ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

Blockchain Based Examination System for Maintenance of Examination Records

Anita Dhami[1], Prof. Dr. D. R. Ingle [2]

Student, Bharati Vidyapeeth College of Engineering, Navi Mumbai, India

HOD, Department of Computer, Bharati Vidyapeeth College of Engineering, Navi Mumbai, India

ABSTRACT: The main objective of this paper is to provide a framework based on Blockchain to carry out and evaluate academic exams in an equal way with self-generation of certificates after the completion of the exam. We illustrate how a self-sufficient educational ecosystem can be developed over a chain of blocks for a fair evaluation without the need for a reliable central entity to obtain certificates or degrees that demonstrate its ability in a subject. To make the test as transparent as possible, we store the hash summary of each question asked and each answer to the questions, directly in the chain of blocks. This makes it easier to track exactly how a candidate has received the score, which adds more credibility to the obtained certificate.

KEYWORDS-Blockchain,decentralizedledger, cryptographically,Peer-to-peer database.

I. INTRODUCTION

Blockchain is a distributed cryptographically designed distributed ledger. Records all transactions made on a network. It is a chronological chain of blocks where each block consists of a block header. The block header records the hash of the previous block along with a merklee root and a date / time of the current block. This helps ensure the integrity of the blocks and allows the block chain to detect any invalid block, which makes it extremely secure. In this paper, we illustrate how the use of a blockchain-compatible peer-to-peer examination system can solve the problems identified in the security domain [1] and the integrity of current examination systems. We propose a framework to conduct a decentralized exam using blockchain for better evaluation and maintenance of exam records, so that records are more credible, reliable and secure than the current exam system. The current examination system suffers from extreme cases of manipulation of scores in the database, both by students [1], external security criminals or privileged information with administrative access. These concerns can be addressed by the proposed blockchain-based system.

Blockchain Architecture

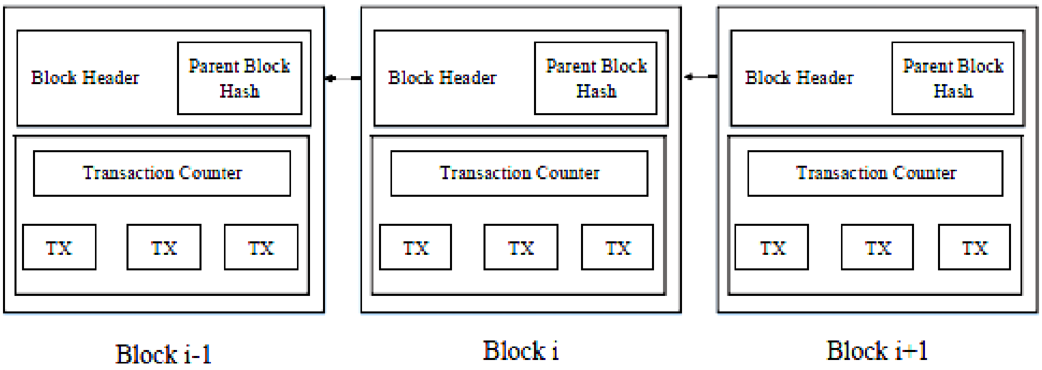

Fig. 1.1: An example of blockchain which consists of a continuous sequence of blocks.

Copyright to IJIRCCE DOI: 10.15680/IJIRCCE.2019. 0703007

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

Blockchain is a sequence of blocks, which contains a complete List of transaction records as a normal public record[14] Figure 1.1 shows an example of a blockchain. With a hash of the previous block contained in the block header, a block It has a single parent block. The hashes have also been memorised (the children of the ancestors of the block) in the chain of ethereum blocks [15]. The first block of a blockchain,It's called a genetic block that does not have a main block.

(A)Block

block contains the block header and the block body as shown in Figure 1.2. The block header contains: (i) Block version: identify which set of block validation rules to follow.

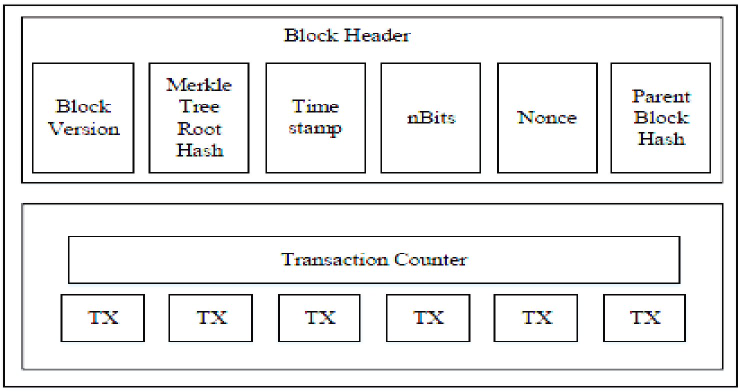

Fig 1.2 Block Structure

(iii nBits: target beginning of a valid block hash
(iv) Root Hash of the Merkle tree: the hash value of all transactions in the block
(iv)Timestamp: current time as seconds in universal time from 1 January 1970.
(v) Nonce: a four byte of field, which generally begins with 0 and increases 4 each hash calculation.
(vi) Parent Block Hash: hash value of the previous block which is a 256-bit that points to the previous block.
vi) Transaction counter: consists of a transaction and the extreme number of transactions that a block can enclose depends on the size of the block and the size of each transaction.[12].

(B) Digital signature

Each user has a private and public key pair. The private key that will be kept confidential is used to sign transactions. The basically digital signature is involved in two phases:first is signature phase and second is verification phase. For example, an A1user wants to send a message to another B1 user. (1) In the signing phase, A1 encrypts their data with own private key and sends B1 ,the encrypted result and the original data. (2) In the verification phase, Bob validates the value with Alice's public key. In this way, B1 could easily check whether the data was tampered with or not. The typical digital signature algorithm used in blockchains is the digital signature algorithm of the elliptic curve (ECDSA) [12].

II. LITERATURE REVIEW

Since blockchain technology is a fairly new field of study [13], publications have it.They based their research on available documents and professional-oriented sources, such as related forums (for example, [2]). So far, the extension of peer-reviewed publications was very limited and, therefore, an analysis of the articles submitted to peer review has not yet been carried out. With the growing academic interest, more and more publications ensure that scientific rigor is emerging. Therefore, this paper aims to focus on peer evaluation.Publications as the main source of information.

Blockchain technology is known as the underlying basis of Bitcoin-A Peer-to-Peer Electronic Cash System .The original bitcoin paper [2] by Satoshi Nakamotoin the year 2008 proposes a solution to the double-spending problem using a digital signature based peer-to-peer network. The network uses timestamped transactions to keep track of the chronology of occurrence of transaction and validates it using a hash-cash based proof-of-work mechanism [3]. The paper proves that it is possible to make transactions without any involvement of a trusted third party to validate those transactions.

Proof of Stake:
The first Proof of Stake algorithm was implemented in PeerCoin. PeerCoin used the concept of coinage and minting to produce new blocks unlike the proof-of-work based bitcoin. It was designed such that, the stake in the network obtained by allocating the coins would in-turn help mint new coins[4].

Proof of Stake versus Proof of Work:
The “Proof of Stake versus Proof of Work” whitepaper [5] by BitFury Group discusses various consensus algorithms like PoW (Proof of Work), PoS (Proof of Stake) and DPoS (Delegated Proof of Stake). It helps in understanding how each of these algorithms work and the factors they consider for validation of blocks.

Delegated Proof of Stake:
BitShares uses DPoS for achieving consensus. Instead of miners, it uses a mechanism to appoint and assign the tasks to delegates. The BitShares documentation [6] explains that such delegates are appointed by the users of the network using their votes. Each participant in the network gets to vote for a delegate and the top N delegates with most number of votes are appointed. These delegates sign the blocks with transactions, produced after every fixed interval of time, switching turns. It eliminates the need for any mining and is capable of operating with very less confirmation time.

Ethereum and Smart Contract:
Ethereum [7] demonstrates how a message passing framework can be implemented on the blockchain. The autonomous self-executing programs on the blockchain are referred as a Smart Contract. These smart contracts make it possible to do monetary transactions without the involvement of a third party, upon successfully executing the contract.

Blockchain based social media platform: The InterPlanetary File System (IPFS) [11] is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files. It forms a Merkle DAG (Directed Acyclic Graph) [11] upon which systems like blockchains can be built.

In order to form an educational community around the blockchain, it is important to look into existing blockchain based platforms, especially social media platforms. Some of the most notable ones are Steem [8], Synereo [9], Akasha and YOYOW [10]. Out of these, Steem and Akasha seem to be the most promising one in terms of performance and user base and serve as base model for our framework. YOYOW argues that its Proof of Flow (PoF) [10] is much better at solving the problems faced by the Steemblockchain, but it’s still not functional.
IPFS: The InterPlanetary File System (IPFS) [11] is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files. It forms a Merkle DAG (Directed Acyclic Graph) [11] upon which systems like blockchains can be built.

III. PROBLEMSTATEMENT

The current examination system involves an evaluator from an academic institution. However, there is no validation of the validation performed by the assessor. In cases where a new evaluation is performed, it is performed. This makes the evaluation system highly centralized and presents many problems related to centralized assessment. Centralized assessment is highly susceptible to score manipulation. The manipulation can be performed at any time; from the first evaluation to the manipulation during the final insertion of the data in the database. Because the data is stored in the database and is the control of a database administrator, it generates human interference susceptible to corruption or threats.

Another fundamental problem with the scorecard of the current examination system is that they do not provide sufficient data for performance. Score cards contain very limited information on performance, since only the final score assigned by one or two evaluators counts without the questions asked in the mode. Without having an idea of the types of questions that are asked by a candidate, correlating the score with the caliber of wrong conclusions.
We use a public blockchain with decentralized evaluation and maintenance of examination records to solve all the problems and provide a better alternative. In the decentralized evaluation mechanism, we perform two types of evaluations, one for the questions and one for the answers to the questions. The community votes for the validity or the relevance of the posted question in a particular category. Thus, the quality of the questions can be expected to be much better as decided by the consensus of the users obtained by the translation of their votes on each question.

IV. FRAMEWORK OF EVALUATION SYSTEM

The work-flow of the proposed framework is as follows:

1. Users register at the blockchain front-end with a gatekeeper of the blockchain in order to verify that they are either students or teachers. Users could provide Pretty Good Privacy(PGP) signed message from their known public handle and verify it from their academic- emailid.
2. Once we verify that the users are indeed teachers or students, we allow them to call functions which generates and allocates a public/private key pair to interact with the blockchain. The keys are generated with the help of a unique code assigned to them after manual verification. The details of the users are removed from the server that verifies the authenticity of the users after the users are verified and the keys are allocated to keep the system decentralized from the operations point ofview.
3. Once a key-pair is generated, a user can then perform the following major tasks and the framework is shown in Fig.1.3
   a. Post new questions signed with their private key. Existing users post questions with the relevant tags. The mechanism of posting a question is a transaction signed by the private key of the user. The public key is made available in a public repository of each account on the blockchain for everyone to verify the authenticity of thetransaction.
   b. Post answers to existing questions with their private key. Existing users post answers to the previously posted questions. The mechanism of posting is a transaction signed by the private key of the user posting theanswer.
   c. Race to choose as delegates. Each user must elect 31 delegates who vote with the weighted votes attached to each gaming site to determine the order of preference for the election of each candidate as a delegate. The votes can be changed at any time; however, the election of 31 delegates within the first 100 days is a mandatory activity for each user. This is done to ensure that the voting mechanism is as decentralized as possible with greater participation in the voting. If the sample size of the users in the network is N and the total number of voters is K, the final result of the vote is proportional to the N / K value. The lower the value of K, the more saturated and distorted it will be. the final score. The greater the value of K, while K <= N, the result will be more unbiased. Therefore, the result is less partial when K approaches N. The result is considered biased if the result is directly related to the votes of a small population. Even if the result can be partial, even with full participation, the result with the total participation of the voters can be considered as a direct representation of the consent of all participants. This solves the most fundamental problem of a consensus mechanism based on voting for low participation by increasing participation and resulting in less distorted outcomes. The task of each delegate is to produce blocks by verifying the authenticity of transactions in the block. A delegate is also required to maintain the servers of the complete nodes with the most reliable copy of the block chain verified by the signatures of each transaction. Delegates have additional roles when they are juxtaposed with the miners of the bitcoin block chain. Delegates are elected by voting consent. Therefore, the responsibility to be honest and less harmful to the network in any way increases the possibility of being elected as a delegate. Each user in the network gets a specific number of slots to choose a delegate. Each box is associated with a weighted vote with which a delegate is chosen. The voting mechanism is one of the many versions of Borda's famous voting mechanisms. The classification of the delegate is determined by the accumulated score obtained when calculating the votes of all the users of the network.
   d. Vote on questions, answers and other delegates using the private key. Users can vote on existing questions and

answers to express their agreement or disagreement. This model of voting to express agreement or disagreement is followed in all the popular forums like Stackoverflow, Reddit and Quora. However, in this model, the votes are weighted and provide more accurate representation of one's agreement or disagreement in terms of the validity of the posted questions or answers. The users can also vote for other users to elect them as their favorable delegates to produceblocks.

- Merkle Root for the block - It is a hash of all the transactions in a block.
- IPFS hash of the Question - Uniquely identifies the Question in a distributed file system.
- IPFS hash of the Answer - Uniquely identifies the Answer in a distributed file system.
- Timestamp - UTC (Universal Time Coordinated) time of block production.
- Delegate - Account identifier of the delegate producing the block.
- Delegate Signature - Signature of the delegate using the signing key.
- Transactions - The list of transactions that occurred since the production of the last block.

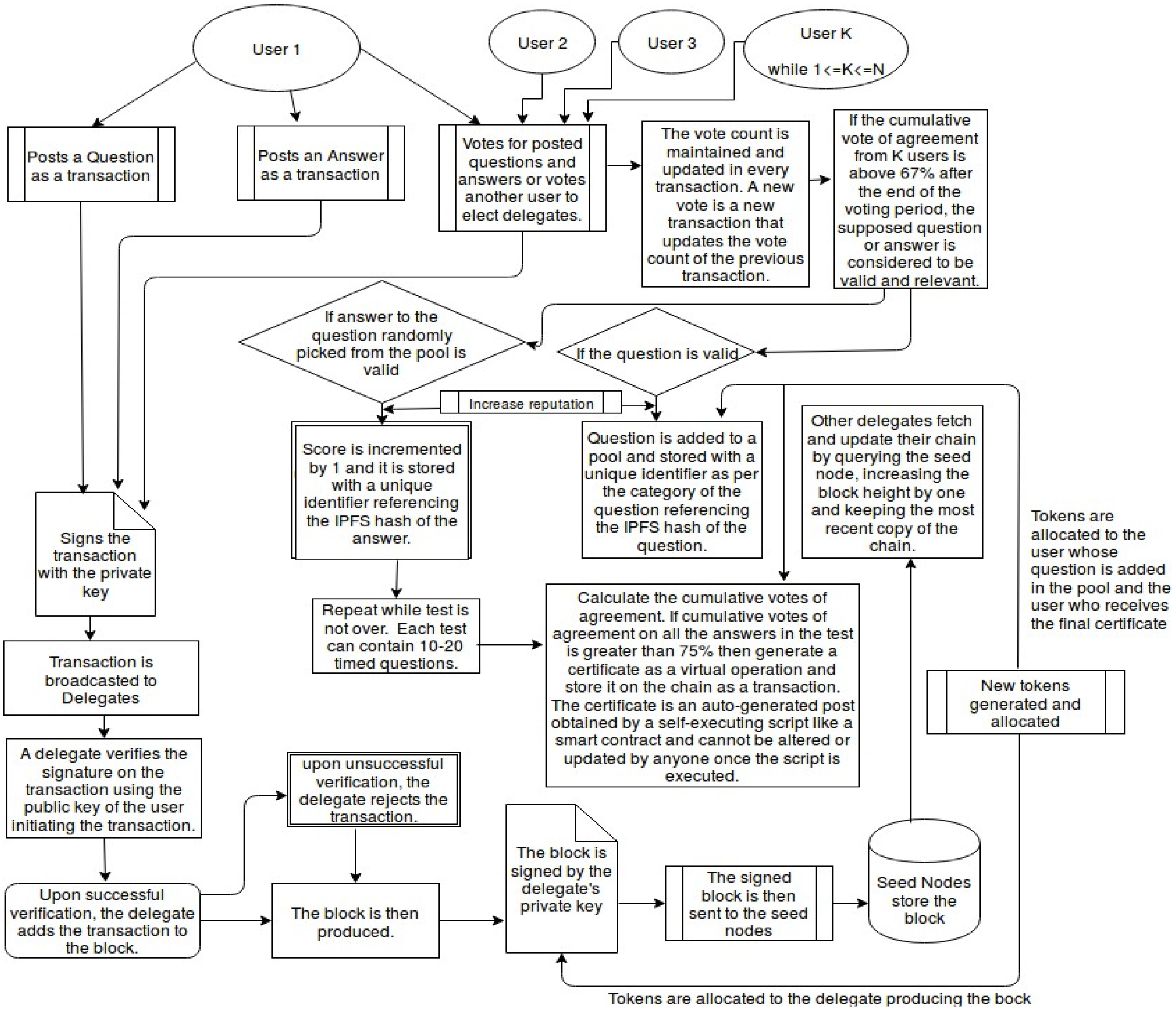
User 1
User 2
User 3
User K
while 1<=K<=N
Posts a Question as a transaction
Posts an Answer as a transaction
Votes for posted questions and answers or votes another user to elect delegates.
The vote count is maintained and updated in every transaction. A new vote is a new transaction that updates the vote count of the previous transaction.
If the cumulative vote of agreement from K users is above 67% after the end of the voting period, the supposed question or answer is considered to be valid and relevant.
If answer to the question randomly picked from the pool is valid
If the question is valid
Increase reputation
Score is incremented by 1 and it is stored with a unique identifier referencing the IPFS hash of the answer.
Question is added to a pool and stored with a unique identifier as per the category of the question referencing the IPFS hash of the question.
Other delegates fetch and update their chain by querying the seed node, increasing the block height by one and keeping the most recent copy of the chain.
Tokens are allocated to the user whose question is added in the pool and the user who receives the final certificate
Signs the transaction with the private key
Repeat while test is not over. Each test can contain 10-20 timed questions.
Calculate the cumulative votes of agreement. If cumulative votes of agreement on all the answers in the test is greater than 75% then generate a certificate as a virtual operation and store it on the chain as a transaction. The certificate is an auto-generated post obtained by a self-executing script like a smart contract and cannot be altered or updated by anyone once the script is executed.
Transaction is broadcasted to Delegates
New tokens generated and allocated
A delegate verifies the signature on the transaction using the public key of the user initiating the transaction.
upon unsuccessful verification, the delegate rejects the transaction.
The block is signed by the delegate's private key
Upon successful verification, the delegate adds the transaction to the block.
The block is then produced.
The signed block is then sent to the seed nodes
Seed Nodes store the block
Tokens are allocated to the delegate producing the bock

Fig. 1.3: Flow diagram of evaluation system

4. Post Question as a transaction signed using the private key. A user posts a question with a tag that indicates the category of the question considered to be relevant by the user. The question is posted as a transaction that is signed with the private key of the user posting the question. The signatures are derived from the content of the post and the private key. The signature is a 256 bit binary serialized representation of the transaction. The serialized binary representation serves as the message for signature. The signing is done on the SHA256 hash or the digest of the message of the transaction instead of the actual content of the message
5. Signed transactions are then broadcasted on the network for delegates for verification.
6. Delegates verify the transaction signature, timestamp and validity.
7. Upon verification, delegates add the transaction to the current block N and sign the block to broadcast it to the network.
8. Subsequent delegates also verify the Nthblock and they add the $(N+K)$th block on top of the Nth block upon verifying the validity of the Nth block. If the delegates find invalid transactions or invalid signatures in the previous block i.e the $(N+K-1)$th block, they consider it to be invalid and they add their $(N+K)$th block not on top of $(N+K-1)$th block but on top of $(N-X)$th block. Where N = Previous Block, K = Number of blocks between the Nth block and the current block, X $\in W$and is the difference between the last irreversible block number and the Nth block number. The last irreversible block is considered to be the block from which and beyond, no transactions can be altered and it is immune to double spending.
9. A user votes for a question submitted by someone else as a transaction signed using the private key of the user. This voting acts as a reviewing process of the questions submitted by individuals and the votes allocated determine the quality of the question. Voting for Questions as a transaction can be seen as a function that takes in Question identifier as an input and produces a corresponding Transaction as : *transactoion_id = Vote(question_id, voter_private_key).*
10. If at least one user casts a vote, that is *vote_count> 0* and a vote casted with agreement of takes a value of 1 while a vote casted with disagreement takes a value of -1, we calculate *score* as : *score = sum_of_votes/total_votes.*
11. If and only if $score$>0 at the end of the voting session, store question Q in the pool as the double hash of the question identifier *SHA256(SHA256(question_id))* and map it with the meta-data.
12. Posting answers can also be seen as a transaction signed using a private key. *Step 4* to *Step 8* remain same in the context of answering existing questions.
13. After *Step 8*, check the score of answers as :
    - *(total_attempted_answers/total_questions_asked)*×*(score_for_each_answer)* and total_score=
    - $\Sigma ni=1(attempti \times scorei) \div \Sigma ni=1(Qi)$.
14. If *i>0 and score >0.67*, then generate a certificate as an implied transaction from the blockchain to the candidate as a virtual operation, just like the coinbase transaction in Bitcoin. 67 is picked here because that indicates clear majority and indisputable consensus. Technically, it can be any number greater than 51 [7].
15. Transactions are verified by delegates during which the signature of the account initiating the transaction is verified along with the signatures of the previous delegates. If the signatures do not match for whatever reason, the delegates are ought to reject the transaction.
16. Upon verification of the transaction signature, the delegates add the transaction to their block. This operation ensures that the signatures and the transactions are not forged.
17. The block is added to the chain after a deterministic time interval. The time interval can be assumed to be 3 seconds. So, every block is produced after 3 seconds of the previous block production. This indicates that all the pending transactions are also sorted out and settled within this time period.
18. The block is then signed by the delegate's private key. A block is produced when the delegate signs the block.
19. The block is then sent to the seed nodes. Seed nodes are like dumb nodes which only store the entire copy of the blockchain.
20. The seed nodes receive the blocks and store them on top of the existing blockchain. This increases the height of the block by 1 every time. Two blocks can be at the same height if there is a fork, however the forks settle before reaching the seed nodes as the delegates are likely to favor one block from either of the chains.

21. The delegates then fetch and update their blockchain by querying the seed node. The delegates sync their copy of the blockchain with the latest available blocks that provides the base for the future blocks and the very status of the chain itself.

A. Delegate selection

A selection of the delegateWe set an odd number L as a limit for the main delegates expected to produce blocks giving them round robin rounds. Therefore, we selected two other delegates who are not present in the upper list of L randomly from the delegates queue and assigned the two delegates for the production of the last two blocks in that cycle. Since the system is deterministic, if the production time of the block was 5 seconds and if = 31, the first delegates would have taken 31 × 5 seconds to produce the block one after the other. At the end of the block production of delegate number 29, we selected 2 other random delegates before the cycle repeats. This random assignment is done to ensure that the system is safe from the attackers who own it and run it completely. Therefore, a production cycle of blocks in such a system would require (29 × 5) + (2 × 5) seconds. In each round, all published questions and answers are stored in the block chain.

B. Tokens incentive.

Like any large public blockchain, this framework also proposes the generation of tokens for network sustainability. Sustainability is assumed to derive from the financial incentive granted to the delegates to produce the blocks and keep the network in the best functional condition. Tokens are not extracted, however, the token generation mechanism is such,we explore each route from here, but first we need to establish what a block header of this block chain would consist of. Therefore, the following fields are the contents of the proposed blockchain header:

- Block height: identifies the position of the block in the block chain.
- Previous block ID: is the hash of the previous block.

whenever a delegate produces a block, new chips emerge. These tokens will have a fixed daily volume limit and can be marketed in various cryptocurrency exchanges. This motivates the delegates to be honest and provide a quality service to the network.

Tokens are generated and assigned to users whenever their application is accepted by the majority of the platform's voting population. Tokens are also assigned to candidates whose answers receive final certificates. This mechanism provides monetary rewards for playing honestly. Therefore, it is more advantageous for users to support and maintain the system rather than damage it to obtain financial benefits. It also encourages users to post relevant and valid questions, as well as good answers.

C. Reputation

There needs to be a way to indicate the performance of the users on the platform such that it cannot be traded. Therefore, we need a separate numerical value that indicates the performance and credibility of the user. The reputation can be calculated from value of 1.0 in increasing value of maximum 0.1. The higher the reputation, the better the status of the user in the platform will be. The reputation and the incentive are not linked so that bribery even in the platform is not encouraged. If a user participates in voting with V for questions or answers and the total number of votes casted for the same post is N, the total number of votes agreeing to the validity of the post is U, the total number of votes disagreeing to the validity of the post is D such that $(U+D) = N$, then the reputation R of the user will be calculated depending upon various scenarios as follows:

If $V = U$, $R = R + (1/U)$ provided at least $(N/3)+1 \in U$.
If $V = D$, $R = R + (1/D)$ provided at least $(N/3)+1 \in D$.
If $V = U$ *and* $(N/2)+1 \in D$, then $R = R - 1/D$.
If $V = D$ *and* $(N/2)+1 \in U$, then $R = R - 1/U$.

D. Contract for certificate generation

A smart contract can be implemented for auto-generation of the certificate once the consensus of the evaluators for the exam is above 75 percent. Since the platform itself will be free and it wouldn't cost much to retake the exam, the limit of at least 75 percent consensus can be imposed. That number can however be adjusted as per the consensus of the users on the platform. The goal of the certificate is to indicate that the user has successfully convinced a community of evaluators who hail from various educational institutes all across the world, that he/she has the knowledge required to pass the exam. The certificate will therefore be more credible and valuable as it represents a global certification instead of a centralized certificate from one institution alone.

E. Implementation

We simulate the voting mechanism by randomizing the vote selection using a ruby script on the local system. The network connectivity speed and latency is assumed to be ideal which might differ when trying to replicate the simulation amongst different nodes connected via the internet. Simulating the deterministic DPOS based architecture like the Steemblockchain [8] or the Bitshares Blockchain [6], we assume that the block production time is 3 seconds [8]. We simulate the voting transaction distribution in different blocks every 3 seconds and determine how the transactions would occur if they were to be deployed on the live DPOS based blockchain.

Comparison with current system

When we compare the proposed framework and the existing system, we can come to the conclusion that peer evaluation on a public blockchain is much more decentralized, transparent and credible. Since data posted on the chain cannot be deleted or modified without leaving a trace of doing so, the proposed system prevents any kind of unobserved malicious activity with the evaluation. The certification approach used in this framework is democratic and transparent which makes it less susceptible to manipulation and forgery.

V. CONCLUSION AND FUTURE SCOPE

Conclusion

The purpose of this paper is to illustrate an approach to use the blockchain to perform the decentralized exam and for a better evaluation of the examination records. We follow a version of the consensus mechanism based on voting, called Stake Test. We try to solve the lack of problems of transparency and credibility in the current examination system by recording the details of the examination in the immutable public block chain so that each operation is registered as a transaction. The model is based on the incentive approach of the crypto-economy to be honest and uses a built-in cryptocurrency to reward the positive contribution that improves the quality of the platform and the network. The quality of the contribution is decided by the community using the votes.

Future scope

This research establishes the fundamental framework for the use of a chain of blocks in the field of academic education. The current approach can be further improved by developing a scalable web application hosted on IPFS, which allows interaction with the blockchain using a browser. As the current framework has not been extensively tested to determine scalability, the document suggests that additional improvements can be made in the scalability aspect of the blockchain in terms of the number of transactions processed per second and the number of tests performed simultaneously.

REFERENCES

[1] D. Das, ”Hacking into the Indian Education System”, [Online]. Available: https://deedy.quora.com/Hacking-into-the-Indian-Education-System.

[2] S. Nakamoto, ”Bitcoin: A Peer-to-Peer Electronic Cash System,” http://Bitcoin.org; satoshin@gmx.com, pp. 1-8, 2008.

[3] A. Back, ”Hashcash - a denial of service counter-measure,” http://www.hashcash.org/papers/hashcash.pdf, 2002.

[4] S. King, S. Nadal, ”Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,” http://www.peercoin.net/bin/peercoinpaper.pdf, 2012.

[5] BitFury Group, ”Proof of Stake versus Proof of Work,” http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf 2015.

[6] BitShares, ”BitShares,” [Online]. Available: http://docs.bitshares.org/bitshares/dpos.html.

[7] D. G. WOOD, "ETHEREUM: A secure decentralisedgeneralised transaction ledger," GAVIN@ETHCORE.IO [Online]. Available: https://pdfs.semanticscholar.org/ac15/ea808ef3b17ad754f91d3a00fedc8f96b929.pdf.

[8] D. Larimer, N. Scott, V. Zavgorodnev, B. Johnson, J. Calfee and M. Vandeberg, "Steem: An incentivized, blockchain-based social media platform.," March 2016. [Online]. Available: https://steem.io/SteemWhitePaper.pdf.

[9] D. Konforty, Y. Adam,, D. Estrada and L. G. Meredith, "Synereo: The Decentralized and Distributed Social Network," 15 March 2015. [Online]. Available: https://bravenewcoin.com/assets/Whitepapers/Synereo-Decentralised-and-Distributed-Social-Network.pdf.

[10] YOYOW, "YOYOW non technical whitepaper: a blockchain-based media content producing and sharing platform," [Online]. Available: https://yoyow.org/files/YOYOW-non-technical-whitepaper-EN.pdf.

[11] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System (Draft 3)," [Online]. Available: https://raw.githubusercontent.com/ipfs/papers/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf

[12]A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.

[13] Zhao, J.L., Fan, S., Yan, J.: Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financ.Innov.2, 28 (2016).