International Journal of Engineering & Technology, 7 (2.6) (2018) 269-274

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Blockchain based examination system for effective evaluation and maintenance of examination records

Rahul Acharya[1]*, Sumitra Binu[2]

[1]Christ (Deemed to be University), India
[2]Christ (Deemed to be University), India
**Email: acharyarahul.now@gmail.com*

Abstract

The main objective of this paper is to provide a Blockchain based framework for conducting and evaluating academic tests in a peer-to-peer manner with auto-generation of certificates upon successful completion of the examination. We illustrate how a self-sustained education ecosystem can be developed on top of a blockchain for a fair evaluation without the need of a central trusted entity for obtaining certificates or degrees that prove one's dexterity over a subject. In order to make the test as transparent as possible, we store the hash-digest of every question asked and every question answered, directly on the blockchain. This facilitates the tracing of how exactly a candidate received the score that he/she received, adding more credibility to the obtained certificate.

Keywords: *Blockchain; Education; Consensus; Decentralization; Transparency*

1. Introduction

Blockchain is a cryptographically engineered distributed ledger. It records all the transactions executed in a network. It is a chronological chain of blocks where every block consists of a block header. The block header records the hash of the previous block along with a merklee root and a timestamp of the current block. This contributes towards ensuring the integrity of the blocks and enables the blockchain to detect any invalid blocks making it extremely secure. In this paper, we illustrate how using a peer to peer examination system supported by blockchain could solve the problems identified in the domain of security [1] and integrity of current examination systems. We propose a framework for conducting decentralized examination using blockchain for better evaluation and maintenance of examination records such that the records are more credible, reliable and secure in juxtaposition with the current examination system. The current system of conducting examination suffers extreme cases of score manipulation in database either by students [1], external security breachers or by insiders with administrative access. These concerns can be addressed by the proposed blockchain based system.

2. Literature Review

Bitcoin: A Peer-to-Peer Electronic Cash System
The original bitcoin paper [2] by Satoshi Nakamoto 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 [4] :
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.
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:

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 Steem blockchain, 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.

3. Problem Statement

The current examination system involves an evaluator from an educational institute validating the answers to the questions asked. There is however no re-validation of the validation performed by the evaluator. In cases where re-evaluation is done, it is done by a handful of people. This makes the evaluation system highly centralized and there are many problems associated with centralized evaluation.

- Centralized evaluation is highly susceptible to score-manipulation. The manipulation can be done at any stage; right from the first evaluation to the manipulation during the final data-entry in the database.

- Since the data is stored in the database and it is under the control of a database administrator, it brings in the human interference which is susceptible to bribery or threats.

- Another fundamental problem with the scorecard of the current examination system is that they do not provide enough data to represent the performance of a candidate taking up the test. The scorecards contain very limited information about the performance as it only accounts the final score granted by one or two evaluators without disclosing the questions asked and the manner in which the questions were answered. With no idea of the types of questions asked to a candidate, correlating the score with the caliber of the candidate mostly leads to inaccurate conclusions.

- Centralized issuance of degrees or certificates is susceptible to manipulation. The certificates received by a candidate upon completion of a course indicate that the candidate has the expected skills and knowledge demanded by the successful completion of the course. However, the certificates can be forged or granted even when the candidate doesn't meet the criteria of receiving the certificates if an institution decides to grant it no matter what. There is no way to know whether the certificates issued by an institution are issued even when the criteria of issuance is not satisfied by the performance of the candidate. Nevertheless, the process of just validating the authenticity of the issued certificate is expensive and slow.

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.

4. 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-email id.
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 of view.
3. Once a key-pair is generated, a user can then perform the following major tasks and the framework is shown in Fig. 1.
    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 the transaction.
    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 the answer.
    c. Race to be elected as a delegates. Every user is required to elect 31 delegates by voting for them with the weighted votes attached for each slot in order to determine the order of preference of election of each candidate as a delegate. The votes can be changed at any time; however, picking the 31 delegates within the first 100 days is a mandatory task of each user. This is done to ensure that the voting mechanism is as decentralized as possible with increased voting participation. If a sample size of users on the network is N and the total number of voting population is K, the final outcome of the vote is proportional to the value of N/K. The lesser the value of K, the more saturated and biased the final result is. The larger the value of K, while $K<=N$, the more unbiased result will be. Therefore, the result is less biased when K approaches N. The result is considered to be biased if the outcome is directly correlated to the votes of a small population. While the result might be biased even with complete participation, the result with complete participation of voters can be considered to directly represent the consensus of all the participants. This solves the most fundamental problem of a vote-based consensus mechanism of low participation by increasing participation and therefore resulting in less-biased outcomes. The task of each delegate is to produce blocks by verifying the authenticity of the transactions in the block. A delegate is also required to maintain full node servers with the most honest copy of the blockchain verified by the signatures of each transaction. Delegates have additional roles when juxtaposed with miners of the bitcoin

blockchain. The delegates are elected by the consensus of voting. Thus, a responsibility to be honest and less harmful to the network in any manner increases the probability of being elected as a delegate. Each user in the network gets a specified number of slots to elect a delegate. Each slot has a weighted vote attached to it with which a delegate is elected. The voting mechanism is one of the many versions of the popular Borda Voting mechanisms. The ranking of the delegate is determined by the cumulative score obtained by calculating the votes of all the users on 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 produce blocks.

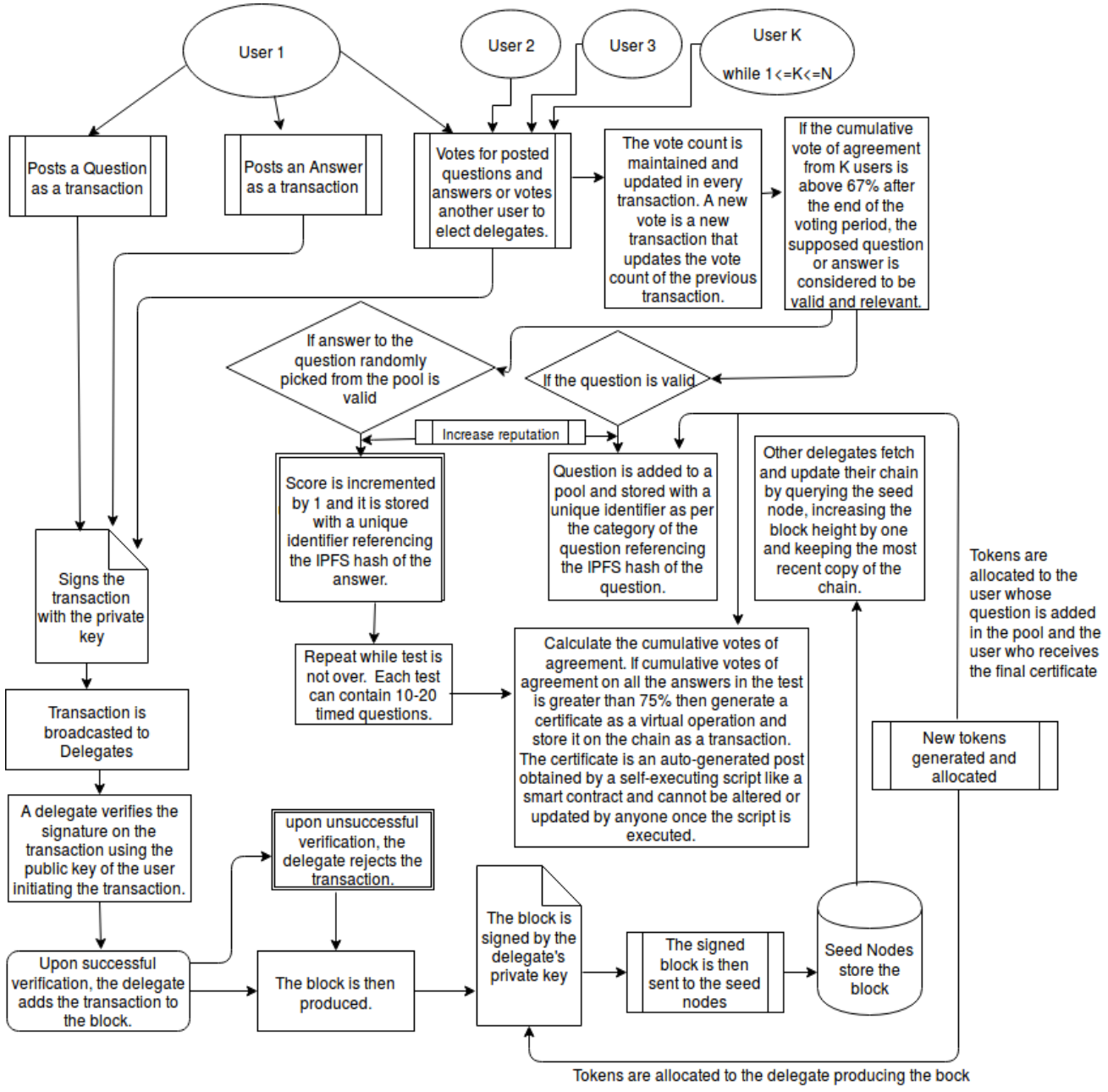

Fig. 1: Flow diagram of evaluation system

We explore each path from here subsequently but first it is necessary to establish what a block header of this blockchain would consist of. Therefore, the following fields are the contents of the proposed blockchain header:

- Block height - It identifies the position of block in the blockchain.
- Previous Block id - It is the hash of the previous block.

- 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.

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. We can use python ecdsa package to sign and to make sure that the transactions are canonical.
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 N^{th}block and they add the $(N+K)^{\text{th}}$ block on top of the N^{th} block upon verifying the validity of the N^{th} block. If the delegates find invalid transactions or invalid signatures in the previous block i.e the $(N+K-1)^{\text{th}}$ block, they consider it to be invalid and they add their $(N+K)^{\text{th}}$ block not on top of $(N+K-1)^{\text{th}}$ block but on top of $(N-X)^{\text{th}}$ block. Where N = Previous Block, K = Number of blocks between the N^{th} block and the current block, $X \in W$and is the difference between the last irreversible block number and the N^{th} 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= $\sum_{i=1}^{n} (attempt_i \times score_i) \div \sum_{i=1}^{n} (Q_i)$.
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

We set an odd number L as the limit for top delegates who are expected to produce blocks by giving them turns in a round robin fashion. We then pick two more delegates which are not present in the top L list randomly from the delegate queue and assign the two delegates for production of the last two blocks in that cycle. Since the system is deterministic, if the block production time were to be 5 seconds and if $L = 31$, then it would take 31×5 seconds for the top delegates to produce a block one after the other. At the end of the block production by the 29th delegate, we pick 2 more delegates randomly before the cycle repeats. This randomization is done to make sure that the system is safe from being completely owned and run by attackers. Thus one cycle of entire block production in such a system would take $(29 \times 5) + (2 \times 5)$seconds. In each round, all the questions and answers that are posted are stored on the blockchain.

B. Incentivization with tokens

Like every major public blockchain platforms, this framework also proposes the generation of tokens for sustainability of the network. The sustainability is assumed to come from the financial incentive given to the delegates for producing the blocks and keeping the network in the best functional state. The tokens are not mined, however the token generation mechanism is such that

every time a delegate produces a block, new tokens come into existence. These tokens will have a daily cap of fixed volume and they can be traded on various cryptocurrency exchanges. This motivates the delegates to stay honest and provide quality service to the network.

The tokens are also generated and allocated to users every time their question gets accepted by the majority of the voting population of the platform. The tokens are also allocated to candidates whose answers receive the final certificates. This mechanism provides monetary rewards to play honest. Therefore, it is more beneficial for the users to support and maintain the system than harm it for financial benefits. It also encourages users to post relevant and good 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 Steem blockchain [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.

```
#Ruby Script to simulate voting
#It assumes 50 questions are proposed
#It assumes 2000 users are voting
#It randomly upvotes or downvotes

Voting = [1.0,-1.0]
def get_score
  score          = 0.0
  score_sum = 0.0
  vote_sum  = 0.0
  accepted_qcount = 0
  block_height   = 0
  start_block = Time.now
  for question_count in 1..50
      for voter_count in 1..2000
        puts "# #{voter_count}"
        puts "Cast your vote"
        vote = Voting.sample
        puts (vote==1)? "UPVOTED":"DOWNVOTED"
        vote_sum += vote
        puts "Net vote = #{vote_sum}"
        score = vote_sum
        puts "score  = #{score}"
        finish_block = Time.now
        diff = finish_block - start_block
        if diff >= 3
          block_height += 1
          puts "BLOCK NUMBER: #{block_height}"
          start_block = Time.now
        end
      end
    score_sum += score
    if score > 0
     q_count += 1
     puts "Question Added "
    else puts "Question Not Added"
    end
  end
end

get_score
```

F. *Juxtaposition with current system*

When we juxtapose 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.

5. Conclusion and Future scope

5.1. Conclusion

The aim of this paper is to illustrate an approach to use blockchain for conducting decentralized examination and for better evaluation of the examination records. We follow a version of the vote-based consensus mechanism called the Delegated Proof of Stake. We try solving the lack of transparency and credibility problem in the current examination system by recording the details of the examination on the immutable public blockchain such that every operation is recorded as a transaction. The model is based on the crypto-economics approach of incentivization for being honest and uses an inbuilt cryptocurrency to reward positive contribution that improves the quality of the platform and the network. The quality of the contribution is decided by the community using their votes.

5.2. Future scope

The present research lays the foundational framework of using a blockchain in the field of academic education. The current approach can further be enhanced by developing a scalable web application hosted on the IPFS, that allows interaction with the blockchain using a browser. Since the current framework has not

be extensively tested for scalability, the paper suggests, further improvements can be made on the aspect of scalability of the blockchain in terms of numbers of transactions processed per second and the number of examinations conducted 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 decentralised generalised 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.