Incorporation of Blockchain in Student Management System

S.M.K.V. Pramod Kumar, K. Kiran Kumar, R. Sai Krishna, P.S.G. Aruna Sri

Abstract: ***Blockchain is the trending technology which was proposed by Satoshi Nakamoto. It is viewed as a prospect by businesses, for example, fund, training and medical services, because of its decentralization and non-altering highlights. In this paper we are going to implement a new approach for storing student data and a way to verify student certificates via blockchain technology. In the present student management system substantive data symmetry exists among colleges and utilizing organizations. The features of blockchain are transparency and immutability are being explained and their usage in the following paper. The student data can be stored in the Blockchain network in the Hyperledger framework which includes the roles of students, universities. This offers a critical endeavour on the use of blockchain innovation to Student-Management participation as a pilot advancement for innovation sending.***

Index Terms: Blockchain, Hyperledger, Student-Management-System.

I. INTRODUCTION

The present Student Management System (SMS) needs consistent assembly among colleges and organizations. The present university framework isn't efficient with centralized way of storing the data. To prevent tampering of student data which is most important blockchain technology can be implemented in SMS.

The ledger technology or blockchain technology lays a good pavement for the implementation of SMS with the help of its features like transparency, immutability and distributed way of storing the records.

Every organization has important data which needs to be protected. The existing system which is centralized storage is the one which needs backups of the data stored in the central sever. On the other hand, if the data (may be a file or folders) modified in the server the updated file will be accessed by everyone which has to be prevented. Blockchain technology helps the organizations to store the data in each system connected in the network. With this way of storing the data a file cannot be modified at ease. For example, if a file is modified in a system it cannot be modified on all the systems in the network because each system has its own copy stored in database which is known as decentralized and distributed ledger. This technology is called as blockchain because the data is in form of blocks and all the blocks are connected to each other ultimately forming a chain of records. The main use of this technology is to prevent third party members or organizations in a transaction. With help of blockchain technology cryptocurrencies like Bitcoin, Ethereum etc. came in to existence. This can be the future way to transaction which include only sender and receiver and no third parties to make a transaction. A transaction may be in form of money exchange, certificates etc. In this paper we assume student records are stored in form of blocks in blockchain network. Consider a case where a student has joined in another institution for higher education. SMS helps the foreign or new university to verify the certificates of the students. The paper proposes that the student has a wallet which contains the certificates or information regarding the courses which are completed [1]. When the student is about to join a higher education university, that institution shall join the network and validates the certificates produced by the student. For the validation process 2-2 multi signature protocol is used.The paper discusses the existing inconsistency of information between universities and employer corporations, an incomplete credit system for students. Information transparency, validity and applicability can be ensured with the help of blockchain technology [2].Smooth integration is accomplished between students, academic institutions and employer corporations, strengthening the utilization and transparency of educational and employment organisations.The paper describes a blockchain technology application that is Bitcoin which is a trust-free system. For money exchange, a peer-to-peer network system is proposed. There is no need to recognize peers and they can still leave and join the network in their interest. Blocks which are a transaction record are officially accepted or verified by casting a vote with the peer's CPU. This consensus mechanism can enforce any required rules and incentives [3]. This paper proposes a framework based on blockchain to implement processes of insurance transactions as smart contracts. Studies performed to review the robustness showed that the parameters used during the emergence of blockchain should be specially selected as they directly impact the latency of the network. The repository is not encrypted but deep level access control can be used to encrypt it. Every smart agreement would have its own set of validating peers and this can be extended even to the level of exchanges, allowing separate set of validating peers for each exchange [4].

Revised Manuscript Received on April 07, 2019.

S.M.K.V. Pramod Kumar, Department of Electronics and Computer Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India.

K. Kiran Kumar, Professor,Department of Electronics and Computer Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India.

R. Sai Krishna, Department of Electronics and Computer Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India.

P.S.G. Aruna Sri, Associate Professor, Department of Electronics and Computer Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India.

The paper proposes a system on how to store the private information of an individual. Private information should not be trusted by foreign entities where they are susceptible to attack and misuse. Instead, users have to own and maintain control of their data without sacrificing the quality of security or restricting the ability of businesses to produce customized services. The proposed system allows this by combining a blockchain re-purposed as an access-control user. Customers are not needed to trust foreign entities and are always aware of the information gathered about them and how that is used [5].

This paper provides a block chain-based E-auction system that ensures privacy, non-repudiation, not modifiable electronic contacts. Because of the sophistication of the contract, buyers come in smart contracts for secured orders, and might call the wrong contract function. For instance, reveal function is accidentally called by the buyer to open all auctions, so the auction must be terminated and reconfigured. We will set the oversight decision for multiple functions for this sole purpose and perform the function before first calculating if this function can be administered by the caller [6].

In this paper the author suggested new information sharing block chain system. It brings many benefits to the management of the distribution chain. Transaction data should not usually be disclosed to third-party where they are vulnerable to misuse. By combining the block chain with a better encryption solution, the proposed platform makes this possible [7]. Moreover, the block chain identifies users as their encrypted data's owners. Organizations or firms can focus on using data without worrying about properly managing and compartmentalizing it.

In this paper, the author proposed a system to secure one's identity as many social media and online websites are used to communicate and to safeguard against infiltration, online abduction of characters and to provide the person's real public image. Since the users can sign up for the account on social media websites using fake information using a system like TURS, the users can protect their identity against theft and provide an authentic user-related reputation for a trusted network [8].

The author presented a group of hardened smart contracts which can be used to provide blockchain-based e-commerce alternatives for tiny, medium size businesses in accordance with one another and an identification system. The processes that companies and entrepreneurs use can transfer to Syscoin without any need to redefine the way people are working today. Syscoin's is a mix of unique features in an framework that enabled strong security through merged-mining and low inflation enabled permissionless payments and services to be used today in commercial enterprises and enterprises as well as providing Syscoin token holders an investment suggestion [9].

Decentralized digital content distribution system based on blockchain has been proposed and a prototype has been developed. The proposed system does not currently have an incentive mechanism for calculating mining. This means that when each minor calculates the hash value, no cost can be protected. In the case of the Bitcoin system, a little BTC would be paid to the miner as an encouragement for the utilization of his resources [10].

II. Methodology

The proposed system uses decentralized and distributed network where the student data is stored in form of blocks. These blocks are connected to one another forming a chain of records. We implement this system using Hyperledger fabric network because this is a type of system that belongs to organisation so that data should be in private mode. There are other networks such as Ethereum, but they are used to implement systems which are related to public data.

Hyper Ledger: The Hyperledger is a huge exploratory improvement regarding open and standard blockchain innovation. With the help of the Linux Foundation, Hyperledger has pulled in the cooperation of numerous specialized and money related organizations. In March 2016, under the sponsorship of the Linux Foundation, the Hyperledger venture formally joined the source code contributed by individuals from Block stream, Digital Asset Holdings and IBM into another code base to frame another undertaking level blockchain base. This code accumulation is called Hyperledger Fabric. This is expected to exchange, keep up, and recover data on explicit resources inside an agreement organize. Hyperledger allows the usage of plugin modules, which will additionally advance the use of Smart Contracts for different business situations.

The blockchain in Hyperledger Fabric can be comprehended in the model of state-machine replication, where an administration keeps up some state and customers conjure tasks that change the state and produce yields. The blockchain copies a "trusted" registering administration through an appropriated convention, kept running by hubs associated over the Internet. The hubs share the shared objective of running the administration yet don't really confide in one another.

Block: A block is the one which contains data of the transaction and ready to join the network. A block contains information like block id, current hash, previous block hash, message, date etc depending upon the application. The initial block in a blockchain is known as Genesis block where the previous hash value of this block will be 0 since it doesn`t have any previous blocks. The hash value of this block will be previous hash value of the next block and it continues.

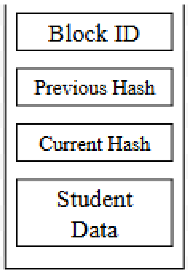


Fig.1 Block and its contents

Blockchain: A chain formed by linkage of the blocks based upon their current and previous hash value [11].

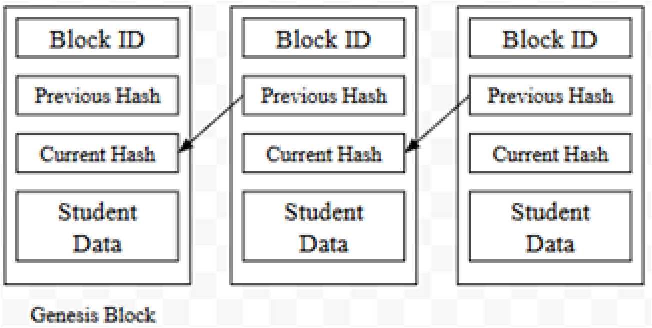


Fig.2 Blockchain structure

Certificate Authority (CA): Responsible for authority of organisation, also called Member Service or Identity Service.
Transaction: Implements chain code on Ledger and performs a data or smart contract exchange.
Orderer: Responsible for agreement administration, sorts unverified exchanges, gives the worldwide request for affirming.
Chaincode: The application rationale code on blockchain, obtained from a Smart Contract, running in a confined compartment condition.
Ledger: Contains the blockchain (with all exchange data), and the World State.
World State: A key-esteem database, causes chain code to store the worldwide status of exchanges.

III. ALGORITHMS USED IN BLOCKCHAIN

SHA256: The activities inside the SHA256 hashing calculation are performed on words that are 32-bit long utilizing eight working factors names as A, B, C, D, E, F, G and H that are additionally 32-bits long. Consequently, the word length of the SHA256 calculation is of 32 bits. The qualities for these working factors are figured at each round and this procedure proceeds till 64 rounds have been The SHA256 Hashing Algorithm finished. In all respects critically, it ought to be noticed that all increases in the SHA256 hashing calculation are performed modulo 2^{32}. Henceforth, the user ought to translate all augmentations referenced from now on in this content as increases performed modulo 2^{32} SHA256 additionally takes a 256-piece initialization vector which is fixed for the principal message square. A transitional message digest acquired toward the finish of the initial 64 rounds which fills in as the for the following message square. The SHA256 hash work is assembled utilizing the Davies-Meyer development where the IV is added to the yield toward the finish of 64 rounds. Along these lines, after 64 rounds of the message pressure capacity and expansion of the calculation delivers a halfway message condensation of 256 bits. After the whole message squares have been hashed, an incentive on 256 bits is gotten that is the last message review of the information message. The SHA256 hashing calculation is hence practically identical to a square figure with a 256-piece message square size and a 512-piece key (message obstruct) that is ventured into sixty-four 32-bit round keys utilizing the message scheduler for every one of the 64 rounds of this figure. The Bitcoin convention exploits the torrential slide property of the SHA256 calculation that makes it exceptionally hard for assailants to discover alternate routes in finding another square that begins with the stipulated number of 0s. The following area will bring a profound plunge into the internal parts of the SHA256 calculation.

RSA: RSA algorithm works using public key and private key. The public key is exchanged between the person who wants to send the information or make a transaction. The sender encrypts the data using the combination of public key and private key which is known only to him. Then the receiver receives the data and decrypts it using public key sent by the sender and the private key of the receiver. RSA decryption works on cipher text.
Every person or group that wants to be involved in communication using strong encryption needs to produce a couple of codes or keys, namely public key and private key. The key or code development process is described below.
Select two big prime numbers, i and j, to produce the RSA module (x). Determine the value x = i*j. Let n be a large number for solid encryption, usually at least 512 bits.
The number e must be higher than 1 and lower than $(i - 1)(j - 1)$. No common factor must be discovered for e and $(i - 1)(j - 1)$ except 1. The variables e and (i-1) (j-1) are co-prime numbers.
The RSA public key is formed by the pair of numbers (x, e) and publicly disclosed. While x is part of the public key, the difficulty of factoring a big prime number ensures that the attacker is unable to find the two primes (i & j) used to obtain x in the limited amount of time. That's RSA's endurance.
With the help of variables i, j and e private key d is produced which is known only to the user. There is a unique number d for given x and e. We can say that the inverse modulo of (i-1) (j-1) as d which means that d ranges in between (i – 1) (j - 1). The 1 modulo (i-1) (j-1) is obtained when d is multiplied to e.

IV. FLOW CHART AND SEQUENCE DIAGRAM

The below flow chart describes the flow of certificate validation between two universities. First student applies for a new university of higher education. The new university reviews the application and contacts the old university.
To verify the certificates, the old university sends a request to join the blockchain network of the university. The new university then joins the network of the old university. Then the old university verifies the records in their database, and it validates the certificates.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

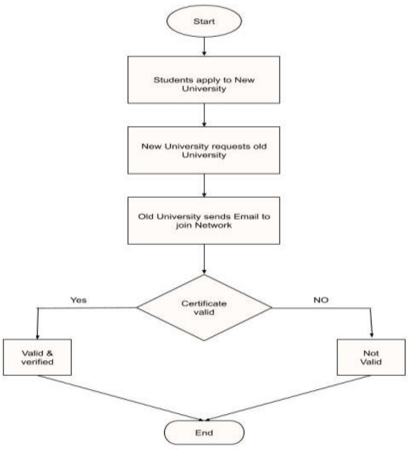

Start
Students apply to New University
New University requests old University
Old University sends Email to join Network
Certificate valid
Yes
NO
Valid & verified
Not Valid
End

Fig.3 Flow chart of the certificate validation

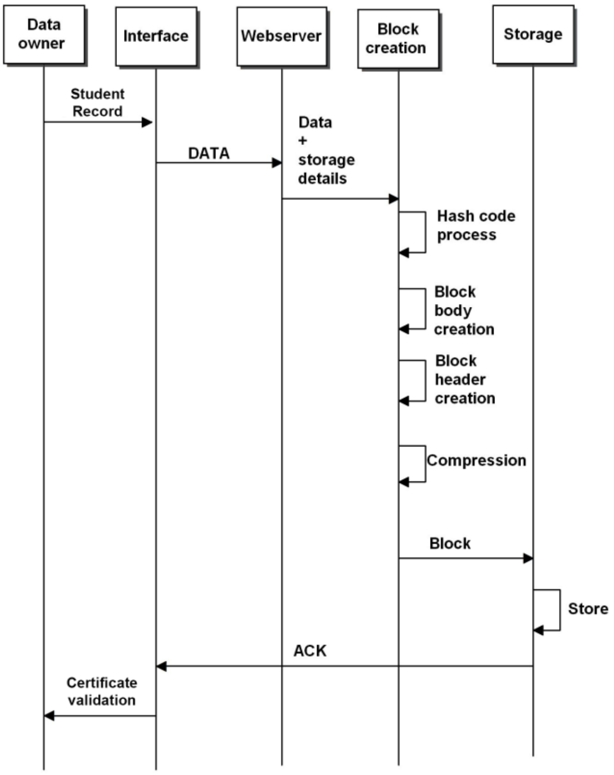
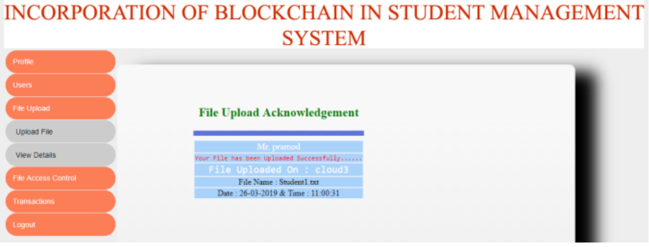


Fig.4 Sequence Diagram for storing blocks in blockchain

The above sequence diagram describes the storage of the block in blockchain. Each student record is treated as a block in the blockchain. The block consists block header and student data. The block header consists hash code of the previous block, current hash value, time stamp and nonce. First block is called genesis block and doesn't contain any data. The data owner must upload student records in blockchain network and creates a request. The web interface receives the data and sends to the web server. When the web server receives the data entering request a hash code is generated for that data. Since we treat each student record as a block a new block is created. Once the block is created the block address is created. The block is sent to the network for storage. Once the block is stored successfully acknowledgement is sent to the data owner. Then the certificate can be validated anytime in future.


INCORPORATION OF BLOCKCHAIN IN STUDENT MANAGEMENT SYSTEM

File Upload Acknowledgement

Mr. pramod

Your File has been Uploaded Successfully......

File Uploaded On : cloud3

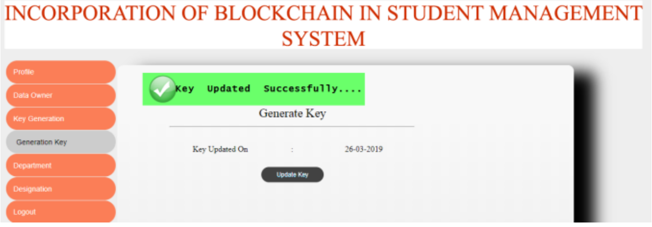
File Name : Student1.txt

Date : 26-03-2019 & Time : 11:00:31

V. Results

Fig.5 Data owner uploads a record to the network

The data owner uploads a file into the network and receives an acknowledgement along with the time stamp.


INCORPORATION OF BLOCKCHAIN IN STUDENT MANAGEMENT SYSTEM

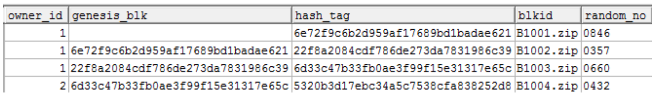
✓ Key Updated Successfully....

Generate Key

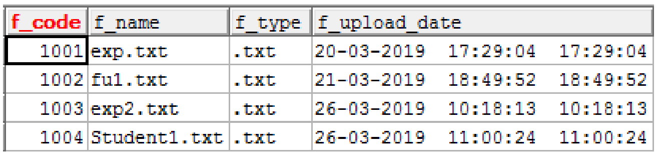
Key Updated On : 26-03-2019

Fig.6 Generation of the key for the uploaded record.

The hash code is generated for the file uploaded by the data owner.



owner_id	genesis_blk	hash_tag	blkid	random_no
1		6e72f9c6b2d959af17689bd1badae621	B1001.zip	0846
1	6e72f9c6b2d959af17689bd1badae621	22f8a2084cdf786de273da7831986c39	B1002.zip	0357
1	22f8a2084cdf786de273da7831986c39	6d33c47b33fb0ae3f99f15e31317e65c	B1003.zip	0660
2	6d33c47b33fb0ae3f99f15e31317e65c	5320b3d17ebc34a5c7538cfa838252d8	B1004.zip	0432



f_code	f_name	f_type	f_upload_date
1001	exp.txt	.txt	20-03-2019 17:29:04 17:29:04
1002	ful.txt	.txt	21-03-2019 18:49:52 18:49:52
1003	exp2.txt	.txt	26-03-2019 10:18:13 10:18:13
1004	Student1.txt	.txt	26-03-2019 11:00:24 11:00:24

Fig.7(a) Format of the database which stores the records

Fig.7(b) Block data which stores hash values and block ID

The data is stored in the data base in the above format. The data base includes file code, file type, file upload time stamp, file name, data owner id i.e. the id of the owner by whom the file is uploaded, previous hash code, current hash code, block id and nonce.

VI. Conclusion and Future Scope

Implementation of blockchain in student management system to store the student records in form of blocks and also validation of student certificates between universities is proposed.

In future this paper can be developed by proposing a way to implement fully functional student management system which include attendance, student marks, student payment receipts towards the university etc.

REFERENCES

1. Aida kamiali, kristjan koi, marjan heriko, "eductx: a blockchain-based higher education credit platform", ieee access 2018.
2. Gill green, qin liu, hongming zhu, "education-industry cooperative system based on blockchain", hoticn 2018, ieee 2018.
3. Satoshi nakamoto, "bitcoin: a peer-to-peer electronic cash system".
4. Sushmita ruj, kwok-yan lam, “a blockchain framework for insurance processes”, bsc 2018, ieee 2018.
5. O.nathan, p. Alex sandy,”decentralizing privacy using blockchain to protect personal data”, spw 2015 ieee 2015.
6. I. Chang lin, y.h. Chen, "blockchain based smart contract for bidding system",icasi 2018 ieee 2018
7. M. Nakasumi,"information sharing for supply chain management based on block chain technology" ieee cbs 2017.
8. A. Yasin, l. Liu,"an online identity & smart contract management system", ieee acsac 2016.
9. J. Sidhu,"syscoin: a peer-to-peer electronic cash system with blockchain-based services for e-business",ieee 2017
10. K. Jay, a. Akutsu,"the blockchain-based digital content distribution system", icbdc ieee 2015.
11. P.s.g. Aruna sri, d.l. Bhaskari, "a study on blockchain technology", ijet 2018.

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*