iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IV **Month of publication:** April 2020

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

Secured E-Assessment using Blockchain

Yash Karande[1], Shubham Karad[2], Abhishek Aswale[3], Aniket Lamage[4], Rakesh Shirsath[5]
[1, 2, 3, 4]*UG Scholar,* [5]*Professor, Computer Engineering Department, Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India*

Abstract: ***The main aim is to provide a blockchain-based system for the evaluation and storage of online examination results. Also, the generation of certificates upon successful completion of the test. We illustrate how without any central trusted entity we can build a self-sustained examination system on top of blockchain for a fair evaluation. The result generated for each and every test undertaken by every student will be stored on the blockchain for transparency. The most important point here is to make sure data integrity is maintained.***

Keywords: Decentralized applications, Distributed databases, Nodes, Hash, Block, Time Stamp, Nonce, Consensus, Forks, Encryption, Token, Proof of Authority.

I. INTRODUCTION

To build a blockchain-based evaluation and storage system for online examination. In this system the candidate marks the relevant answers to the questions. Those answers will be evaluated on the chain code provided by Hyperledger Fabric. The evaluated result will be stored on the blockchain, along with the student name, id, test id, etc attributes. With this solution, we are addressing the issues with the current examination system. The traditional examination system is purely central making it highly susceptible to data manipulation. There is a lot of involvement of humans for evaluation, storing of the exam. Since the data is stored in the database which is under the control of a database administrator, again bringing human interference which is susceptible to bribery or threats. So, the objective is to make the evaluation an automated process and store results on blockchain to maintain data integrity.

II. LITERATURE SURVEY

About a decade ago Satoshi Nakamoto, the person/group behind Bitcoin, presented how blockchain can be used to solve the double-spending problem and how maintenance of records can be done using a distributed peer-to-peer linked database. Bitcoin orders transactions and group them with the timestamp and stored in a constrained-size structure so call blocks. A blockchain can be considered a distributed database where the committed blocks are immutable. The database is organized as a list of ordered blocks one after another, having the hash of previous and next block stored along with the data and timestamp so that a chain like structure is accomplished. [1] Blockchain is being used in other fields beyond cryptocurrencies, with Smart Contracts (SCs). A smart contract or SC is an agreement between parties that are engaging in any of the transactions. Though these parties don't trust each other, the agreed terms are automatically enforced on all the stakeholders. A well-known method to do it is Proof-of-work (PoW). PoW requires one to solve computationally complicated and complex problems like finding hashes with specific patterns so that the authentication and verification are ensured. Proof-of-Stake (PoS) protocols split stake blocks proportionally to the current wealth of miners (Pilkington, 2016). In this way, the selection is fair most of the time and prevents the domination of the wealthiest participant present on the network. [2] The data stored in a blockchain is resistant to modification due to the cryptographic hash. If data of one block is modified, all blocks afterward should be regenerated with new hash values. Now, consider that for millions of peers that are connected to that network and have the whole copy of the blockchain, it's practically impossible to do so. This feature of integrity and immutability is fundamental to blockchain-based applications. Maintenance of peer-to-peer (P2P) ledgers for cryptocurrencies has become one of the best applications based on blockchain. PoW uses an intentional computationally high costing algorithm which increases the difficulty identification of any foreign Sybil attack to a high level. Due to this, a large hardware investment required for any particular network participant. The peers who successfully create any blocks will receive rewards for their expenditure of computation power. Even though any peer has a lot of computational power, the profit is in making blocks instead of attacking them. This mechanism demotivates the intruders, resulting in protection of this decentralised ledger. [3]
A purely peer-to-peer version of electronic cash allows payments to be done without any intermediate financial institution. The currency can be directly sent from one party to another. Double-spending can be prevented by the use of digital signatures, it also provides a type of enforced trust on the parties included in a transaction. Double spending can be solved by hashing the transactions using the current timestamp on an ongoing chain of hash-based proof-of-work.

It will form a record that cannot be manipulated without redoing the PoW. The longest chain serves as proof that it came from the largest pool of CPU power and the events are witnessed. The network requires minimal structure to be followed. Messages are broadcasted to all the peers on the best effort basis, the peers can leave and re-join the network at will. All the peers need to accept the longest proof-of-work chain to get proof of what happened while they were not connected. The hash begins with a number of zero bits, algorithms such as SHA-256 are used to hash the data. Implementation of proof-of-work by incrementing a nonce in the block till the value is found which shows the block's hash. As all the blocks are chained, the work to change any block will need to redo hashing for all the blocks after that specific block. [4]

Blockchain has already shown its potential for transforming traditional industry with its characteristics such as decentralization, persistence, anonymity, audibility, and integrity. [5]

Another great perk of blockchain is decentralized apps or so-called dApps. For an application to fall in the criteria of a dApp, it has some of the constraints like the application must be completely open-source, it must operate autonomously, and with no entity controlling the majority of its tokens. The application may adapt its protocol in response to proposed improvements and market feedback but all changes must be decided by a consensus of its users. Also, the application's data and records of operation must be cryptographically stored in a public, and it has to use a cryptographic token by which the miners/farmers should be awarded for their contribution. The classification is of any dApp is done in 3 categories Type I, Type II, and Type III. Type I decentralized applications have their own blockchain. Bitcoin is the most famous example of a type I decentralized application but Litecoin and other "alt-coins" are of the same type. Type II decentralized applications use the blockchain of type I decentralized application. Type II decentralized applications are protocols and have tokens that are necessary for their function. Type III decentralized applications use the protocol of type II decentralized application. Type III decentralized applications are protocols and have tokens that are necessary for their function. [6] Anyone can operate and participate in the network by just spending CPU cycles and demonstrating a PoW in a "Permissionless" blockchain such as the one used by Bitcoin cryptocurrency. In a "Permissioned" blockchain model, the participants are validated and are only given specific access that is allowed by the established identities. Hyperledger uses a "Permissioned" based model which is a collaborative effort to create an open-source and enterprise-grade distributed ledger codebase and framework. A permission-based blockchain model uses Proof of Authority or (PoA). Some of the key features of Hyperledger fabric are, Golang implemented smart contracts (called as Chaincode), pluggable consensus protocol, Security support through certificate authorities (CAs) for TLS certificates, enrollment certificates, and transaction certificates, support for REST APIs and CLIs. It has a life cycle as follows Deploy transaction, Invoke transaction, Query transaction. [7]

The Interplanetary File System (IPFS) is a peer-to-peer distributed file system. It connects to all computing devices with the same system. IPFS can be considered as a single BitTorrent swarm, exchanging objects from a single Git repo. It makes a generalized Merkle Directed Acyclic Graph that is used by all of the version control systems, blockchains and even permanent web. IPFS provides a very high throughput content-addressed block file storage model with content-addressed hyperlinks. IPFS does not have a single point failure and the nodes do not trust each other in the network. It is a next-generation file sharing system that can also be used as a global, mounted versioned namespace and file system. IPFS has the potential to replace HTTP and make the traditional web distributed. [8] A web-based exam system where the participants can access it through the help of the internet or intranet can be called as an online examination system. The main aim of the online examination system is to reduce the overall time taken for evaluation, remove any loose ends by eradication human intervention and generate more accurate results. [9]

III. ALGORITHM (SHA-256)

An n-bit hash is known as a map from arbitrary length messages to n-bit hash values. The n-but cryptographic hash has properties like oneway hashing and collision resistance. Digital signatures use such algorithms to maintain security. Some of the current popular hashing algorithms include n = 128 (MD4 and MD5), n = 160 (SHA-1) which cannot be trusted beyond 64 or 80 bits of security. The goal of Advanced Encryption Standard (AES) is to encrypt the given data with 128 or 192 or 256 bits of keys that are currently in use. SHA-256 works the same as MD4, MD5, and SHA-1: The message to be hashed is first padded with its length so that it'll be a multiple of 512 and then that generated message is parsed into message blocks of the length of 512 bit. The H(0) which is the initial value is fixed and the further hashes are calculated as follows,

$$H^{(i)} = H^{(i-1)} + CM^{(i)}(H^{(i-1)});$$

where C is the SHA-256 compression function and + means word-wise mod 232 addition. H(N) is the hash of M.

The SHA-256 compression function uses a 512-bit message block and a 256-bit intermediate hash value, it is basically a 256-bit block cipher algorithm. And it encrypts the intermediate hash value using the message block as key. SHA-256 message schedule and SHA-256 compression function are the main components.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

Computation of the hash of a message begins by preparing the message:

1) Padding function: Suppose the length of the message M, in N bits. Append the bit to the end of the message, and then k zero bits, where k is the smallest non-negative solution to L+1+k = 448 mod 512. So that it can be appended to the 64-bit block which is equal to the number ` written in binary. For example, the (8-bit ASCII) message "abc" has length 8*3 = 24 padding is done with a one, then 448-(24+1) = 423 zero bits which results the length to become the 512-bit as a padded message.

$$01100001\ 01100010\ 011000111\ 00...0_{(423)}\ 00011000_{(64)}$$

The length of the padded message should now be a multiple of 512 bits.

2) Parse the message into N number of 512-bit blocks as $M^{(1)}$, $M^{(2)}$ . . ., $M^{(N)}$. The first 32 bits of message block i are denoted $M^{(i)}_0$, the next 32 bits are $M^{(i)}_1$, and so on. Usage of big-endian convention is done throughout, so each 32-bit word has the leftmost bit stored as the most significant bit position.

The hash computation proceeds as follows:

For i = 1 to N (N = number of blocks in the padded message)

{

Initialize registers a, b, c, d, e, f, g, h with the (i-1)st intermediate hash value

$a = H_1^{(i-1)}$

$b = H_2^{(i-1)}$

…

$h = H_8^{(i-1)}$

For j = 0 to 63

{

Compute Ch (e, f, g), Maj (a, b, c), $\sum_0^{(a)}$, $\sum_1^{(e)}$, and W_j

$T1 = h+1(e) + Ch\ (e, f, g) + K_j + W_j$

$T2 = 0(a) + Maj\ (a, b, c)$

h = g

g = f

f = e

e = d + T1

d = c

c = b

b = a

a = T1 + T2

}

Compute the ith intermediate hash value $H^{(i)}$

$H_1^{(i)} = a + H^{(i+1)}$

$H_2^{(i)} = b + H^{(i-1)}$

…

$H^{(i)} = h + H^{(i-1)}$

}

$H(N) = (H_1^{(N)}, H_2^{(N)}, . . .,.H_8^{(N)})$ is the hash of M.

The SHA-256 compression function is pictured as follows:

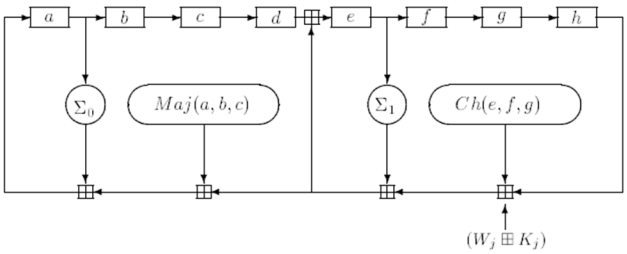


Fig. 1 j th internal step of the SHA-256 compression function C

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

IV. ARCHITECTURE

As seen from the architecture diagram, the user will first be prompted to a login and signup page. The user has to first signup on the portal, as soon as the user signs up for a new account, a new test will be allocated to him/her. All the details that the user entered while signing up will be stored in any traditional database. Here the main aim is to maintain the integrity of the results of any test taken by any student. The signup details can be temporarily be stored in any NoSQL databases like MongoDB or Firebase Firestore.
To take the exam the user has to login with the account that was created while signing up. On login, the user will be given the test screen where questions will be pulled from a question set which is stored in a blockchain. The question set will be written in blockchain by the examination authority prior to the examination. As Hyperledger fabric has PoA, it will be utilized here, the writing authority will be given to the entity that is conducting the examination. On the other hand, the users or the students who will be taking the exam will only have read access.
As soon as the user submits or finishes his/her test, the response will be taken from the view to the controller for minor JSON validations. If those validations are passed by the response, the whole exam data is then given to chaincode for evaluation. The responses of the user will be compared with the actual correct answers and result will be generated. The generated result will be then stored in blockchain along with attributes such as exam id, user id, roll no, name, etc. The above framework works on the popular MVC architecture pattern.
After undertaking the test, the user then can get his/her result by logging into the same account used for taking the exam. The results will be again pulled from the blockchain. The private information like phone number or email that was taken from the user can be maintained in a private collection. Only the respective person who has read access to it can see it. There is also a provision to download the certificate if one qualifies the minimum cut-off criteria.

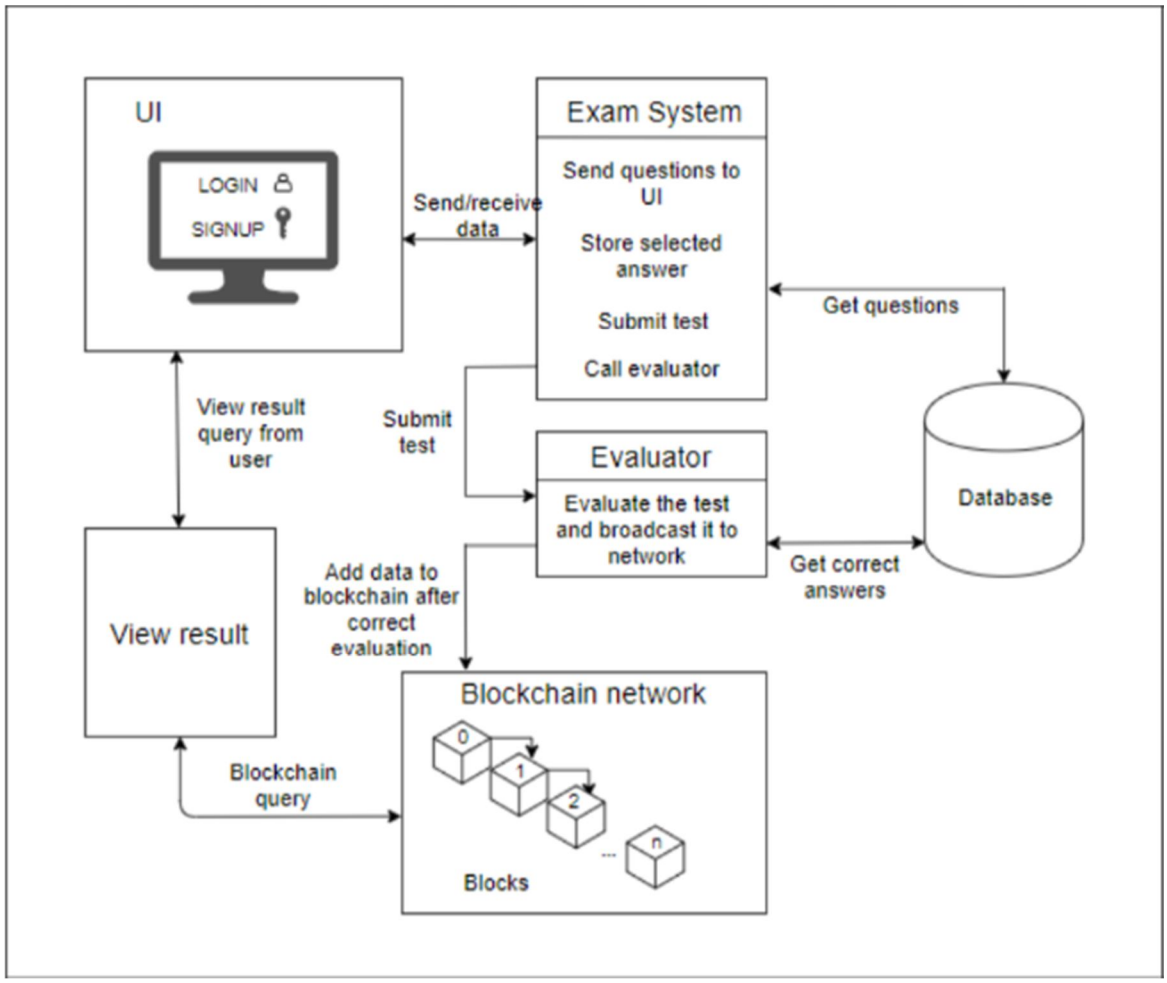


Fig. 2 Online examination architecture diagram

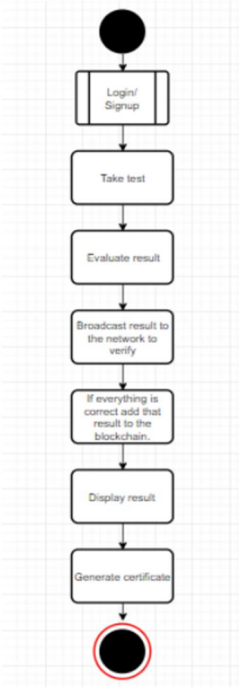


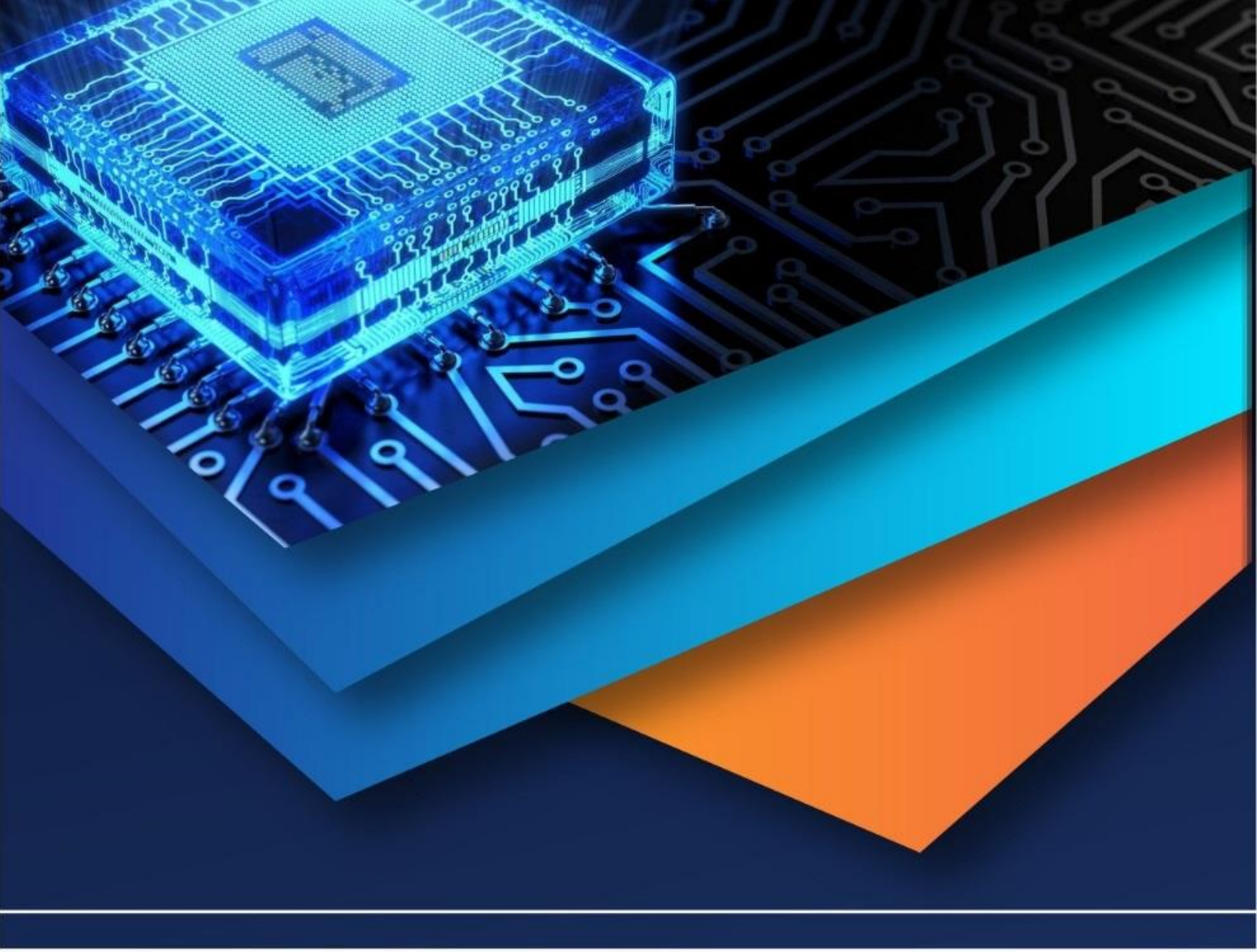
Fig. 3 Online Examination flow diagram

V. CONCLUSIONS

The aim is to illustrate an approach to use blockchain for evaluation and storage for online examination, such that it depicts a decentralized system. We here follow an authority-based consensus mechanism call as Proof-of-Authority. We are trying to solve the lack of transparency that is faced by the current traditional examination system. We address this problem by storing the results on an immutable blockchain such that each and every test result will be stored as a transaction.

REFERENCES

[1] Rahul Acharya, Sumitra Bin 'Blockchain based Examination System for Effective Evaluation and Maintenance of Examination Records'.
[2] FranCasino, Thomas K.Dasaklisb 'A literature review of blockchain-based applications: current status, classification and open issues'.
[3] Constantinos Patsakisa 'Decentralized applications: the blockchain empowered software system'.
[4] Satoshi Nakamoto 'Bitcoin: A peer-to-peer electronic cash system'.
[5] Hong-Nin g Dai, Zibin Zheng 'An overview of blockchain technology'.
[6] Wei Cai, Zehua Wang, Zhen Hong 'Decentralized Applications: The blockchain empowered software system'.
[7] Christian Cachin 'Architecture of the Hyperledger Blockchain Fabric'.
[8] Juan Benet 'IPFS: Content addressed versioned, P2P file system'.
[9] Muna R. Hameed, Firas A. Abdullatif 'Online Examination System'.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY