Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 4026 - 4038
Received 05 March 2021; Accepted 01 April 2021.

Securing Digital academic Records using Blockchain

S Kharthikeyan[1*], Suruithi J P[2], Suruthika S[3]
[1]Assistant Professor(Sr.G),Dept. of CSE,KPR Institute of Engineering and Technology, Coimbatore
[2, 3]UG Student, Department of CSE, KPR Institute of Engineering and Technology, Coimbatore
*mailkharthik@gmail.com

ABSTRACT

Education has a great impact in today's economic growth in the country. Today's education system has many challenges and issues such as, introduction in modern technologies and tools in teaching learning process have failed, lack of proper mechanism for storing all the history of digital academic records and evaluating student credentials. This can be prevented by using the blockchain technology in the field of education to provide a trusted, transparent, distributed, and securely share store and verify learning achievements In our proposed work, a better solution is provided in the form of a distributed ledger to store the digital records like internal marks and attendance for the students using SHA256 in alignment with Blockchain. Our work not only saves the time, but leads in reducing the paper work in the institutions. By using the Blockchain technology in the education institutions, the records are maintained safe and protective.

Keywords: Blockchain; Distributed Ledger; Consensus; SHA256; Nonce; Cryptocurrency; Ethereum

Introduction

One of the emerging technologies in the Industry 4.0 is the blockchain technology which is not only one system, it's a mixture of the many methods like cryptology, algorithms, arithmetic calculations and consensus algorithms that are distributed. A blockchain has of six fundamental components as we discuss below:

1.1 Decentralized

Blockchain is not dependent on one centralized node that behaves as a sort of principal node, every node in the network that participates has the feasibility to record, pile and edit the archive as a ledger, and collectively form a blockchain. Any kind of new entry in the record block, or updates will be verified by all the nodes in the network.

1.2 Transparent

The data recorded in every block by the individual node is distributed amid further connected nodes such that it is evident to every node which generates transparency across all associated nodes. It means that there is no hidden secrecy a node can maintain without the knowledge of other nodes in the network.

1.3 Anonymous

For the transactions to be unidentified, implement a secure protocol, we hash the data before sharing. Any transaction for the matter, has to undergo a secured protocol that gets a hash value to access the information across the nodes that are there connected in the network. Addition to that each and every such transaction has to be validated by all the nodes.

1.4 Consensus Base

As every node is associated visibly through blockchain and modifications are done only when most of the nodes consent the change, wholly the nodes are authorised to transfer and update

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 4026 - 4038
Received 05 March 2021; Accepted 01 April 2021.

data securely giving a consensus base in the arrangement. Any node cannot claim a false transaction between other nodes unless all the nodes provides a consensus.

1.5 Immutable

All data are perpetually reserved which cannot be changed until somebody takes control of moderately 51% nodes concurrently. Any kind of change requires nod from the entire nodes connected in the network. One cannot simply change or edit the information as such in the network implemented through blockchain.

1.6 Open Source

Utmost blockchain systems are hospitable to all, permitting the members to switch the program and technology in ways in which most accurately fits their requirement. But, it doesn't makes a call that someone be able to make a change in the working blockchain solution. It just concludes that all nodes connected are visibly tolerant to the change.

1.7 Blockchain Structure

The structure of the blockchain is pretty interesting to learn and develop. Basically, it is seen as a chain of blocks where information is stored in each block. Every block in the blockchain has five components: 1) the most data; 2) hash of preceding block; 3) hash of current block; 4) timestamp and 5) meta information

1.7.1 Main Data

The primary component of a block in the blockchain is the main data. It has the source or the information that has to be maintained. The information relies on the nature of operation; it's generally a transfer between two nodes. But, it is mostly of any information that needs to be updated. To access the main data is not much easy. We maintain it using the hash function.

1.7.2 Hash of preceding block

During a transaction execution, as a result of a mathematical computation which is not reversible, a hash value is produced and disseminated to the nodes in a network. Many hashing algorithms are used, however the Merkle Tree is prime. It allows hash without much difficult and upfront de-hash opportunities.

1.7.3 Hash of current block

The closing hash value is noted down in block header (hash of current block), whereas the information itself is kept in the body of the block. Blocks are normally of a length there by permitting a restricted count of transactions per block. Normally, the information is secured based on the number of zeros that is followed by the hash values.

1.7.4 Timestamp

Last, but not the least, is the interesting component called the timestamp. As the name indicates, this component refers to the time period when the block was created. It includes Nonce (Number Once) and additional information like value of Nonce, signature of the block, or other user defined data. The Nonce is again an outcome of complicated mathematical computation that is hard to crack.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 4026 - 4038
Received 05 March 2021; Accepted 01 April 2021.

The application of blockchain to education remains in its premature times. Very few educational bodies have begun to apply blockchain skill as it is safe and protective. Most of those institutions are spending on the technology for the aim of authorizing and distributing academic certificates along with the achievements of the learning consequences of students.

On the other hand, scholars within the arena trust that blockchain technology has much to supply and safer to use then other technologies. Academic marks are extremely respected as they function a metrics of the human assets of their holders. Assets denotes to the talents, capabilities, awareness and capacities accomplished by means of education.

Academic credentials are predominantly significant employed circumstances as they function a promise of not only the information, proficiency and abilities of the holders, but also of their capabilities, consistency and commitment. Due to its value, publics habitually lie around their qualification in academics by submitting marks in certificates observed that the majority candidates lie a minimum of about some a part of their educational credentials and knowledge. By using this Blockchain, the marks can be stored completely so that these fake activities can be prevented.

Blockchain technology basically is often understood like database that is distributed and orderly saves a sequence of knowledge packed into non-transparent blocks. Yet, the opportunity of our study is to develop a framework to execute security demands in academic documents authentication and education system within the blockchain.

And, this blockchain system provides businesses the precision to check worker's academic marks at the time of recruitment and it avoids huge spell to examine the academic records. So the marks obtained by students and their attendance can be kept safe by using this technology. As we are using this blockchain technology for storing the internal marks and for storing the attendance, we can store the details in a hash value so that the previous stored and currently stored data can be retrieved. The following diagram depicts the attributes of a block in a blockchain system.

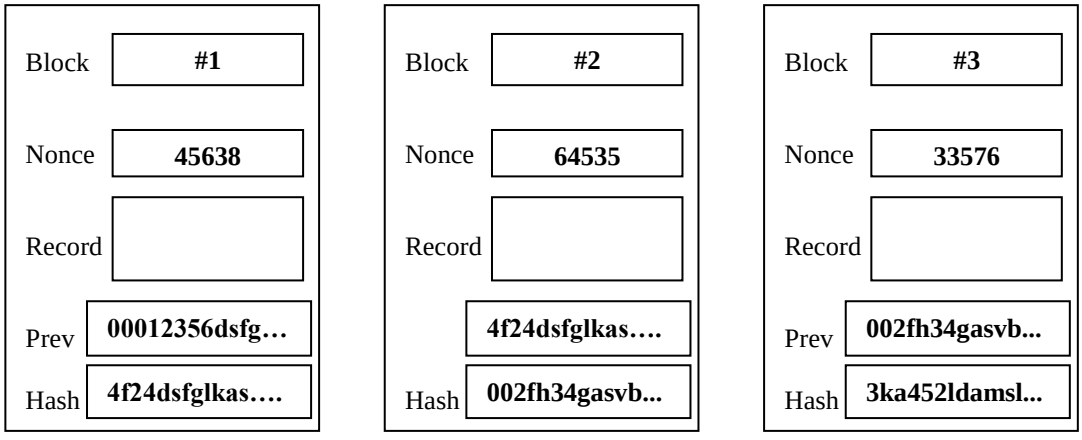


Figure 1. Attributes of a block in Blockchain application

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 4026 - 4038
Received 05 March 2021; Accepted 01 April 2021.

1.8 Blockchain Architecture

Blockchain is implemented in a distributed environment with the nodes that are connected in the network collectively. The platform is set to share the information enhancing distributed computation on the information. Every single user is identified as a node in the network connected in a distributed manner. A copy of the data or information is maintained by every node. Whenever there is an updation in the records or data, the block is updated regularly. The figure below shows the architecture of a blockchain.

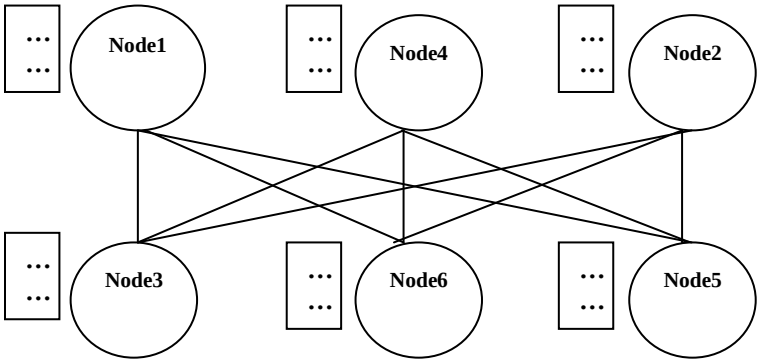


Figure 2. Architecture of Blockchain

Literature Review

Omar S Saleh et al. [1] identified the existing certification way out are confidentiality, integrity, authorization, authentication, secrecy and ownership. So, in their work they have used blockchain based framework for the academic certificate verification. This methodology focuses much better on authorization, authentication, secrecy and ownership refrains.

Mukul Rane et al. [2] focused on the impression or platform pay slip facility to the changeover problem and announces a framework to inspect academic records across institutions and universities. The work has a utilizing hyperledger like a exclusive agreed blockchain offering a sophisticated output, value effectiveness, comprising confidentiality compared with tactics for mutual blockchain.

Guang Cheng et al. [3] depicted the possible use of the blockchain in the academic system and institutions. The work clarifies using the blockchain technology in various matters in the present education system and different educational institutions which could be solved in the essential zone and how it can be fixed in education. Generally, the authenticating experts and the central bodies yield supplementary time to carry out the procedures.

If the procedure is implemented through blockchain, there is a great potential in reducing the possibility of the central server downtime. Since there is not much trust on the central power, it takes very less time to complete the process. Bearing in mind that the information warehoused on the blockchain is tamper proof. This information is restricted to modify, if implemented on blockchain network. The records are stored as tamper proof smart contracts.

Dinesh Kumar et al [4] identified that transparency and data immutability are the key aspects of blockchain. The idea looks like a distributed ledger where the network connected node authenticates and marks the final consensus for inserting the information in the network. The

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 4026 - 4038
Received 05 March 2021; Accepted 01 April 2021.

progression of academic record generation is exposed and disseminated across the parties so that anyone in the organization or party can authenticate the data of an educational certificate by means of blockchain system. The Ethereum technology too guarantees information saved in blockchain network is encrypted, consequently only the possessor of certificate can view and share it as they demand. Therefore, educational institutes have a chance to work together with any employers and issue authorizations on the blockchain to eliminate bogus educational certificates.

Rishav Chatterjee et al [5] runs the various methods and means to contemplate the consensus as accumulating the Proof of Work (POW) to the blockchain. Implementing the algorithm, various bodies extent to the consensus, for instance, to augment the conforming the transaction to the respective blockchain or not. Here, the strain can be enlarged to crack the cryptographic conundrum and it makes much perplexing to unravel by cumulating the supplementary number of prominent zero's in the complete cryptographic conundrum

F. Tschorsch et al [6] depicts the data nearby the string of the knowledge is used that cryptographic token, which usually mentions to the development and the transition of the cryptocurrencies along with the storage. Mostly the cryptographic token denotes to the string of the information referring to the knowledge possessing the original data. Ethereum is the fuel for applications of distributed platform based.

Artyom Kosmarski [7] studied the impact of blockchain with many academicians, IT experts and tried to bridge the barrier by learning the experience of implementing blockchain based solutions in the academics. The research groups the responses in various themes like immatured and weak view of the application, legal issues, wide adoption of the blockchain system, information that conflicts, trustiness and the ownership on blockchain.

Marinos Themistocleous et al [8] have analysed the major impact factors in education with the evolution of blockchain technology. The digital up skill in resources, key training requirements for jobs and access to the data are understood as major challenges through the implementation of blockchain. It is also considered that blockchain would be an essential factor that can differentiate the income among the countries in the world.

Rui Zhanget al [9] have summarised the security and privacy techniques among mixing, group signature, ring signature, ABE, HE, SMPC, NIZK, TEE – based solutions and game based solutions. It is noted that most of the techniques hides the identity of the signer from the group of users. Some of the operations like addition and multiplication are handled effectively, whereas the complex functions are identified less efficient. These reviews has led us to implement our work using SHA 256 algorithm.

Roshani S Bele et al [10] have used a unique code to provide a paper based certificate and other information. The certificate is identified with the help of this unique code through which the certificate is issued and updated in a blockchain system. Every certificate is saved much secured in terms of a block in the application which is developed and implemented through blockchain technology. The unique code is a hash value which is the outcome of a mathematical computation function. This function is much secured and implementable because the process is tedious to reverse and break. Thus, we were inclined to choose a much more secured algorithm SHA 256 in our work.

Methodology

Each institute has significant records which has to be safe guarded. The prevailing system of centralized storage is one such that requires backups of the information saved in the central sever.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 4026 - 4038
Received 05 March 2021; Accepted 01 April 2021.

Conversely, if the information is altered in the server, the updated record will be retrieved by all nodes which should be disallowed.

The traditional paper based marks are vulnerable with fraud occurring through forgery and mistakes. Paper based marks are inaccessible quickly, limited flexibility, lengthy process, high-cost and are non-eco-friendly. The students applying for jobs immediately after graduation, the students applying for abroad universities. The recruiters are all facing problem with respect to marks verification. And in attendance maintenance the existing system has the paper based records in the educational institutions and not in the digital based

The proposed work implements a blockchain based education system and attendance entry. Our scheme implements decentralized and distributed network through which every student academic information is stored as a chain of blocks. These blocks are connected to one another forming a chain of records. A blockchain-based storage of students internal mark system that uses "permissioned blockchain" to enable liquid democracy SHA-256 algorithm is used generating hashing values accuracy.

Blockchain based education system to keep records of all the transactions related to student internal marks. The existing marks can be viewed and if any changes made in it, the updated marks as well as the existing are viewed as we are using Blockchain in it. The maintenance of transactions are additional benefits in it. The attendance are kept in an digital way using blockchain so that it cannot be changed or cannot be deleted as it is safe

3.1 SHA Algorithm

Secure Hash Algorithm (SHA) is a standard cryptographic algorithm that generates a hash value with the help of hash function. Following are the steps used in the algorithm

3.1.1 Pre-processing

- Step1: The given text is converted into binary to which the binary value 1 is appended at the end
- Step2: This data is padded with 0s till it becomes a multiple of 512
- Step3: Continue appending 64 bits at the end which is divisible by 512

3.1.2 Hash Value initialization: Pseudo code

Develop the data in continuous 512-bit portions:
Divide the data into 512-bit portions
for every portion
Develop a 64 capacity text array t[0..63] of 32-bit words
Copy portion into first 16 words t[0..15] of the text schedule array
Extend the first 16 words into the remaining 48 words t[16..63] of the text schedule array:
for x : 16 to 63
s0 := (t[x-15] rotateright 7) xor (t[x-15] rotateright 18) xor (t[x-15] shiftright 3)
s1 := (t[x- 2] rotateright 17) xor (t[x- 2] rotateright 19) xor (t[x- 2] shiftright 10)
t[x] := t[x-16] + s0 + t[x-7] + s1
Set the variables to present hash value:
m := hash0
n := hash1
o := hash2
p := hash3
q := hash4

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 4026 - 4038
Received 05 March 2021; Accepted 01 April 2021.

r := hash5
s := hash6
t := hash7
Compression procedure:
for x : 0 to 63
RES1 := (e rotateright 6) xor (e rotateright 11) xor (e rotateright 25)
tx := (e and f) xor ((not e) and g)
t1 := h + RES1 + tx + k[x] + t[x]
RES0 := (a rotateright 2) xor (a rotateright 13) xor (a rotateright 22)
trt := (a and b) xor (a and c) xor (b and c)
t2 := RES0 + trt
t := s
s := r
r := q
q := p + t1
p := o
o := n
n := m
m := t1 + t2
Append the compressed portion in present hash value:
hash0 := hash0 + m
hash1 := hash1 + n
hash2 := hash2 + o
hash3 := hash3 + p
hash4 := hash4 + q
hash5 := hash5 + r
hash6 := hash6 + s
hash7 := hash7 + t
Write the final hash as
final:= hash := hash0 append hash1 append hash2 append hash3 append hash4 append hash5 append hash6 append hash7

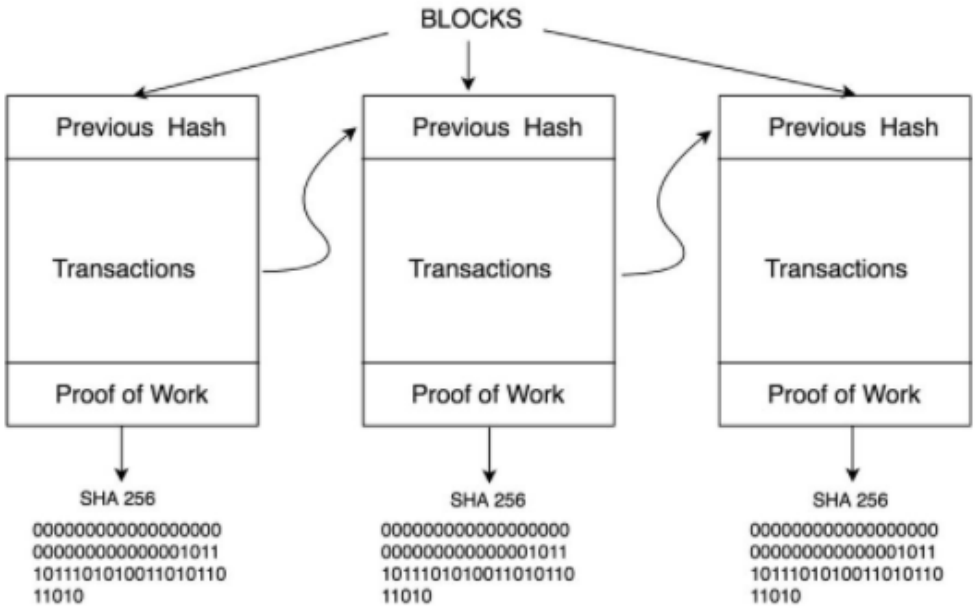


Figure 3. Digital Record Maintainance using Blockchain

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 4026 - 4038
Received 05 March 2021; Accepted 01 April 2021.

4. Implementation and Results

Our implementation work suggests to apply Blockchain in the student academic record maintenance to reserve the student data in the form of chain of blocks along with acceptance of student endeavours and university credentials. This work can be employed in coming times by signifying a way to craft an entirely functional system. Our implementation includes various modules as follows.

- Registration
- Login
- Mark entry
- SHA256 algorithm implementation

Register: The student will register with the valid information and it will be stored in the database.

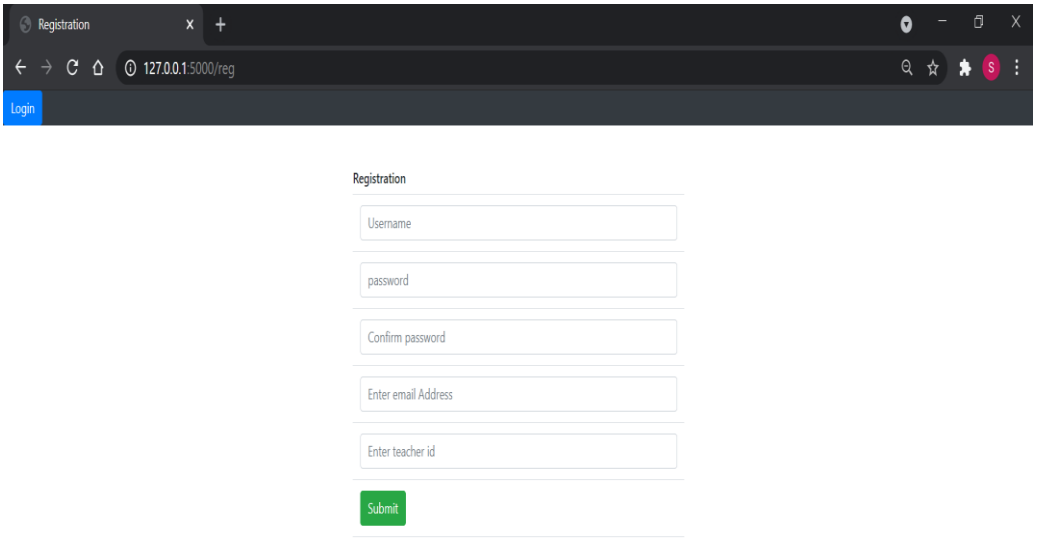


Fig 4. Student Registration

Login: By using the valid username and password the students and teachers can login into the website

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 4026 - 4038
Received 05 March 2021; Accepted 01 April 2021.

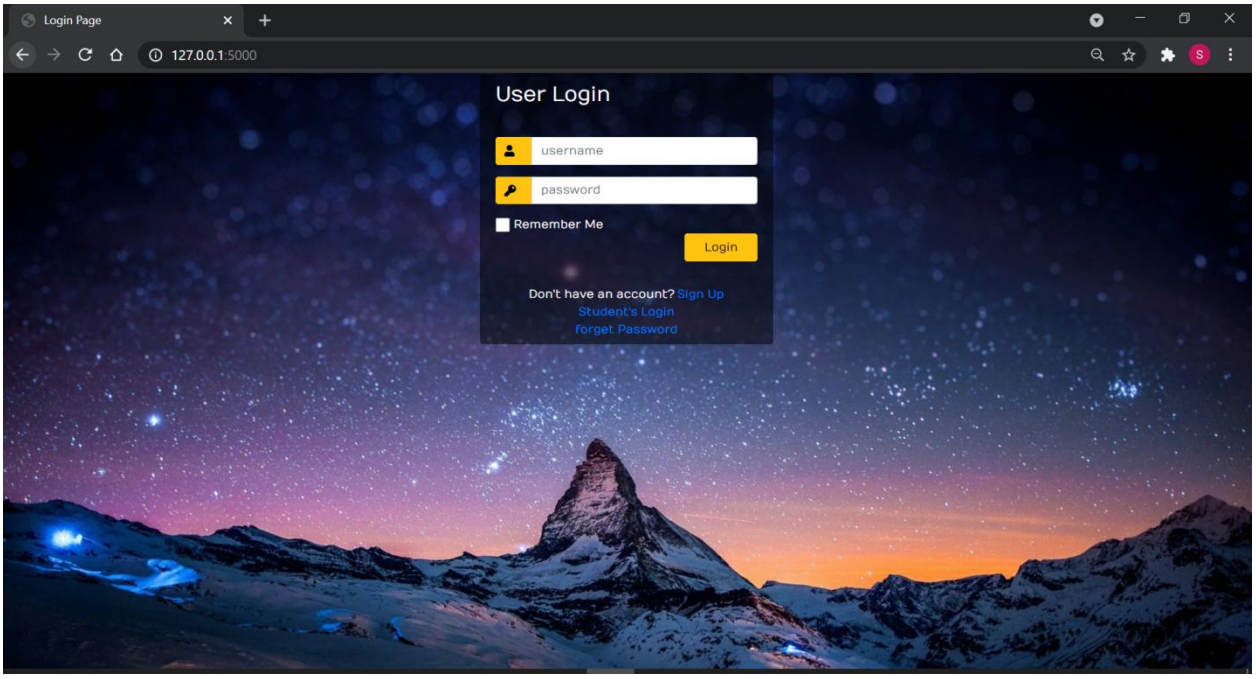


Figure 5. Login view for students and teachers

Internal mark entry: The faculty will be entering the internal marks for the every students individually.

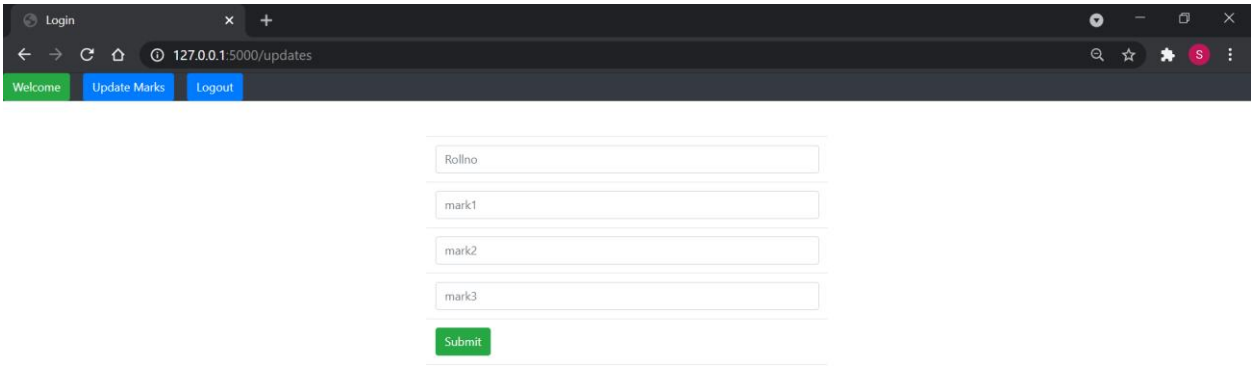


Figure 6. Mark entry system with SHA 256 implementation

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 4026 - 4038
Received 05 March 2021; Accepted 01 April 2021.

View internal mark: Once the mark is inserted both the student and teachers can view the marks.

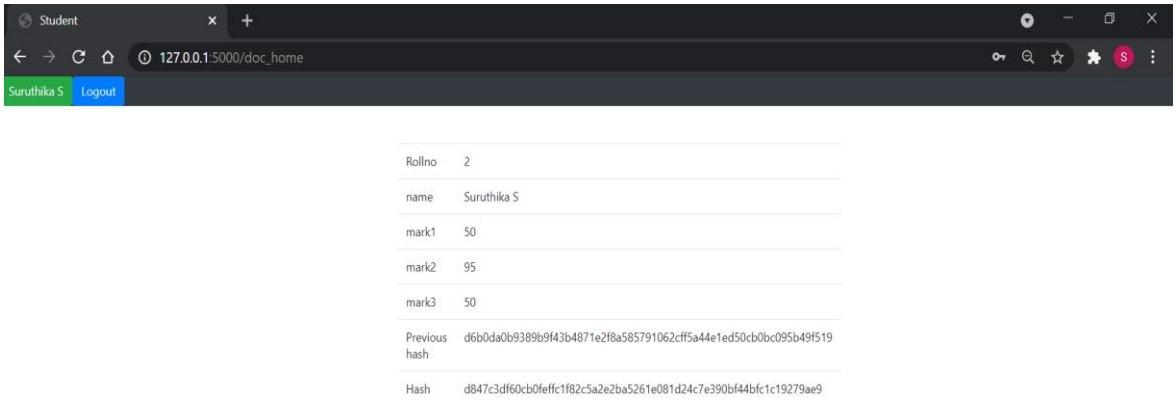
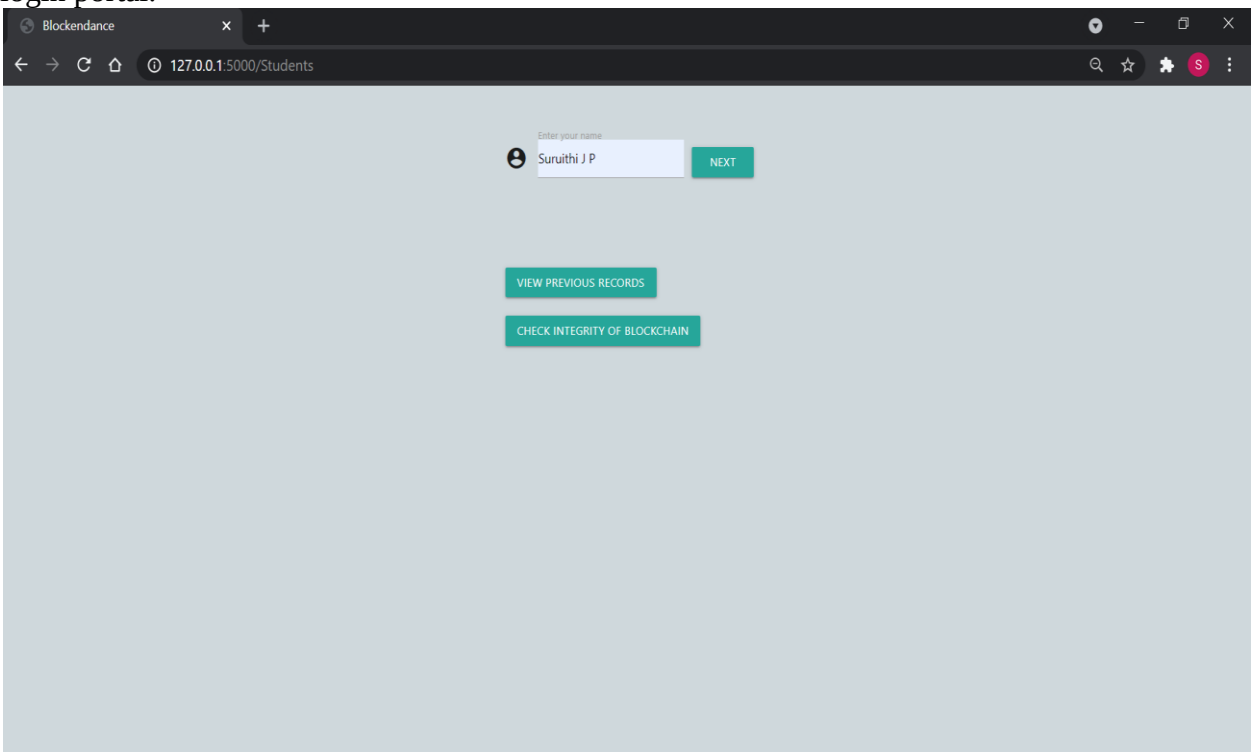


Figure 7. SHA 256 implementation as Blockchain

Login for attendance: The faculty can enter their attendance for the students by using the same login portal.



Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 4026 - 4038
Received 05 March 2021; Accepted 01 April 2021.

Figure 8. Faculty login page

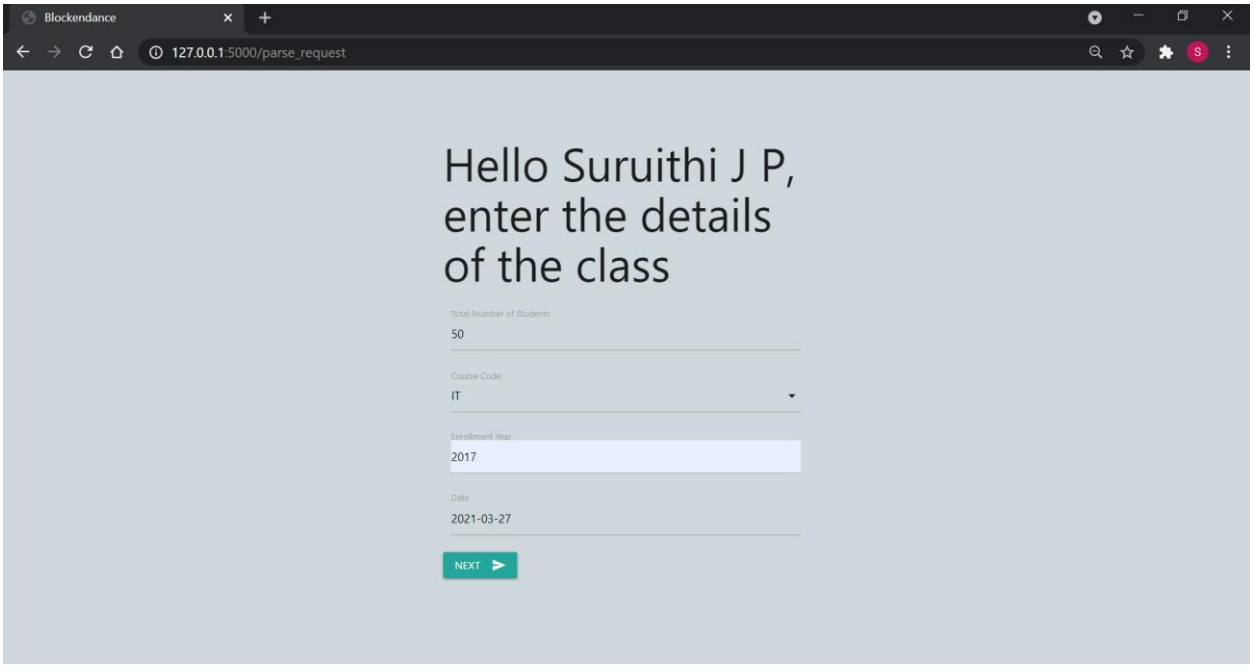


Figure 9. Selection of data for attendance entry

Attendance Entry: The faculty can mark the status of attendance for every student which is again stored using SHA256 as a sequence of blocks

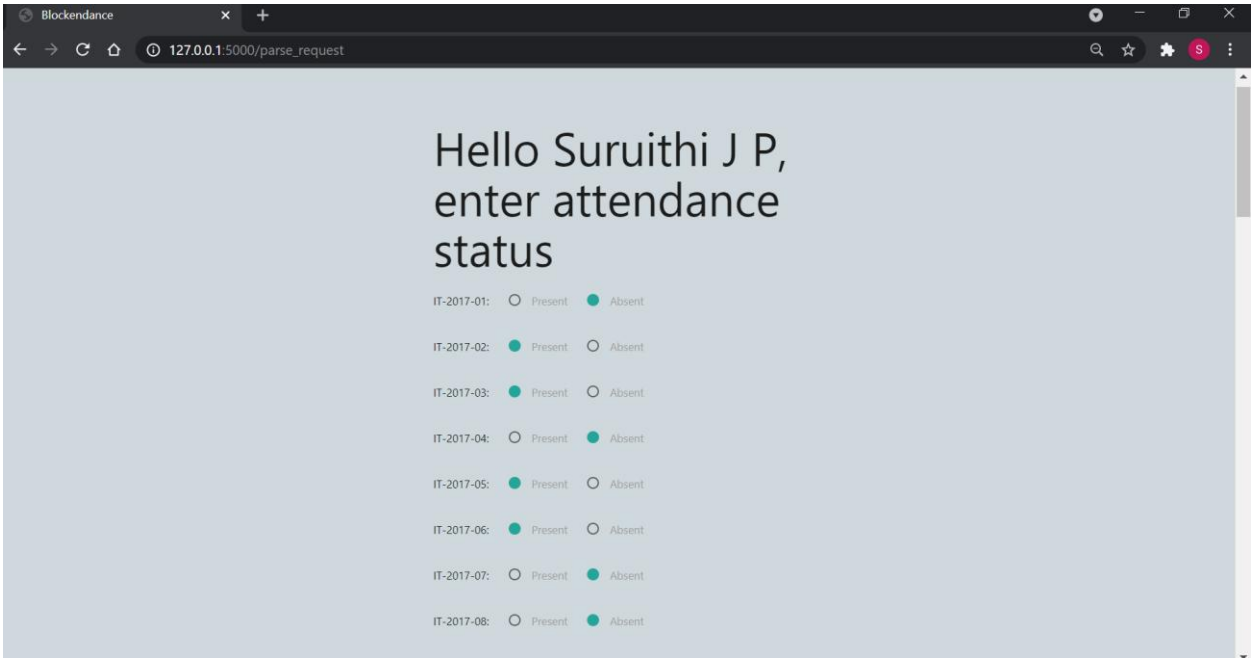


Figure 10. Selection of data for attendance entry

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 4026 - 4038
Received 05 March 2021; Accepted 01 April 2021.

Conclusion and Future Enhancement

Blockchain is the safest technology. It has the ability to change the platform of education. As we are using this technology in the education field, it will be more useful and helpful in storing the academic records. Blockchain Technology is gaining popularity day by day. The projected stage profits the benefit of the blockchain so as to make a totally trustworthy education academic system. And thus, we implemented a system which is working on the blockchain technology implementing SHA256 algorithm. It transfers the upper academic records storing scheme from the current real time physical information or traditional digital records to an effectual, streamlined, pervasive form, And including this the digital based attendance records can also be maintained by the institutions which are all supported blockchain technology.

So, in our work, data security of mark entry is the salient feature in our proposed system. The data is stored using the hash value generated by SHA256 algorithm implemented. The data is stored in a block which cannot be changed. The system possess the hyper ledger in a network where all the users or the nodes connected can save the data as well as verify the same. This system has a great scope in educational systems and institutions reducing the risks of fraudulent entries in the system and changes.

At present, there is a paper based internal mark storage and even digital based is available in some of the institutions but the blockchain based internal marks storage can be done by our project. The marks once entered should not be updated. At the unavoidable circumstances, if the marks are edited, the record can be preserved through the blockchain system that we have implemented and is known to all the nodes connected in the network. This gives us the maintenance and the storage of records 100 times safer than our normal conventional paper basis methods. In this, the existing as well as the updated marks can be viewed so that the fraud in the marks can be avoided and attendance can also be entered and kept safe and protective as we are using blockchain technology. In future, in addition to this the mark sheets verification in blockchain can be included into this project as an enhancement. This may be the future work of this current project.

References

[1] Omar S. Saleh, Osman Ghazali, Muhammad Ehsan Rana, Blockchain based framework for educational certificates verification, Journal of Critical Reviews Vol 7, Issue 3, 2020 ISSN – 2394 – 5125, Page 79- 84

[2] Mukul Rane, Shubham Singh, Rohan Singh, Vidhate Amarsinh, Integrity and Authenticity of Academic Documents Using Blockchain Approach, ITM Web of Conferences 32, 03038 (2020)

[3] Guang Cheng, Bing Xu, Manli Lu and Nian Shing Chen, “Exploring Blockchain technology and its potential applications for education” Springer 2018.

[4] Dinesh Kumar K, Senthil P, Manoj Kumar D.S, Educational Certificate Verification System Using Blockchain, International Journal of Scientific and Technology Research, Volume 9, Issue 3, March 2020 ISSN 2277-8616, Page 82-85

[5] Rishav Chatterjee, Rajdeep Chatterjee, Overview of the emerging Technology: Blockchain, International Conference on Computational Intelligence and Networks, 2017

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 4026 - 4038
Received 05 March 2021; Accepted 01 April 2021.

[6] F. Tschorsch and B. Scheuermann, Bitcoin and beyond: A Technical Survey on decentralized digital currencies, IEEE Communications Surveys and Tutorials, Volume 18, Issue 3, March 2016 , Pages: 2084 – 2123

[7] Artyom Kosmarski, Blockchain Adoption in Academia : Promises and Challenges, Journal of Open Innovation: Technology, Market and Complexity, 16 October 2020

[8] Marinos Themistocleous, Klitos Christodoulou, Elias Iosif, Soulla Louca, Demetrios Tseas, Blockchain in Academia: Where do we stand and where do we go?, Proceedings of the 53rd Hawaii International Conference on System Sciences, January 2020, Page 5338 - 5347

[9] Rui Zhang, Rui Xue, Ling Liu Security and Privacy on Blockchain, ACM Computing Surveys, Volume 1, Article 1, January 2019

[10] Roshani S Bele, Jayant P Mehare, A review on digital degree certificate using blockchain technology, International Journal of Creative and Research Thoughts, Volume 9, Issue 2, February 2021, Page 5150 -5156