Implementation of Blockchain Technology in Education System

Akshay Karale, Harmeet Khanuja

Abstract: ***The Blockchain for Education platform helps us to make the tamper-proof certificates and their correct and the overall permanent allocation of these certificates to learners, as well as verification of certificates. It can reduce the overall frauds and tampering of the degrees and certificates. Blockchain technology can be used to solve many educational problems and can help educators as well as learners to monitor the learning outcomes. The data can be stored securely and tamper proof format when it's stored onto the blockchain network. Here smart contracts can be designed and deployed on to the Ethereum blockchain that can be designed using the solidity programming language. Blockchain can be applied to private, public and consortium sectors depending upon the usage and the scope of the blockchain. Education system can take benefit of this scalability of the blockchain and can be effectively useful in the educational institutions.***

Keywords: Blockchain, Distributed Ledgers, Smart Contracts, Solidity; POW, Consensus.

I. INTRODUCTION

Blockchain can transform the traditional record storage of students and the staff over the distributed network. As the data is stored on the distributed system it is secure and more transparent. The overall data accuracy and immutability is preserved in the distributed blockchain environment. Generally blockchain consist of the various steps while deploying the data onto the blockchain network. Here each user has their own hash value associated which will help them to identify them uniquely over the distributed network. The time stamp is also added as the part of the hash value which is generally from random value.

Issues in the current education system and different educational organizations can be resolved using the blockchain technology in the core area. It can be resolved using the blockchain technology in education system. Usually the verifying authorities and the central institutions take more amount of time for carrying out the operations which is a time consuming process. Using the blockchain technology we can eliminate the risk of the central server down time. As we are not relying on the central authority the process takes fewer amount of time. The data stored on the blockchain is tamper proof and cannot be modified once deployed on blockchain network.

Revised Manuscript Received on July 22, 2019.

Akshay Karale, Department Of Computer Engineering, Marthwada Mitra Mandal's College Of Engineering, Pune.

Harmmet Khanuja, Department Of Computer Engineering, Marthwada Mitra Mandal's College Of Engineering, Pune.

II. LITERATURE SURVEY

The paper [1] depicts the potential application of the blockchain in the education system and organizations. Further explains the different issues in the current education system and different educational organizations can be resolved using the blockchain technology in the core area and how It can be resolved using the blockchain technology in education system. Usually the verifying authorities and the central institutions take more amount of time for carrying out the operations which is a time consuming process. It continues with the blockchain technology we can eliminate the risk of the central server down time. As we are not relying on the central authority the process takes fewer amount of time. Considering that the data stored on the blockchain is tamper proof and cannot be modified once deployed on blockchain network and stored in the form of tamper proof smart contracts. The paper [2] provides the different approaches and ways to consider the consensus as adding the POW (Proof of Work) to the blockchain. Using this algorithm different parties reach to the consensus like to add the corresponding the transaction to the corresponding blockchain or not. Here the difficulty can be increased to solve the cryptographic puzzle and it can be made more challenging to solve by increasing the more number of leading zero's in the overall cryptographic puzzle.

Paper [4] describes how the peer-to-peer electronic cash can help users to send the money from one point to other point without involvement of the third parties. And also added the use of the Ethereum blockchain in the corresponding blockchain network. Further explains how the digital signature and digital certifications can help the educational institutions and disrupt the current centralized systems. Blockchain technology provides more security to the data compared to the central data storage, as we don't need to worry about server down time. Even if we want to hack the overall blockchain network we need to gain the access the 51% access of the network and which is quite impossible to perform. And blockchain is secured by many number of the active nodes in the blockchain network.

[5] Provides the information about the string of the knowledge is used that cryptographic token. Which generally refers to the creation and the transfer of the cryptocurrencies as well as the storage. Generally the cryptographic token refers to the string of the information which actually points to the knowledge having the initial data. [5] Ether is the fuel in the distributed platform based applications. It is used in the Ethereum blockchain.

It further explains that it can be considered as the payment method generally preferred in the Ethereum blockchain network. As it is applied so that developers can develop the quality of the applications. [6]Provides the information regarding the Ethereum blockchain and how it can be implemented in the form of the smart contracts designed using the solidity programming language. [6]Explains the additional and innovative approaches that can made possible using the quality attributes of blockchain technology for the educational systems.

III. BLOCKCHAIN TERMINOLOGIES

A. Transactions

Blockchain contains the shared and the distributed transactional database. When changes are made to data base we have to make a transactions and it has to be agreed and accepted by everyone in the network. The transactions on the network are always cryptographically signed and maintained uniquely.

B. Distributed Ledgers

It is a database held and then updated by each and every participant in the comparatively large network. The overall distribution is kind of unique as the communication occurs in distributed way and it's not carried out by the central authority. Here once it is updated all the nodes in the network receives the updated copy of the corresponding ledger.

C. Cryptographic Token

The string of the knowledge is used that is called as the cryptographic token. Which generally refers to the creation and the transfer of the cryptocurrencies as well as the storage. Generally the cryptographic token refers to the string of the information which actually points to the knowledge having the initial data. It is actually associated with all the blocks in corresponding blockchain [6].

D. Ether

Ether is the fuel in the distributed platform based applications. It is used in the Ethereum blockchain. It can be considered as the payment method generally preferred in the Ethereum blockchain network. As it is applied so that developers can develop the quality applications and the overall network remains healthy and the transfer performs in the correct manner. [6]

E. Ethereum Blockchain

Ethereum is platform which follows the decentralized platform and it can be accessed by deploying the smart contracts. Here we have no need to worry about server down time. As the smart contracts are shared by all the nodes in the network. Here we have the different programming languages to design smart contracts which can be efficiently deployed on Ethereum blockchain. [6]

F. Gas

To limit the overall amount of work done, each transaction is associated with the certain amount of the gas. The value of the gas is calculated with the formula (**gas price * gas**).The moment if an out of gas notification is triggered then it'll revert all the corresponding transaction at the given moment. Usually the actual price of the gas is set by the one who has created the transaction.

G. Smart Contract

Smart contracts are the scripts which are self-executing and can be written in programming languages such as the JavaScript, python or solidity. Smart contracts are generally used to specify the rules while to parties communicate with each other. It can overall reduce the degree of security and helps us to lower the transaction cost.

H. Solidity

Solidity is the object oriented programming language and it has syntax which resembles mostly to the languages like the CPP, python and JavaScript. Generally the remix IDE is used to write the smart contracts in the solidity. It has various inbuilt tools which helps the environment more active and useful for handling the solidity programming environment.

IV. BLOCKCHAIN QUALITY ATTRIBUTES

A. Increased Capacity

The blockchain can remarkably increase the overall capacity of the entire network. As it runs on the principal of distributed computing, the overall power of the entire network can be a plus point which can offers us the overall great power and it's more effective than centralized systems.

B. Better Security

Blockchain technology provides more security to the data compared to the central data storage, as we don't need to worry about server down time. Even if we want to hack the overall blockchain network we need to gain the access the 51% access of the network and which is quite impossible to perform. And blockchain is secured by many number of the active nodes in the blockchain network.

C. Immutability

Immutable ledgers is one of the important aspect in the blockchain technology. Usually any database which has a central system is prone to attack. In the blockchain the data is stored as in the distributed ledgers system which will make it more to tamper proof and transparent among all the parties. It has the smart contracts which are self-executing scripts and they will help to make the overall blockchain network more stable and immutable. As all the ledgers are kept up to date and has all the copies shared among all the nodes in the corresponding blockchain network. [6]

D. Faster Settlement

In the traditional systems usually the settlement cost is more and as its central authority based systems the settlement time is more compared to the distributed networking in the blockchain. Here in the blockchain we do not need to depend on the central authorities and it will overall decrease the settlement cost and time also increase speed and efficiency of transactions.

E. Decentralized System

Decentralized systems usually provides us many advantages over the traditional centrally managed systems. Blockchain can provide the overall power to the actual owner of the data by giving him unique ID to access the data over the blockchain network. Blockchain technology provide the great functionally with the overall tamper proof data and it will help all the parties to keep the transactions in the network transparent. It can help to bring the massive and remarkable changes in the current industries.

V. ALGORITHM

A. Proof Of Work (POW): Introduction

Proof of Work (POW) is the consensus algorithm which is used by many of the popular cryptocurrencies. Using this algorithm different parties reach to the consensus like to add the corresponding the transaction to the corresponding blockchain or not. Here the difficulty can be increased to solve the cryptographic puzzle and it can be made more challenging to solve by increasing the more number of leading zero's in the overall cryptographic puzzle. It usually refers to the overall computing power a specific user has and if the user can solve puzzle in lesser amount of time he will be awarded with the certain amount of cryptocurrencies. More advanced algorithms to proof of work are proof of concept (POC) and proof of statement (POS).

B. Proof Of Work: Working

It is used to confirm transactions and once it is confirmed new blocks are added to the blockchain. Mathematical puzzle requires more amount of computational power and resources. The solution to the proof of work or mathematical equation is called as the 'hash value'. The benefits of using the POW is the anti-dos attacks defense and the low impact of stake for the mining possibilities

The following are the types of puzzle:

1. Finding hash function.
2. Finding input knowing the corresponding output.
3. Presenting a number as the multiplication of other two numbers.

VI. BLOCKCHAIN IN EDUCATION

In education systems the certificates states that the achievements of the learners or educators and different activities are mostly issued on paper or other physical formats. Paper certificates are prone to tampering and forging. The digital certificates stored onto the blockchain networks are difficult to forge and they are tamper-proof [2]. Here we do not need the third parties to verify the details. Here we don't have central data base to store all the data or to maintain the registries for longer period of time. Blockchain technology supports protection against counterfeit certificates and simplified verification of Certificates with lesser amount of the resources. Blockchain consist of three steps while considering the digital certification and storing the data onto the blockchain.

First we need to identify the certification. Then these certification authorities have to issue certificates to educators and learners. And lastly the main task is the verification of certificates by educators and learners. Mostly the learners receive the paper certificates with built-in security features, so maintaining the integrity and the immutability of the data can be challenging task. It can be resolved using the blockchain technology in education system. Educators only receives the copies or notarized work of learner's paper certificates and to verify these certificates the educators need to rely on the central authority and it is time consuming process, so the blockchain technology can be effectively used in education system. Currently the Sony and University of Nicosia has successfully implemented the blockchain in education for storing the digital certificate and issuing the degrees. [1]

VII. IMPLEMENTATION OF BLOCKCHAIN IN EDUCATION

A. Digital Certification: Working

Initially the learner inputs his personal information with the Unique id and then the information is kept on to the learner's Blockchain. Later the data sent for the verification to the respective verifying institution. After successful verification of the data the success token is sent to the learner and then the data is safely stored onto the corresponding of the given type of the institute's private blockchain network.

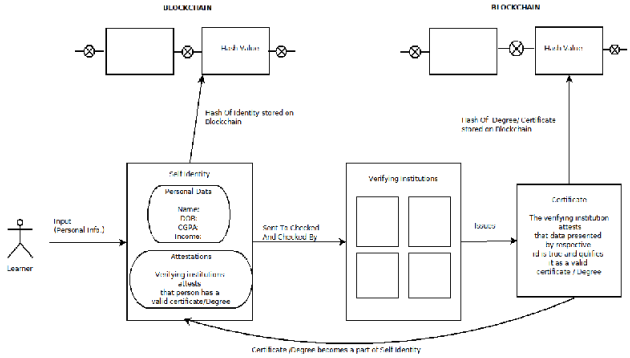

Fig.1 Digital certification overview

B. Important Characteristics of Digital Certificates

The certificates are stored digitally onto the blockchain network with the generated hash. Here the issuer and the verifying authority has their own separate blockchain for storing the digital certificates. Over the regular certificates they are stored digitally on to the thousands of the computers which will make it more secured and powerful than the normal certificates. It requires fewer resources to maintain, issue and access than the existing digital certification.

C. Digital Signature

It can be specifically used to verify that it's signed by the specific and valid user. As the digital signature consist of the time stamp which is indeed generated by the specific user and so it cannot be modified or tampered. Here the user uses the private key to digitally sign the document and using his public key the recipient can verify the identity and confirm the document. Digital signature is more secured than the electronic signature and can be used to keep data more securely.

D. Benefits Over Traditional Approach

Without the central authority we can apply the blockchain in education system which can be used in the formal assessment and storing the digital certificate and the degrees. Informal learning data such as the research experience, skills and the on-line learning experiences and the individual interests can be easily stored onto the blockchain is safer format. Private information of learners and educators can be stored onto the blockchain networks in the immutable form.

E. Distributed Database In Educational Environment

Blockchain ledger is distributed so any changes made to them can be monitored by the remaining candidates, so it can reduce the problems like degree frauds.
As the overall data is stored on distributed blockchain network, all the learners can keep the track of the details so the overall tampering of the actual data can be avoided, as the blocks on the blockchain cannot be altered once they are deployed. Using the proof of work algorithm the data stored on the distributed blockchain network can be verified and then it'll be stored on the network with valid credentials.

VIII. MATHEMATICAL MODEL

Consider S as the set of details of the learners to be stored on blockchain.
S -set of input, output and functions.
I - set of input with the details of the students or staff
O-set of output consisting the conformation of the data on blockchain smart contract.

I = {Index,Timestamp,Nonce,Hash,Previous Bock Hash}

- Index - Total blockchain length +1.
- Timestamp – creation time.
- Nonce – per-decided difficulty for hash calculation.
- Hash – current block hash.
- Previous Block hash – hash of previous block in blockchain.

F = set of functions
F={createNewBlock,CreateNewTransaction,ProofOfWork, ChainIsValid }

- createNewBlock() – adding new block on blockchain
- createNewTransaction() – adding details to block.
- ProofOfwork() – consider the check point for nonce calculation with specified difficulty.
- ChainIsValid() - consensus algorithm used for finding valid chain.

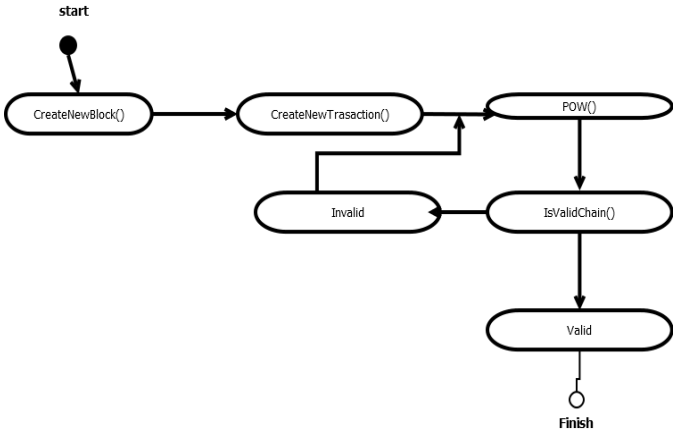

Fig.2 State Diagram: Functions working Overview

O = {Data, Learner's Id, Specific hash}

1. Data - Block-wise details stored onto the blockchain.
2. Learner's id and detailed information with records.

IX. RESULTS

A. Block

The fundamental element of the blockchain considered as the block. It can consist of one or many records which can hold the records for multiple students. It has the details as the block number, nonce value, the details about the students and the respective hash value of the current block.

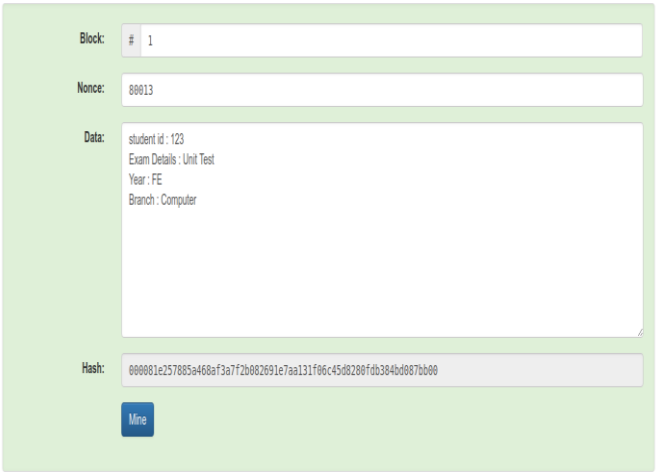

Fig.3 Block Structure

B. Blockchain with valid input

Here the respective details of the students are stored in the educational blockchain. The previous block hash is applied as the input for the next block. The nonce calculation will differ regarding changes in the actual data.

Fig. 4 Student details on blockchain

C. Blockchain with tampered input

The previous block hash is applied as the input for the next block with proper hash value. The nonce calculation will differ regarding changes in the actual data. When user tries to modify the actual stored data on blocks the alert will be shown in red color, depicting the tampering in the actual stored data.

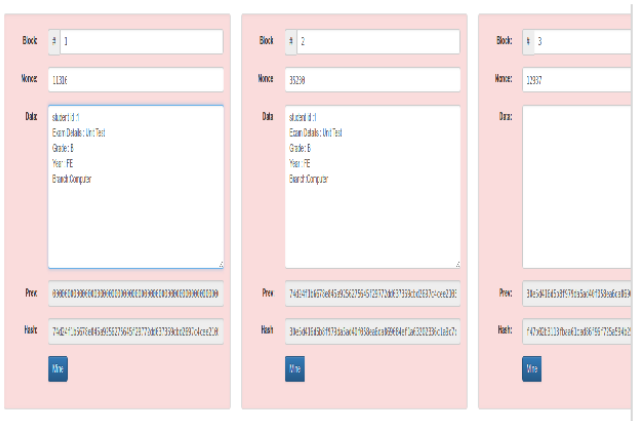

Fig.5 Student details on blockchain with tampering

X. ADVANTAGES

1. Immutability can be provided as the blocks that are added to the blockchain cannot be modified once they are created.
2. Storing the data on to the blockchain is highly secured as the user is provided with the unique id that can be generated using the current time-stamp.
3. Blockchain technology helps us to increase the speed of the operations and it will help educators to store the data quickly.
4. They can be easily scaled up-to the large educational systems by considering the consortium or the public blockchain.
5. Most of the resources are open source which will help investors for less capital investment.

XI. SYSTEM WORKING OVERVIEW

A. Learners' Module

The learner consist of their own ID which will help them to uniquely identify them on blockchain network. They are provided with the different rights while storing the data on to blockchain .Learners can inert the theory attendance, insert assignment marks, insert lab and test attendances. After confirming the identity of the learner through the verifying institution he can successfully store the data onto the blockchain using the smart contracts.

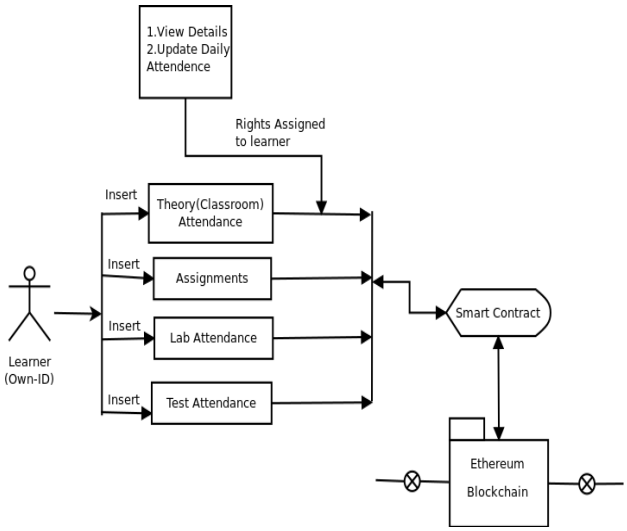

Fig. 6 Learner's Module on Blockchain

B. Staff's Module

The Staff/Educators has their own private ID which will help them to uniquely identify them on blockchain network. They are provided with the different rights while storing the data on to blockchain. Staff can assign lab marks, update test marks as well as the theory and the assignments submitted by the earners. After confirming the identity of the learner through the verifying institution educators can successfully store the data onto the blockchain using the smart contracts.

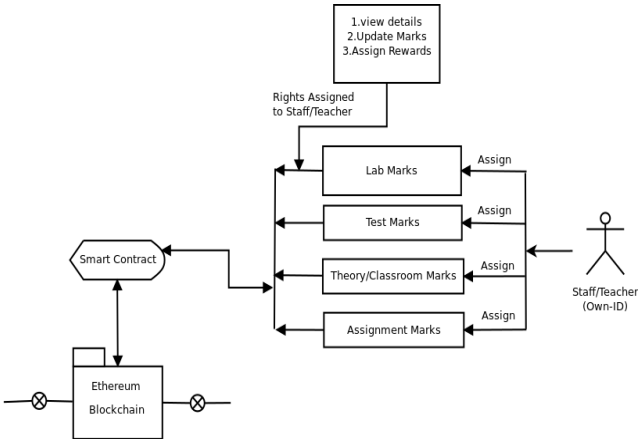

Fig. 7 Staff's Module on Blockchain

XII. FUTURE EDUCATIONAL APPLICATIONS

1. "Learning is earning" can be applied by considering the digital currencies in the learner's wallet and it can motivate learners to join different educational activities.
2. Formative assessment is kind of challenging as we need to record all the details of the learner' activities. It can be made more simplified and can be used in more systematic way in educational system.
3. We can maintain the digital identity of the different these parties safe and it can be securely stored on to the blockchain network.
4. The smart contract will reduce the overall need of the involvement of the third-party and increases the overall performances.
5. The more number of the educational issues can be solved using the smart contract based blockchain systems.
6. Every detail of teaching and learning can be made more simplified using the blockchain techniques.

XIII. CONCLUSIONS

Blockchain works on distributed technology. In that different cryptographic techniques and different consensus algorithm such as proof of work (POF) is used. Blockchain provides decentralization, tamper-proof data storage, easily scalability of the data and also provides immutability so it can be effectively used for education system. Blockchain can be used for storing the certificates and degrees.

It can reduce the overall frauds and tampering of the degrees and certificates. Here smart contracts can be designed and deployed on to the Ethereum blockchain that can be designed using the solidity programming language. Blockchain can be applied to private, public and consortium sectors depending upon the usage and the scope of the blockchain. Education system can take benefit of this scalability of the blockchain and can be effectively useful in the educational institutions.

REFERENCES

1. Guang Cheng, Bing Xu, Manli Lu and Nian Shing Chen, Exploring Blockchain technology and its potential applications for education Springer [2018].
2. Rishav Chatterjee, Rajdeep Chatterjee, Overview of the emerging Technology: Blockchain .IEEE [2017]
3. Alexander Grech, Anthony F. Camilleri, Blockchain in Education, IEEE [2017]
4. Satoshi Nakamoto,Bitcoin: A Peer-to-Peer Electronic Cash System,.White paper.[2008]
5. F. Tschorsch and B. Scheuermann, Bitcoin and beyond: a Technical Survey on decentralized digital currencies, IEEE [2016]
6. Data Flair , Weblink : https://data-flair.training/blogs/types-of-blockchain,[2018]
7. Allen Ezell and John Bear.Blockchain for Education: Lifelong Learning Passport – dotmagazine.[2018]
8. D. Eastlake, 3rd and T. Hansen,US Secure Hash Algorithms andSHA (Informational). [2011]
9. G. Wood, Ethereum: A secure decentralized generalized transaction Ledger used in blockchain, Byzantium version,[2018].
10. Agility A. Proof-of-Knowledge:same Blockchain, different Available at:https://tail.aqquadro.it/proof-of-knowledge.[2017].

AUTHORS PROFILE

Mr. Akshay S. Karale, pursuing ME in computer engineering at Marthwada Mitra Mandal's College Of Engineering, Pune. Prominently works on Ethereum blockchain development and Machine learning.

Prof. Harmeet Khanuja, works as Professor in Department of computer engineering at Marthwada Mitra Mandal's College Of Engineering, Pune, She's done her masters in computer engineering form Pune Institute of Computer Technology and currently pursuing her Ph.D.