes use of the encrypted records despatched via way of means of the trainer to calculate pupil aliases. After that the server will keep the correspondence of aIDsiswa and H (kpvserver, pupil ID, Tag) in its nearby database. Students' attitudes and grades below the modern-day tag are sure to the alias. The alias technology module information waft is illustrated in Figure 7. The distinct strides are as follows:

Stride 1: The instructor Send a request to register a label to sign up a selected tag (any character string) at the server. The request is tag, Skpvpengajar (Tag).

Stride 2: Since verifying the identification of the trainer and signature correctness, server exams if the tag is a replica of the nearby tag used. If there are duplicates, registration request was rejected and the trainer is reminded to extrade the tag, and stride 1 is repeated. Otherwise, the correspondence among the tag and the trainer ID, and the tag may be saved at the nearby server.

Stride 3: If a student completed the task, his attitude statistics may be despatched to the server with the student ID, current tag he has, timestamp, learning material ID, and signature of all messages, i.e. student ID, Tag , Ack, MIDi, T, Skpvsiswa (Student ID, Tag, Ack, MIDi, T).

Stride 4: After verifying the scholar's identification and signature correctness, the server will fetch withinside the neighborhood database whether or not the tag exists. If there is, stride five

may be performed. Otherwise, mission submission fails and the scholar may be reminded to extrade the tag in his message.
Stride 5: The server retrieves withinside the nearby database whether or not the scholar alias aID that fits the hash of the scholar ID, non-public server key and tag, H(kpvserver,studentID, Tag), exists. If there is, stride nine can be performed. Otherwise, stride 6 is performed.
Stride 6: Server sends aliases registration request to the trainer matching the tag. The alias registration request consists of the scholar ID and tag which desires to be encrypted with a personal server key after which encrypted with the trainer's public key, particularly Ekpbpengajar (Ekpvserver(StudentID, Tag)).
Stride 7: Since receiving an aliases registration request from the server, the instrucot decrypts the request to get the student ID and tag. Then, teachers need to encrypt your student ID and mark it with a private key and a public key server teacher, then send an encrypted message to a server, which Ekpbserver (Ekpvteacher (student ID, Tag)).
Stride 8: Server uses private key to decrypt message in order got the teacher Exp (student ID, Tag). Then, the server counts H (Ekpvpengajar (student ID, Tag)) as a student alias on the server and blockchain, namely aIDsiswa = H (Ekpvpengajar (student ID, Tag)). Then, the server will save the correspondence of aIDsiswa and H (kpvserver, student ID, Tag) in the local database.
Stride 9: The server calls the assessment gadget to assess the student's attitude, then facts it with the blockchain.

3.5.2 Action record

When a getting to know movement occurs, Tag, Ack, MIDi, T, Student ID (StudentID, Tag, Ack, MIDi, T) are despatched to the server. When a scholar alias is taken, the getting to know attitude (Ack, MIDi, pMi, aIDsiswa) is despatched to the assessment machine. The assessment machine presents value. After server receives the value, it then calls the actionRecord_bc() interface from blockchain to document the getting to know movement. Specifically, the parameters required with the aid of using bc_action Record() are actionID, scholar aID, MIDi, pMi, T, value, Sserver(aIDstudent, MIDi, pMi, T, value). It have to be cited that actionID is the ID of this movement, that's received with the aid of using concatenating strings: actionID = aIDstudent + T. actionRecord_bc() is precise in Algorithm_1.

3.5.3 Value Calculation

Anyone can submit a request to the values calculated Blockchain, however he desires to understand the aliases of students in The server and blockchain. The correspondence among the pupil ID and aliases is known only to the instructor and server. Students can check their grades through aliases furnished with the aid of using the server, and the server handiest provides their aliases to the student. Since the daily grade consists of the daily assignment grade and the grade Assigned with the aid of using the teacher, the grade calculation technique need to be:

Algorithm_1
actionRecord_bc (actionID, student aID, MIDi, pMi, T, grade, Sserver(student aID, MIDi, pMi, T, grade), status) Input: ID of an action, the action ID; Student alias, aIDstudent ; Learning material ID numbered i, MIDi ; learning material property numbered i, pMi ; Timestamp of current action, T; The value of the assignment is given via way of means of the assessment system, grades; signed message, Sserver(aIDstudent, MIDi, pMi, T , value);
Output: Status of this function if executed successfully, status;
1: Ask if actionID already exists withinside the ledger;
2: If there is then submitted mistake actionID;
3: end if
4: Create an movement object;
5: Convert enter content material to JSON format;
6: Write in the ledger;
7: Turn back status;

Diurnal value = Array Ratio 1[0] (Array Ratio2[] Array Grade1[]) + ArrayRatio1[1] (ArrayRatio3[] ArrayGrade2[]).The instructor-described ratios 1, 2, and three are arrays of 3 decimal places, and the sum of every array is identical to 1. The instructor-described ratio 1, ArrayRatio_1[], is the share of the instructor's task and students' day by day exercise withinside the overall day by day grade. The instructor-described ratio of 2, ArrayRatio2[], is the share of every project grade assigned through the instructor withinside the very last grade of the project. The instructor-described ratio of 3, ArrayRatio3[], is the share of students' day by day exercise ratings for every form of homework withinside the very last day by day exercise score. ArrayGrade1[] is an array fee that corresponds to the project given through the instructor. ArrayGrade1[] is a fixed of values that corresponds to a student's day by day exercise. ArrayRatio2[] · ArrayGrade1[] manner the dot made of arrays ArrayRatio_2[] and ArrayGrade_1[].

It ought to be mentioned that, if the homework given through the trainer isn't withinside the database server, the trainer can add their personal studying materials. When checking the results, customers want to signify the share and content material of the day by day value. In this system-precise implementation, arrays of endless period are changed with strings.

To calculate a student's daily final grade, we want to realize the 3 array ratios determined by the instructor, aliases student, the ID of the learning material array provided by the teacher, the daily practice period, and the number of arrays of teaching materials that the teacher needs to share teaching materials.

Aliases are used to retrieve student attitudes which are recorded on the blockchain. To differentiate tasks given through the instructor and the students' exercise assignments, the ID of the studying substances furnished through the instructor is compiled. The validity duration of the each day workout is used to clear out out notes in needless time. The daily practice questions prepared by the teacher have different requirements for the quantity of teaching materials with different properties, so it is necessary to "arrange the amount of learning materials needed by the teacher". scoreCalcu_bc() details in Algorithm_2.

Algorithm 2 scoreCalcu bc(aIDstudent, ArrayRatio_1[], ArrayRatio_2[], ArrayRatio_3[], TeacherAssigment[], period, MaterialRequirements[], value)

Input: Student aliases, aIDsiswa ; Proportion of coaching assignments and students' day by day exercise in overall day by day grades, ArrayRatio1[]; The share of every task grade assigned through the instructor withinside the very last grade, ArrayRatio2[]; The share of students' day by day exercise ratings for every form of homework withinside the very last day by day exercise score, ArrayRatio3[]; The association of the gaining knowledge of cloth IDs given through the instructor, TeacherAssignment[]; Valid time of day by day exercise, period; The composition of the amount of gaining knowledge of substances required through the instructor for distinct homes of gaining knowledge of substances, MaterialRequirements[];

Output: The very last day by day grade of pupil alias is aIDsiswa , grade;

1. Find all of the movement facts owned through aIDsiswa, and save it in actionArray1[];
2. By duration, delete movements in actionArray1[] which might be not valid. Then we get actionArray2[];
3. According to the recorded MIDI in TeacherAssignment [] array actionArray_2 [] divided into actionArrayTea[] and actionArrayDai[]. The order of actions from the actionTeaArray[] array must match the order recorded by the TeacherAssignment[] array. If the user has no active records for a particular MIDi, the action with a value of 0 is replaced;
4. ArrayGrade_1 [] suddenly stand up of the value of the action in action Array [];
5. According to one-of-a-kind pMi, the actionDaiArray[] array is split into 2 arrays, specifically actionRead[], actionWrite[]. Then reset and moves withinside the arrays in line with the values, biggest to smallest;
2. According to the amount requirement, okay, of the written physical games recorded withinside the Material Requirements[] array, take the pinnacle okay moves withinside the actionWrite[] array, calculate the common fee. If the quantity of moves is much less than okay, the moves with a fee of zero are used till the specified quantity is met. Then document the common fee as score_write. Using the equal operation, we will get the common fee of different studying materials. All those values shape the array ArrayGrade2[];

3. Count value = ArrayRatio1[0] (ArrayRatio2[] ArrayGrade1[]) + ArrayRatio1[1] (ArrayRatio3[] ArrayGrade2[]); return value;

3.5.4 Value Recording

Logging the resolved value on the blockchain can save you customers from often recalculating the value as the safety and reliability of the value records registered on the blockchain has substantially improved. The facts to be recorded is aIDsiswa, grade, period, T. It must be cited that the ID value is the ID of this every day value, which may be calculated with H (aIDsiswa).

It ought to be mentioned that checking whether or not the timestamp exceeds the time restrict set with the aid of using the instructor earlier than recording the grade. The timeout is described with the aid of using the period, that's a parameter of the fee calculation set of rules in phase 4.3. When the fee counting set of rules calls the fee log set of rules, it passes the parameters to the fee log set of rules. scoreRecord_bc() is particular in Algorithm_3.

Algorithm_3

scoreRecord_bc(valueID, period, student aID, grade, T, state)

Input: daily value ID, value ID; Valid timeframe for daily exercise, period; Student alias, aIDsiswa; Student daily grades, grades; Timestamp value, T;

Output: Status of this function if executed successfully, status;

1. Calculate ID value, ID value = H (student aID);
2. Ask if IDvalue, already on the ledger;
3. if ID value there then;
4. Reading and converting records on blockchain in JSON format;
5. if the period is equal to the record on blockchain then turn back status;
6. end if
7. Update values and period;
8. Write gradeID, student aID, grade, period, T in ledger;
9. turn back status;
10. end if
11. If the timestamp has now no longer reached the give up of the period, ERROR is returned;
12. end if
13. Create an movement object;
14. Convert enter content material to JSON format;
15. Write in ledger;
16. turn back status;

4. Conclusion

With the existing online learning system, it is still vulnerable and easily modified by teachers and system managers. Therefore, the author proposes an online blockchain business intelligence learning system that functions to monitor students every day learning and automatically evaluates their attitudes so that they can relieve boring teacher workloads and can provide honest and correct evaluations of students' attitudes. The author has designed a system structure with four layers, details the statistics float and some of the key algorithms withinside the system.

After the author analyzes the system advantages proposed in this article, implements smart contracts, and proves its availability. To modify the data illegally would be costly and it would also harm the targeted data. Because the blockchain-based online learning system has good security plus it uses smart contracts and alias methods.

In the future, the author Will attempt to enhance the device proposed in this article by implementing multiple servers at the layer that are gaining knowledge of machine servers and friends withinside the blockchain network.

Process	Execution time
Connection	310.423 ms
Initialization	260.396 ms
bc_actionRecord()	2184.000 ms
bc_scoreCalcu()	2189.745 ms
bc_scoreRecord()	2182.372 ms
Query	14.252 ms

Table 2. Test result

References

[1] S. Kugamoorthy and S. Weerakoon, “Continuous Assessment Methods: Critical review for quality improvement of the Postgraduate Diploma in Education Programme of the Open University Sri Lanka,” *Int. Res. J. Hum. Soc. Sci.*, vol. 5, no. 10, 2018.

[2] J. Ma, “Hong Kong college students’ perceptions of continuous assessment in the context of academic literacy instruction,” in *English literacy instruction for Chinese speakers*, Springer, 2019, pp. 265–280.

[3] E. G. Alayafi and P. Gunduz, “An essential tool for continuous assessment: The learning portfolio,” in *Revisiting EFL assessment*, Springer, 2017, pp. 237–259.

[4] E. Guustaaf, U. Rahardja, Q. Aini, H. W. Maharani, and N. A. Santoso, “Blockchain-based Education Project,” *Aptisi Trans. Manag.*, vol. 5, no. 1, pp. 46–61, 2021.

[5] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, “A review on consensus algorithm of blockchain,” in *2017 IEEE international conference on systems, man, and cybernetics (SMC)*, 2017, pp. 2567–2572.

[6] U. Rahardja, Q. Aini, Y. I. Graha, and M. R. Tangkaw, “Gamification Framework Design of Management Education and Development in Industrial Revolution 4.0,” in *Journal of Physics: Conference Series*, 2019, vol. 1364, no. 1, p. 12035.

[7] A. C. Nugraha, “Penerapan Teknologi Blockchain dalam Lingkungan Pendidikan: Studi Kasus Jurusan Teknik Komputer dan Informatika POLBAN,” *Produktif J. Ilm. Pendidik. Teknol. Inf.*, vol. 4, no. 1, pp. 15–20, 2020.

[8] U. Rahardja, Q. Aini, M. D. A. Ngadi, M. Hardini, and F. P. Oganda, “The Blockchain Manifesto,” in *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2020, pp. 1–5.

[9] T. M. Fernández-Caramés and P. Fraga-Lamas, “Towards next generation teaching, learning, and context-aware applications for higher education: A review on blockchain, IoT, fog and edge computing enabled smart campuses and universities,” *Appl. Sci.*, vol. 9, no. 21, p. 4479, 2019.
[10] S. Sudaryono, Q. Aini, N. Lutfiani, F. Hanafi, and U. Rahardja, “Application of Blockchain Technology for iLearning Student Assessment,” *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 14, no. 2, pp. 209–218, 2020.
[11] M. Hardini, Q. Aini, U. Rahardja, R. D. Izzaty, and A. Faturahman, “Ontology of Education Using Blockchain: Time Based Protocol,” in *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2020, pp. 1–5.
[12] J. Zhong, H. Xie, D. Zou, and D. K. W. Chui, “A blockchain model for word-learning systems,” in *2018 5th International Conference on Behavioral, Economic, and Socio-Cultural Computing (BESC)*, 2018, pp. 130–131.
[13] A. Grech and A. F. Camilleri, *Blockchain in education*. Luxembourg: Publications Office of the European Union, 2017.
[14] P. Williams, “Does competency-based education with blockchain signal a new mission for universities?,” *J. High. Educ. policy Manag.*, vol. 41, no. 1, pp. 104–117, 2019.
[15] G. Wood, “Ethereum: a secure decentralised generalised transaction ledger (2014).” 2017.
[16] P. A. Sunarya, U. Rahardja, L. Sunarya, and M. Hardini, “The Role Of Blockchain As A Security Support For Student Profiles In Technology Education Systems,” *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 4, no. 2, pp. 203–207, 2020.
[17] P. Ocheja, B. Flanagan, and H. Ogata, “Connecting decentralized learning records: a blockchain based learning analytics platform,” in *Proceedings of the 8th international conference on learning analytics and knowledge*, 2018, pp. 265–269.
[18] Q. Aini, U. Rahardja, and A. Khoirunisa, “Blockchain Technology into Gamification on Education,” *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 14, no. 2, pp. 147–158, 2020.
[19] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, “The blockchain as a decentralized security framework [future directions],” *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18–21, 2018.
[20] R. M. H. Thamrin, E. P. Harahap, A. Khoirunisa, A. Faturahman, and K. Zelina, “Blockchain-based Land Certificate Management in Indonesia,” *ADI J. Recent Innov.*, vol. 2, no. 2, pp. 232–252, 2021.
[21] A. Bogner, M. Chanson, and A. Meeuw, “A decentralised sharing app running a smart contract on the ethereum blockchain,” in *Proceedings of the 6th International Conference on the Internet of Things*, 2016, pp. 177–178.
[22] E. Androulaki *et al.*, “et almbox. 2018a. Hyperledger Fabric: a distributed operating system for permissioned blockchains,” in *European Conf. on Computer Systems (EuroSys). ACM*, vol. 30.
[23] A. A. A. Donovan and B. W. Kernighan, *The Go programming language*. Addison-Wesley Professional, 2015.
[24] D. Lizcano, J. A. Lara, B. White, and S. Aljawarneh, “Blockchain-based approach to create a model of trust in open and ubiquitous higher education,” *J. Comput. High. Educ.*, vol. 32, no. 1, pp. 109–134, 2020.
[25] Q. Aini, U. Rahardja, N. P. L. Santoso, and A. Oktariyani, “Aplikasi Berbasis Blockchain dalam Dunia Pendidikan dengan Metode Systematics Review,” *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 6, no. 1, pp. 58–66, 2021.
[26] Z. Fauziah, H. Latifah, X. Omar, A. Khoirunisa, and S. Millah, “Application of Blockchain Technology in Smart Contracts: A Systematic Literature Review,” *Aptisi Trans. Technopreneursh.*, vol. 2, no. 2, pp. 160–166, 2020.
[27] C. Dannen, *Introducing Ethereum and solidity*, vol. 318. Springer, 2017.
[28] S. S. Oyelere, L. Tomczyk, N. Bouali, and F. J. Agbo, “Blockchain technology and gamification-conditions and opportunities for education,” *Adult Educ. 2018-Transformation Era Digit. Artif. Intell.*, 2019.

[29] S. Kosasi, "Karakteristik Blockchain Teknologi Dalam Pengembangan Edukasi," *ADI Bisnis Digit. Interdisiplin J*, vol. 1, no. 1, pp. 87–94, 2020.