International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

An Unimpeachable System for Providing Credit Scores using Blockchain in Educational Institutions

Kalpana Devi S, Bitra Sainadh, Hariharan K, Hemanth T

Abstract: ***Ensuring security in every aspect of transactions the primary task of today's world. Blockchain Technology is used to ensure that digital assets cannot be modified and are transparent by using decentralized hashing techniques. In today's world, Higher Educational Institutions are competing with others by means of accreditation. As a part of this process, the best outgoing student is awarded based on his/her performance throughout the four years attributed to academics, co-curricular and extra-curricular activities. The proposed system is a multifaceted application which works on the basis of providing credits. This system is implemented using Blockchain so that a ledger is distributed among all the users connected in the network, which ensures data manipulation is impossible. Based on the number of credits a student has gained, they will be provided with certain benefits. A staff is provided with administrative access to the application as they are entitled to generate a unique ID for every student. Staff also verifies the authenticity of the certificates that are being uploaded by the students which are hashed using MD5 and are appended to the existing chain. Each block in the chain is hashed using SHA-256 algorithm. A leaderboard can be viewed by the students along with the provision to view their individual scores. The student who tops the leaderboard at the end of the final year will be the best outgoing student of that batch.***

Keywords: ***Blockchain, leaderboard, DLT, SHA-256, hash, credit scores, MD5***

I. INTRODUCTION

The Blockchain technology is based on distributed records of all transactions that have taken place, which is shared among a group of participating users. All the transactions are verified by the majority of the users connected in the Blockchain network. Blockchain became famous after a paper on "Bit coin" was published by Satoshi Nakamoto in 2008. The transactions in a Blockchain are recorded using a digital ledger which is distributed to all the users in the network. The use of digital ledger makes the system more transparent and incorruptible.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
Kalpana Devi S*, Assistant Professor, CSE Department, Easwari Engineering College, Chennai, Tamil Nadu.
Bitra Sainadh, CSE Department, Easwari Engineering College, Chennai, Tamil Nadu.
Hariharan K, CSE Department, Easwari Engineering College, Chennai, Tamil Nadu.
Hemanth T, CSE Department, Easwari Engineering College, Chennai, Tamil Nadu.

Blockchain does not use the concept of central server to store the data. The data is distributed over hundreds of nodes all around the world that are connected together as a part of the network. It is a continuous chain of all transaction details stored in a block format that are not controlled by any single authority. Since the data is available in all the participating nodes, the data can be notarized and is publicly verifiable.
It is used to implement a system in which the timestamp of the document is not modified. Later in 2008, the Blockchain was conceptualized by not requiring the timestamp which is signed by a trusted party and introduce a parameter to stabilize the rate in which blocks are added to the chain. The block time is the average time for the network to create a block in the Blockchain. In some Blockchain every five seconds a block is created. Miners are used to create new block in a chain. This process is called as mining. The main advantages of Blockchain technology is decentralization, immutable, transparency, security and improved accuracy by removing human involvement in verification of data. The Blockchain technology makes the online transaction like financial services, charities and e-commerce more secured.
The Blockchain technology verifies the block without depending on the third parties. In traditional database there is a single point access to the data. But in Blockchain there is no single point access. The primary use of Blockchain is it is used as a distributed ledger.

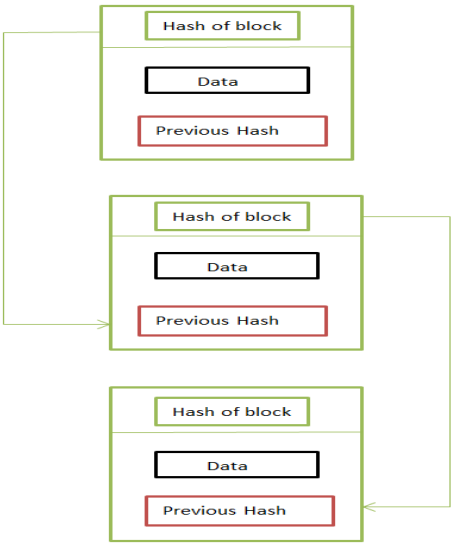

Figure 1: Blockchain Representation

A. DISTRIBUTED LEDGER

A ledger is a data structure, which contains all the transaction details, and is distributed across different computing nodes in the network.

B. CONSENSUS

Consensus is the process that ensures that all users in the Blockchain network come to accordance, with regard to the current state of the Blockchain. Consensus can be achieved using the Proof-of-Work to Proof-of-Stake algorithm.

C. SMART CONTRACTS

Smart contracts are used to make the transactions in a Blockchain more secure and trustworthy. The conditions specified in the contract must be fulfilled, for the transaction to take place.The proposed system provides an unbiased credit score for every student based on their performances in the co-curricular, extra-curricular and academic activities. Every student has to upload their certificates in it. The admin authenticates the uploaded certificates. The authenticated certificates are hashed using MD5 algorithm. Based on the type of certificate the credit scores are automatically generated and attached to the block. Leader board is displayed to the student with the credit scores. The motive of this system is to find the best outgoing student of the year and it also displays the benefits for the student if the student reaches a particular score level. By implementing this system in Blockchain, we can ensure that the student data is secure and cannot be tampered with. Thus, the system helps in identifying the deserving students and awards them.

II. LITERATURE SURVEY

The works and contributions of various authors have been taken into account for survey and their advantages and disadvantages have been analysed in order to make the proposed system work in an enhanced and robust manner.

The authors Shihong Zou and et al. in [1] have explained that there is a wide range of devices connected to the internet, which enables users to send or receive information at any time and any place. With the concept of smart city, these mobile devices help people to communicate and interact through the internet. However, when it comes to any violation of law, any criminal activity or any accidents that take place in a city, there are some people who make use of technology to report it, but most people ignore it. This can be attributed to two main reasons. First, reporting with a person's true identity is suggested, but it may cause the person to be afraid of retaliation by the offender. Second, since there are no benefits to the reporting made by people, they lack motivation for doing the same. Hence, the Report coin System ensures the protection of user identity and the reliability of the reported message throughout the process. Users may also vote an existing report by signing it, in case there are multiple witnesses. The system also provided incentives to those who report a violation in order to motivate them. The transaction records in this system are transparent and cannot be tampered with. The system uses techniques such as the Ring Signature which is used to guarantee the anonymity of the reporter. Zero Knowledge Proof (ZKP), which is used to verify the reported message. Public Key Cryptography (PKC) which is essentially used in the Blockchain implementation. Merkle Hash Tree is used for hashing and a consensus mechanism for a decentralized ledger system. Simulating the system with 1000 to 2500 mobile terminal users, with a threshold percentage of 0.9 the result showed that the average compilation time for all three phases (request phase, reply phase, verification phase) was approximately 230ms. And a success rate of 88% (approx.) was observed for 2500 mobile terminal nodes. However, one issue related with the system is that, it does not have a malicious user tracking mechanism.

Ayesha Shahnaz and et al. in [2] have proposed a method to safeguard all the data in the Electronic Health Records, hereafter called as EHR, using Blockchain as this framework has reportedly been well known for its non-damageable nature. The EHR usually consists of the records of all the patients that are held in a digitized system. EHR had already paved the way for accessing the information of all the patients whose details are stored as digital records from anywhere by anyone in the world who have access to the system. It may sound healthy as it will be easy during the emergency and treatment but it lacks in providing the necessary security to these health records and does not entitle any anonymity of the data which is a highly threatening factor. If the access to the system is acquired by wrong hands it can lead to a greater tragedy as the data is prone to be tampered with. Besides the data being not damageable and providing a secured storage procedure, while Blockchain is implemented for EHR to store records, it can be used to improve the scalability of the system using a technique called off-chain storage of IPFS and thus provides a secure and a scalable Blockchain based solution to the EHR system. One of the concerns of this system is to develop certain policies that have to comply with the rules and regulations of the existing yet advancing healthcare system.

The authors Li, Lun and et al. in [3] proposed a system to provide incentive for announcements made in the vehicular network. There are two major issues associated with the construction of such a network. Firstly, it is arduous to send announcements, which does not disclose the identity of the user. Second, users lack the motivation to make the announcements. The credit coin system enables different signers to create signatures and forward announcements anonymously. The Blockchain based system also provides incentives to motivate the users. Since it is a Blockchain based system, it is tamper resistant. The system uses a threshold ring signature which is a message authentication method, using a threshold value $\boldsymbol{th_1}$ and participant size,$\boldsymbol{p_1}$. Hashing is done using a Merkle Hash Tree. For making announcement, the faults are agreed upon by voting using an algorithm known as Byzantine Faults Tolerate Algorithm. Simulations of the experiment, shows that the transaction part of the user takes approximately 130ms. The major issue with this system is that it is only practical with the existence of smart vehicles and smart transportation methods.

Weilin Zheng and et al. in [4] have a proposed a BaaS platform which is referred as NutBaaS. Blockchain, a framework that is known for its decentralized nature in maintaining the resources and in protecting the identity of the user because of its anonymity is used.

The resources that are held in any Blockchain network can be accounted with great ease. The raising concern for important parameters such as security and reliability has led to the development of NutBaaS.

It acts as an intermediate that helps to overcome the security and reliability issues that happen to occur in a Blockchain network. On a real time basis NutBaaS, is featured to have its application in the cloud computing environments and therein, allows performing the regular business cases seamlessly without a necessity to monitor the systems for their performance. It finds its use in analysis of the smart contracts which are usually similar to virtual agreements in a Blockchain network, deployment of network, monitoring and testing of the systems. NutBaaS, on one hand enhances the security and the reliability of the system with the implementation of advanced services which include the Ideal Chain technology and vulnerability detection in smart contracts. On the other hand, it suffers from new trust related issues that weaken the Blockchain mechanism. Also, the transparency in the deployment and the runtime of the BaaS system has to be considered whilst considering the features such as reliability that has to be offered to the users.

The authors Basit Shahzad and Jon Crowcroft in [5] address the problems associated with security and privacy in an electronic voting system. The paper proposes hashing techniques to provide security of the data, and introduces concepts that help in creating and sealing a block. It uses a consortium Blockchain which ensures that only the governing body (election commission) owns the Blockchain. The arbitrary size of the input is converted into a fixed size output by using a hash algorithm. Blocks are created in order, for the user to register his/her vote. The block is created using a special ID of presiding officer following which the system appends a random integer. Then SHA-256 algorithm is used to produce a hash code and the block is successfully created. To seal the block, the contents of the block are hashed in pairs, Now the entire block that contains these hashed values, is hashed to make it more secure. The issue related to the system, is that the internet connection may not be available at all times, especially in remote places. And also the polling staff must be trained in the technology so that they can guide the voters.

Jorge Castellanos and et al. in [6] have proposed a technique that allows providing scores to every individual student based on their way of behaviour while they are involved in a social video based learning tool for OOPs course. The recent trends have seen that educational institutions, organizations and the governments are attracted towards students who are out of STEM (Science, Technology, Engineering and Mathematics) courses. It is because of the amount of exposure a student gets during their study. It may be because of the research activities they are involved in, the various analytical thinking courses they are enrolled in, and most importantly the group activities to which they are exposed as part of research etc. This makes the students from these courses more reliable because of their knowledge in excelling academically and socially. The students are assessed based on their social skills such as discussion on the platform etc. which is done using social network tools and peer review. The standing issue is that, the system is restricted to just one single course and it has to be extended for all the courses. Another issue is that the social behaviour of the student outside the assessment tool is quite uncertain.

The authors Dongxiao Liu and et al. in [7] proposed a system that uses the Industrial Internet of Things (IIoT) to improve operational efficiency between manufacturers, retailers and also to improve consumer experience. The paper proposes a reputation management system, where retailers get reputation based on customer feedback. The system boosts the common trust between industries and consumer confidence. This system is based on Blockchain technology, in order to maintain user anonymity and to make the system more transparent and tamper resistant using a distributed ledger. The system uses a Zero-Knowledge proof technique, which is used by one user to prove to another user that he/she has the secret **Se** used for a publically verifiable relationship. The PS-signature scheme is used to generate signatures of short size. Even though the system provides anonymity, it is only conditional. The Identity Management (IDM) entity will be able to track the users, in case of questionable behaviour by a user. Also users cannot find out if two valid reviews for a retailer are from the same person with multiple accounts (fraudulent user).

S.Muthamilselvan and et al. in [8] propose a system to protect uploaded documents of the users using the Blockchain technology. Data that is stored in a Blockchain are immutable in nature, and also decentralized, which means it does not depend on any central server. Smart contracts are used in order to transfer data in a trusted manner. The user documents are converted into e-docs using a Quick-Response code. The individual codes form a block having a unique hash value which helps in the formation of continuous blocks. The system uses steganography, which uses biometric data like the fingerprint, in order to protect the document. The problems associated with this system is that, people must be trained about the technology and also, on how to use it.

The authors Leila Ismail and et al. in [9] have explained about a lightweight Blockchain architecture that intends to hold the healthcare data. Traditionally management of healthcare data has been carried out with the help of cloud based data management servers and the client-server systems which were centralized and lacked a concept of maintaining anonymity of the users. Initially the implementation of Blockchain technology in the healthcare data management systems have seen that, although the issues of age-old systems have been overcome, it involved increased power consumption while reducing the chances of scaling the system to a better extent. The normal Blockchain based healthcare data management system which ran on bit coin network had suffered from lower transaction throughput. This system aims at dividing all the available participants in the network into groups where a single copy of the ledger is provided to every group. This system has increased the speedup of ledger by 67% and marking times when network traffic was low in comparison to the bit coin network while the number of blocks are being increased.

Although the system is faster and uses the consensus algorithm, the security of the system is a concern. In the future, systems that use fog computing and real time sensors can be used to improve the performance and the security to a further better scale.

Muhamed Turkanović and et al. in [10] have proposed a Blockchain based system EduCTX that is used to provide credits to the students who are undergoing higher education when they successfully complete activities such as the courses that are associated with the ECTS. In Blockchain technology there involves a permanent, verifiable ledger that caters the process of recording every transaction that is processed. The EduCTX system is based on a distributed peer-to-peer network and aims at offering credits to the students globally in the form of ECTX tokens. The credits earned by the students cannot be altered because of the features of Blockchain framework such as the decentralized nature of the data. The higher education institutions constitute the peer-to-peer network and the credit score of every student is easily viewable by the stakeholders of the higher educational institutions such as the companies that may be willing to offer jobs to the students who have achieved certain number of credits or the other institutions that may be willing to extend an offer to the students with the real potential. In this way the EduCTX system helps in identifying the real talents among the student community and makes it a trustworthy system. Currently, the EduCTX platform is restricted to only utilise ECTS as a standard to provide credit scores to the students. It has to be developed into a system that is acceptable globally and that utilises to its fullest the various appropriate techniques of Blockchain framework.

Table 1: Comparison of various techniques used in Blockchain

S.No.	Related Works	Algorithm Used	Achieved Result	Existing Issues
1	Reportcoin: A novel Blockchain based incentive anonymous reporting system. [1]	Ring Signature, Zero Knowledge Proof (ZKP), Public Key Cryptography (PKC) and Merkle Hash Tree.	**1.** User anonymity and reliability of message is ensured. **2.** Provides a success rate of 88%.	There is no malicious user tracking.
2	Using Blockchain for Electronic Health Records. [2]	Off chain storage of IPFS	EHR records cannot be corrupted in nature.	Needs to comply with the rules of the existing healthcare system.
3	CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles. [3]	Merkle Hash Tree, Byzantine Faults Tolerate Algorithm and Threshold Ring Signature.	**1.** Different signers can generate signature and forward it. **2.**For a ring of size 20, average time to compute for, request phase is 70ms, reply phase is 10ms and verify phase is 130ms	Only works with smart vehicles
4	NutBaaS: A Blockchain as a Service Platform. [4]	Smart contracts and Ideal chain technology	Improves the security and reliability of the network.	Running time to deploy the NutBaaS is more.
5	Trustworthy Electronic Voting Using Adjusted Blockchain Technology. [5]	SHA-256 hashing algorithm and Consortium Blockchain.	Uses hashing technique to create and seal blocks.	**1.** Internet may not be available in remote places. **2.** Polling staff must be trained, to help and guide the voters.
6	A Novel Engagement Score for Virtual Learning Environments. [6]	Social network tools and peer review	Provides incentive based on learning pattern.	**1.** The system is restricted to just one single course and it is extended for all the courses. **2.** The social behaviour of the student outside the tool is quite uncertain.
7	Anonymous Reputation System for IIoT Enabled Retail Marketing Atop PoS. [7]	Zero Knowledge proof technique, PS Signature scheme and Identity Management (IDM) event.	**1.** User anonymity is ensured. **2.**For a set of 20 users the review generation time is 295ms	Fraudulent user accounts maybe used for marketing.
8	E-DOC Wallet Using Blockchain. [8]	Smart contracts, Quick Response code and Steganography	Uploaded documents are protected in a block	People must be trained.
9	Lightweight Blockchain for Healthcare. [9]	Bitcoin and consensus algorithm	A network of 40 blocks will be able to transfer 4000MB of data.	Unable to provide security to all the data in the network
10	EduCTX: A Blockchain- Based Higher Education Credit Platform. [10]	Distributed Ledger Technology and Multi-signature Protocol	Provides credits to students based on academics	Restricted to only utilise ECTS as a standard to provide credit scores to the students

A. RING SIGNATURE ALGORITHM

Ring signature is a cryptographic algorithm, which is similar to the digital signature. It can be performed by any user or node that is connected in a private network using its own keys. The structure of the algorithm is like a ring, hence giving the algorithm the name, ring signature. In this algorithm each entity has its own public and private keys. An entity can generate a ring signature on a message, by using the input (message), its private key and the public keys of all the users or nodes in the network. Any entity can check the validity of the ring signature by using the, given signature, message and the public keys involved. It makes it very difficult for an attacker from outside the network to create a legitimate ring signature without possessing or without having knowledge of, any of the private keys used in a particular network. This algorithm provides anonymity in signature generation, that is, the identity of the person creating the signature remains anonymous in the network.

B. THRESHOLD RING SIGNATURE

This is a variant of the ring signature algorithm. In this algorithm, a particular number of members **t** (threshold) out of the total number of members of the network are required to work together in order to generate the ring signature. And similarly **t** members are required to work cooperatively to decrypt the message.

C. BYZANTINE FAULT TOLERANCE

In distributed computing networks, when any of the components in the network fails and there is no proper information for the other entities in the network, whether that particular component has failed or not, then this situation is referred to as the Byzantine fault. Consider a server is appearing to be both, failed and functioning, to a failure detection system. In this case for one observer of the network the server may appear to be functioning and to another observer it may seem to be failed. This makes it difficult for the rest of the entities of the network to admit that the server has failed and reroute to another server. This situation arises because of lack of consensus between the components of the network. The fault tolerance is achieved through the usage of general purpose computing nodes that communicates with each other using pairwise messages. This helps to achieve consensus, even in the presence of faulty computing nodes. It was found that, if there are **x** faulty nodes, then **(3x+1)** properly functioning nodes were required to achieve a consensus. That is the fault tolerance is achieved if the non-faulty computers have a majority in consensus.

D. ZERO KNOWLEDGE PROOF

The zero knowledge is a cryptographic method, in which one person proves to another person that he knows or possesses secret information, without revealing any specifics about that information. That is, the person must give out a statement that contains only an assertion that the person knows the secret information, but not the information itself. In Blockchain the zero-knowledge-proof is used to protect the identities of the parties that are involved in a transaction. Hence this is used to ensure anonymity in the network.

E. PROOF OF WORK

The proof of work protocol is a form of consensus algorithm, which is used to discourage the denial of service (DOS) attacks on a network. This is done by making the service requester do some work. The work is difficult, but feasible, to be completed on the requester side, while it is easy for the service provider to check or verify the request. In Blockchain, there are several mining processes (miners) that compete with each other to create a block and append it to the chain. Hence, the miners are provided with a task that they must complete first in order to create and append a block in the network.

F. MERKLE HASH TREE

A Merkle hash tree is a hash tree that is used in cryptography. The leaf nodes of the tree consist of the hash value of the data blocks. All the non-leaf nodes consists of the hash value their child nodes. These hash trees are used for verifying the data that is stored in data structures and also to verify data that are transferred between multiple computers. The hash tree is very useful in a peer-to-peer network, where it is used to verify the integrity of the transmitted block and also to ensure that the sending peer is not transmitting a fake block of data.

G. PUBLIC KEY CRYPTOGRAPHY

The public key cryptography is a cryptographic method used for encrypting and decrypting data. This algorithm is used to ensure security for data that is transmitted in a network. In this algorithm there are two keys that are used, public key and a private key. Each user possesses a public key and a private key. While the private key of a user is kept a secret, the public key of the user can be accessible by any nodes in the network. In order to encrypt a message, a user must use the public key of the receiver. This encrypted message can only be decrypted using the private key of the receiver, which is known only to the receiver of the encrypted message.

III. FUNCTIONAL ARCHITECTURE

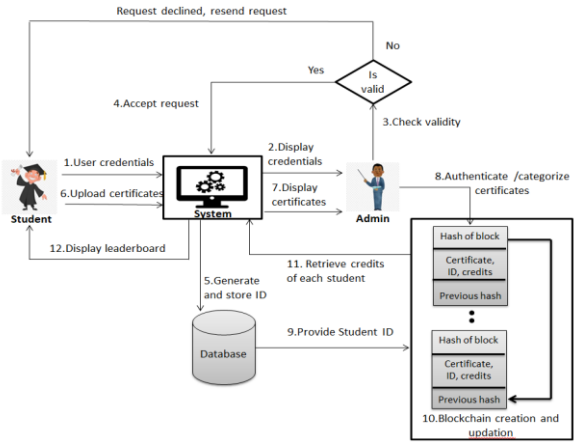

Figure 2: Functional Architecture

The proposed system consists of three main phases- they are Login Phase, Blockchain Creation Phase and Leader Board Display Phase.

In the first phase the student is required to provide the system with his/her user credentials that are used for requesting the creation of a user account. The admin of the system has access to these credentials. Once the admin has verified these credentials, the admin may accept or reject the user request. If the request is rejected the user must resend another request. If the request is accepted, then a unique ID is generated for the user along with his/her account.

This unique ID is then stored in the database. After the successful creation of an account, the student can use his/her credentials to login. In the user account, the students can upload their certificates. These uploaded certificates are displayed to the admin. Once the admin authenticates and categorizes the certificates, credits for the respective category are generated for the student and the certificates are hashed and stored in a Blockchain. The leader board gets updated dynamically, based on the credits earned by each student and can be viewed inside the user account.

IV. ALGORITHMS

A. SHA-256

In SHA-256, the plain text is length padded in order to obtain a multiple of 512 bits result. The obtained result is processed by passing it into 512-bit message blocks. These message blocks are represented as B(1), B(2), B(3)……, B(n) where $1 \leq n \leq \infty$.

The message blocks are processed in a sequential fashion starting with the initial value of the hash function Y(0).

In the calculation of the general hash function, the current hash value is dependent on the previous hash value and thus, $Y(i) = X(i) + C_{B(i)}X(i)$

where, $X(i) = Y(i-1)$ and $1 \leq i \leq \infty$.

C represents the compression function of SHA-256 and '+' denotes the word-wise mod 2^{32} addition. Therefore, Y(n) is the hash of a message or plain text.

In the proposed system, the SHA-256 algorithm has been deployed to calculate the cryptographic hash value of an entire block that holds the records of a student such as the credit score, unique ID, email ID, file, file hash that is obtained by applying the MD5 algorithm, previous block's hash etc.

B. MD5

MD5 is a cryptographic hashing algorithm that produces a 128-bit long hash value. SparkMD5 is an implementation of MD5 algorithm that is used to generate the hash or a certificate for every file that is uploaded by a student at a very faster rate than the normal MD5 algorithm. It allows us to maintain the data integrity by using checksum as a verification strategy.

V. IMPLEMENTATION

A. LOGIN PHASE

The system requires the students to furnish their user credentials, which is used for requesting an accounting creation. The data is then displayed to the staff (admin) of the system in a table format. The admin can either reject or accept the request. If the request is rejected, then the user is redirected to the registration page, where the user will have to resend another request. If the request was accepted, then a unique ID is generated for the user and stored in database, in addition to account creation. This unique ID is generated in order to solve the issue of malicious users in the Blockchain network. Two or more user accounts cannot be created with the same email id. Once the account is created, users can log on to their respective accounts, from which they can upload certificates, view their credits and also can view the leader board.

The unique ID is created using a set of random numbers which are generated using the **Random()** function. This unique ID is associated with the email id of the student, and is stored in the database using the email id of the student.

ALGORITHM 1

Step 1: Start.

Step 2: Initialize a string variable as String status = " ";

Step 3: Invoke the user – defined function createid( ) instance to generate unique IDs for users.

Step 4: On successful generation of unique ID for the user, set status = "accepted"; to enable the user

to login to his/her account.

Step 5: Stop.

B. BLOCKCHAIN CREATION PHASE

After the creation of user account, the students can use their credentials to login. The account of each student provides an option to upload certificates, viewing their respective scores, to view the leader board of their batch and an option to view the overall leader board of all students in the college. The students can upload a scanned copy of their certificates. These certificates can be that of, workshops, internships, technical events in symposiums, extra-curricular activities such as sports and also the semester mark sheets. The uploaded certificate is then displayed to the staff (admin), who then authenticates and categorizes the certificates. Based on the category of the certificate, credit scores are generated to each student. The uploaded certificates are then hashed using fast MD5 hashing algorithm, and the hashed value is then appended in a Blockchain. If a student tries to upload a same document twice, the newly generated hash will be same, as the one already existing in the Blockchain, and hence it will not be uploaded.

A servlet code is used for getting the details of a block such as, credit, email, file name, and the generated hash for the file. These details are got from the form tag of the jsp file. After getting the values, the **addBlock()** function is invoked to add the block to the array list. A connection with the database is established and the contents of the table certificate are updated.

The **isChainValid()** function is used for checking the validity of the created block. It takes three cases into consideration. The first case checks if the hash of the current block and the generated hash of that block are same. If they are not same it will return false. The second case checks if the hash of the previous block and the previous hash content of the current block are same.

If they are same it will return true, else false. The third case checks if the first five characters of the current block hash is the same as target hash. If they are same it returns true.
The output of this module displays the blocks in a JSON format, along with the contents in each block. As new files are uploaded the chain keeps growing in size, which can be seen in the output screen. The JSON data is simultaneously stored in a file using file write command.
The **calculateHash()** function is called after the values for the contents of block have been set. This is done so that the hash is calculated for the entire block along with its contents. The hashing algorithm used to generate the hash is SHA-256.

ALGORITHM 2

Step 1: Start.
Step 2: Create a class Block and get the SHA-256 instance.
Step 3: Initialize an ArrayList blockchain with the name Block.
Step 4: If blockchain is empty, then assign the value of previous block hash to "0".
Step 5: Create a block using the addBlock( ) method and check if the blockchain generated is valid
using the isChainValid( ) method and generate the hash of the block using calculateHash( ) method.
Step 6: Else, get the valid previous block hash by retrieving from the available blockchain and calculate the hash of the current block.
Step 7: Convert the values contained in the block associated with each user in the form of a JSON
object and append successive blocks to the blockchain.
Step 8: Stop.

C. LEADERBOARD DISPLAY PHASE

After hashing and appending the certificates to the chain, the leaderboard needs to be generated. IN order to generate the leaderboard, the JSON data in the file needs to be parsed and the values of the JSON array needs to read as a key value pair. The credits of the student who is currently logged in the session is retrieved from the chain and accumulated in a for loop. The total sum of credits is then displayed in the **score** section of the user account.
Using the total credits of all the students, the leaderboard is dynamically updated using a comparator class which uses the **compareTo()** function. This sorts the students according to their credit scores, and is displayed in a tabular fashion. In addition, the overall leaderboard, to view the credits of all the students in a college is also created and can be viewed from the user account.

ALGORITHM 3

Step 1: Start.
Step 2: Parse the file containing the blockchain using the JSONParser instance to retrieve the values
associated with the JSON objects.
Step3: Get the value associated with the key "credit_score" and sum the credits for each user from the parsed JSON data.
Step 4: Declare a HashMap<String, String> hashlist that holds the email and credits of each student.
Step 5: Display the hashlist as response using the RequestDispatcher instance to view the leaderboard
by checking for the credits of all the students belonging to the same year.
Step 6: Initialize a new TreeMap, for a student of any year of study, to view the general overall
leaderboard that contains the credits earned by all the students in the blockchain by using the
compareTo( ) method of the Comparator class.
Step 7: Stop.

VI. RESULTS AND DISCUSSIONS

Each module has its own set of inputs and expected output. The modules put together makes the generation of the Blockchain possible. The results of each module are discussed here.
The first module is mainly for the creation of a valid user account by using the credentials of the students and to create a unique ID for each student. This is done by the authentication provided by the admin of the system. The generation of the unique ID ensures that, there is no malicious user account created in the Blockchain network.

```
mysql> select * from register;
+------+--------------+----------+---------+------------+----------+------+----------+
| name | email        | password | conpass | mobile     | status   | year | uniqueID |
+------+--------------+----------+---------+------------+----------+------+----------+
| sam  | sam@gmail.com | sam      | sam     | 8465368616 | accepted |    1 | Adm_1421 |
| john | john@gmail.com | john     | john    | 6636345256 | accepted |    2 | Adm_1519 |
| ravi | ravi@gmail.com | ravi     | ravi    | 9897411654 | accepted |    3 | Adm_1086 |
| jim  | jim@gmail.com | jim      | jim     | 87841584122 | accepted |    4 | Adm_1297 |
+------+--------------+----------+---------+------------+----------+------+----------+
4 rows in set (0.00 sec)
```

Figure 3: Output of Login Phase

The second module enables the users to upload their certificates. These certificates are then authenticated and categorized by the admin of the system. The certificates are awarded credit scores. The weightage of the scores depends on the category to which the certificates belong.
The certificate is then hashed using MD5. The hash of certificates, credits and email id of students, together constitute the contents of a block. This block is then hashed along with its contents using SHA-256 algorithm.

Figure 4: Uploaded Certificate

Figure 5: Output of Blockchain Creation Phase

The third module creates and displays the leaderboard. The student who is currently logged in gets the leaderboard of his particular batch or year.

In addition, the student can also view the overall leaderboard, which would contain the credits of all the student of different academic years. The student also gets an option to view his/her individual credit score in their respective user account.

SNo	Name	Year	Credits
1	sam	1	10

Figure 6: Output of Leader Board Display Phase (1)

SNo	Name	Year	Credits
1	jim	4	35
2	ravi	3	30
3	john	2	20
4	sam	1	10

Figure 7: Output of Leader Board Display Phase (2)

VII. CONCLUSION AND FUTURE WORK

Blockchain is an evolving and a very promising technology, as it is used to eliminate fraud, mitigate risk, makes falsification very hard, brings out transparency and authenticity for various uses. The survey provides a thorough investigation on the merits and demerits of the existing Blockchain applications. The most common issue in the Blockchain application is the lack of malicious user tracking mechanism. This investigation provides more opportunities for the future development of the Blockchain Technology. The consensus algorithm can be made more effective in order to solve the malicious user problem. As a futuristic view, the system can be integrated with smart contracts and efficient hashing algorithms such as SHA-512 etc., for effective management on security. Furthermore, this technology finds use in the media industry, where there are many problems related to ownership rights, royalty distribution and transparency

REFERENCES

1. S. Zou, J. Xi, S. Wang, Y. Lu and G. Xu, "Reportcoin: A Novel Blockchain-Based Incentive Anonymous Reporting System," in IEEE Access, vol. 7, pp. 65544-65559, 2019.
2. A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019.
3. L. Li et al., "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 7, pp. 2204-2220, July 2018.
4. W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li and R. Chen, "NutBaaS: A Blockchain-as-a-Service Platform," in IEEE Access, vol. 7, pp. 134422-134433, 2019.
5. B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," in IEEE Access, vol. 7, pp. 24477-24488, 2019.
6. J. Castellanos, P. A. Haya and J. Urquiza-Fuentes, "A Novel Group Engagement Score for Virtual Learning Environments," in IEEE Transactions on Learning Technologies, vol. 10, no. 3, pp. 306-317, 1 July-Sept. 2017.
7. D. Liu, A. Alahmadi, J. Ni, X. Lin and X. Shen, "Anonymous Reputation System for IIoT-Enabled Retail Marketing Atop PoS Blockchain," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3527-3537, June 2019.
8. S. Muthamilselvan, N. Praveen, S. Suresh and V. Sanjana, "E-DOC Wallet Using Blockchain," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2018, pp. 989-993.
9. L. Ismail, H. Materwala and S. Zeadally, "Lightweight Blockchain for Healthcare," in IEEE Access, vol. 7, pp. 149935-149951, 2019.
10. M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform," in IEEE Access, vol. 6, pp. 5112-5127, 2018.
11. X. Yang, Y. Chen and X. Chen, "Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp.
12. M. Borkowski, M. Sigwart, P. Frauenthaler, T. Hukkinen and S. Schulte, "Dextt: Deterministic Cross-Blockchain Token Transfers," in IEEE Access, vol. 7, pp. 111030-111042, 2019.
13. S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266-2277, Nov. 2019.

AUTHORS PROFILE

S Kalpana Devi, Assistant Professor, Computer Science and Engineering Department, Easwari Engineering College. Completed under graduation in B.E CSE at Arulmigu Meenakshi Amman College of Engineering , Madras University in 2004. Completed post graduation in M.Tech CSE at Dr.MGR Educational and Research Institute University in 2008. She has published around 20 papers in National and International journals/conferences. She is a member of ISTE, AAA, IRED, IET. She has a teaching experience of 15 years and her areas of interest are Networking, Design & Analysis of Algorithms and Data Analytics.

Bitra Sainadh, final year student, Computer Science and Engineering Department, Easwari Engineering College. Currently pursuing under graduation in, B.E CSE. He has published a paper in a renowned international journal, IJSTR. Attended workshops on IoT and cloud computing. He has completed a course on Android application development, Web development and Machine Learning.

Hariharan K, final year student, Computer Science and Engineering Department, Easwari Engineering College. Currently pursuing under graduation in, B.E CSE. He has attended workshops on Big Data. He has completed a course on Android application development, Web development and Machine Learning.

Hemanth T, final year student, Computer Science and Engineering Department, Easwari Engineering College. Currently pursuing under graduation in, B.E CSE. He has published a paper in a renowned international journal, IJSTR. Attended workshops on Ethical hacking and cloud computing. He has completed a course on Android application development, Web development and Machine Learning.