Design and Implementation of a Consensus Algorithm to build Zero Trust Model

Annapurna P Patil
Department of Computer Science and Engineering
Ramaiah Institute of technology
Bangalore, India
annapurnap2@msrit.edu

Gaurav Karkal
Department of Computer Science and Engineering
Ramaiah Institute of technology
Bangalore, India
gauravkarkal@gmail.com

Jugal Wadhwa
Department of Computer Science and Engineering
Ramaiah Institute of technology
Bangalore, India
jugaldeepak@gmail.com

Meer Sawood
Department of Computer Science and Engineering
Ramaiah Institute of technology
Bangalore, India
sawoodrocket@gmail.com

K Dhanush Reddy
Department of Computer Science and Engineering
Ramaiah Institute of technology
Bangalore, India
dhanushreddy1014@gmail.com

2020 IEEE 17th India Council International Conference (INDICON) | 978-1-7281-6916-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/INDICON49873.2020.9342207

***Abstract*— Zero Trust Model ensures each node is responsible for the approval of the transaction before it gets committed. The data owners can track their data while it's shared amongst the various data custodians ensuring data security. The consensus algorithm enables the users to trust the network as malicious nodes fail to get approval from all nodes, thereby causing the transaction to be aborted. The use case chosen to demonstrate the proposed consensus algorithm is the college placement system. The algorithm has been extended to implement a diversified, decentralized, automated placement system, wherein the data owner i.e. the student, maintains an immutable certificate vault and the student's data has been validated by a verifier network i.e. the academic department and placement department. The data transfer from student to companies is recorded as transactions in the distributed ledger or blockchain allowing the data to be tracked by the student.**

Keywords*— Distributed Systems, Blockchain, Trust Model, Zero Trust Model, Consensus Algorithm

I. INTRODUCTION

Distributed systems is a concept where a group or network of systems work together and behave like a single system. The systems work in conjunction with one another to ensure that the system remains functional even if one of the nodes/systems crash or have a fault. The main advantage of a distributed system is to allow for horizontal scaling. Regular systems use vertical scaling where in the hardware resources are increased to increase the compute power. By building a distributed system, horizontal scaling is leveraged which is to add another system/node when there is too much traffic or load on one system. Such a type of scaling allows for low latency and fault tolerance. Consistency and concurrency is a major fault in such systems which are tackled using a concept known as consensus.

Consensus is the agreement of nodes in a distributed system on which transactions to commit and which to abort. This way the system remains consistent and allows concurrency of data among all the nodes in the distributed system. Consensus among such nodes is achieved using consensus algorithms which allow nodes to agree based on a common value. Consensus algorithms work in a manner where a majority of the nodes have to agree before any kind of transaction occurs. This allows various attacks and leaves vulnerabilities to data as well as man in the middle attacks. The concept of zero trust model and blockchain can be used to improve this security. Zero Trust model is built such that the entire process is that each node is trusted before which the system can come to a consensus. This implies that all nodes are trusted and a 100% majority is required for any kind of transaction to occur. Blockchain and the concept of distributed ledger allows the components in the system to secure the data. Distributed ledger is a special kind of database that works as an append only database using cryptographic signatures. Thus, using such a system allows securing of data of users as well as allow the user to trust the system that they are using. Such a system would be able to have vast applications and allow automation and security of various systems which are tedious and manual currently.

II. NOVELTY OF PROPOSED WORK

The objectives of the proposed work are -

978-1-7281-6916-3/20/$31.00 ©2020 IEEE

Authorized licensed use limited to: Khulna Univ of Engineering & Technology - KUET. Downloaded on May 29,2022 at 06:32:54 UTC from IEEE Xplore. Restrictions apply.

- Build a consensus algorithm that works on zero trust model
- Develop a distributed ledger to store transactions
- Build a system that has an automated mechanism for verification
- Allow data owners to have confidence in the system

To build a model satisfying the above objectives the use case of the placement system in colleges is chosen. The placement system model that is currently used by the placement department is where companies visit the campus for recruitment drives, specify their eligibility criteria and request for student data. The issues caused by this model are redundant input of student data and inability to verify the data entered by the student at the registration phase. The proposed model aims to automate this entire process and resolve the issues by eliminating redundancy and providing a framework for verification.

III. Literature Survey

In order to address the issue of trust in distributed systems, there's a need for consensus models. In order to join the blockchain network, the users are required to prove themselves. Blockchain introduces consensus algorithms to achieve an agreement among distributed systems on a single point (data). Consensus Mechanisms have been divided into two categories: incentivised and non-incentivised algorithms. Some of the popular consensus algorithms are Proof of Work (PoW) and Proof of Stake (PoS). These algorithms provide rewards to the participants and hence fall under incentivised algorithms.

Blockchain is being adopted in higher educational institutions [1]: Blockchain is being utilised in many sections around the world like banks, government, defence and education. Today, universities are trying to incorporate blockchain technology to the education system. Securing the data transaction such as the student's academic profile and certification is a very crucial part in security professions. The research highlights the studies that cover the possibility of adopting blockchain technology in educational institutions.

Education-Industry Cooperative System Based on Blockchain [11]: The paper makes use of the blockchain technology features such as transparency and non-tampering features to implement the Education-Industry Cooperative System on the Hyperledger framework. The system stimulates the roles for universities and companies in the system using the certificate authority service and transaction in the framework. The system enables enterprises and universities to share information transparency providing security.

A Blockchain Consensus Mechanism for Educational Administration System [4]: The blockchain-based educational system contains a set of nodes and uses a consensus mechanism to address trust which is a key to system implementation. This paper proposes a refined consensus mechanism on group based educational systems, using a voting scheme that credits reward and punishment to ensure the effectiveness of nodes elected and eliminate malicious nodes.

Proof of Contribution: A Modification of Proof of Work to Increase Mining Efficiency [12]: Proof-of-Contribution (PoC) reduces the energy consumption by rewarding the miners with difficulty of a puzzle. This mechanism further motivates the miner to solve the puzzle as they receive regular mining fees. This approach thus reduces the energy consumption level.

Proof of Work requires the prover to perform a resource intensive computational task to achieve the desired goal. Once computed, the obtained result is verified by the verifiers that require less resource. The prover's are basically miner's who create a valid block. They use a lot of computational power to generate a block which is then presented to the verifiers in the network for verification. The work done by the miner is used as a factor to address trust. The algorithm does not restrain attackers from creating blocks, but it makes it difficult for the attackers. In order for the attacker to succeed, the attacker must have 51% of the mining power in the network which is a huge amount.

Proof of Elapsed Time (PoET) is a consensus algorithm that removes the need for high resource utilisation and computational power. It instead works on a randomized timer system for participants in the network. Each participant is given a random timer object and the first one whose timer expires is the one to produce the block i.e. the participant wakes up and becomes the block leader.

IV. Hybrid Approach Of Proof Of Work And Proof Of Elapsed Time

The proposed consensus algorithm is a hybrid algorithm that combines a modified Proof of Work and a modified Proof of Elapsed Time.

Proof of Work requires the prover to perform a resource intensive computational task to achieve the desired goal. Once computed, the obtained result is verified by the verifiers that require less resource. They use a lot of computational power to generate a block which is then presented to the verifiers in the network for verification. The work done by the prover is used as a factor to address trust. When the student wants to share data with a company, the student node runs the Proof of Work algorithm to do work and creates a block. A target value is generated as a result which is stored in the Proof structure which is added to the newly created block. During the request pipeline, the academic and placement department verify the computation work done by the student node by comparing the target value stored in the block. If verified correctly, then the block is passed along in the pipeline, else it's discarded. Hence, the work done by the student node is used as a factor of trust which is verified by the verifier network which is the academic and placement department. Proof of Elapsed Time (PoET) is a consensus algorithm that removes the need for high resource utilisation and computational power. Concept of proof of elapsed time is used to avoid man in the middle attack with verification of timestamp. If any external malicious node tries to modify the block, the timestamp is recorded and verified by other nodes in the system. Since the nodes take longer to verify, it can be assumed that the block is tampered and is discarded.

Authorized licensed use limited to: Khulna Univ of Engineering & Technology - KUET. Downloaded on May 29,2022 at 06:32:54 UTC from IEEE Xplore. Restrictions apply.

The longer time taken by the nodes for verification indicates a form of tampering of the system. The Academic department obtains the block from the Student node and verifies the timestamp when the block was created. If the time period is below a certain threshold, the block is passed along to the Placement department, else it's discarded. Next, the Placement Department obtains the block and verifies the timestamp when the block was created and when it was verified by the Academic Department. If the time periods are within the threshold, the block is verified successfully, else it's discarded.

V. Proposed Zero Trust Model

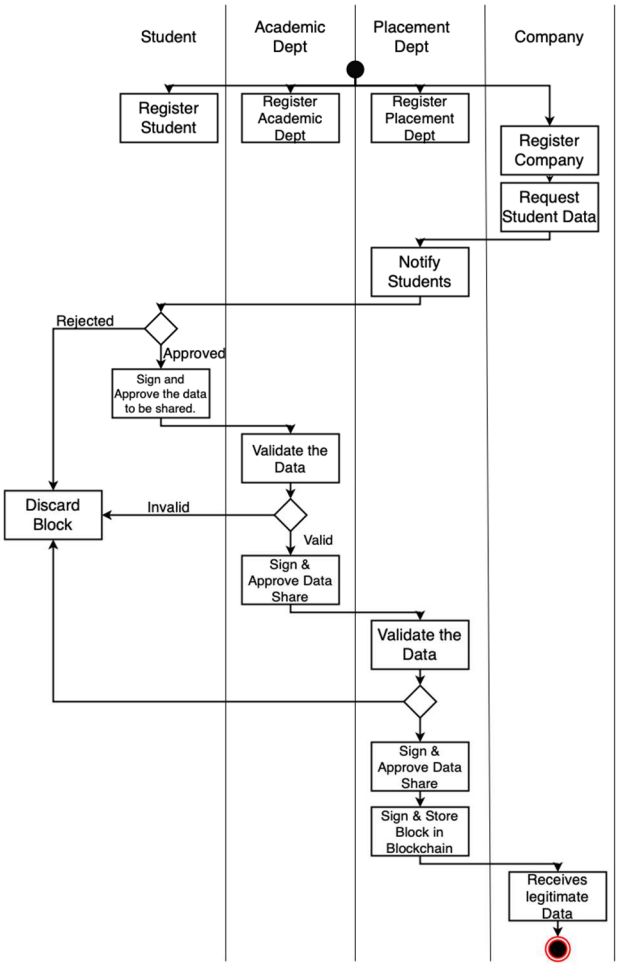

Fig. 1. Workflow of proposed Placement System

```
Begin:
  Initialise blockchain
  Begin:
    Add genesis block to the chain
  End
  Initialise placement and academic nodes
  Begin:
    Generate private and public keys for placement
    node
    Store Placement node keys in DB
    Generate private and public keys for academic
    node
    Store Academic node keys in DB
  End
  Initialise Student node
  Begin:
    Generate private and public keys for student node
    Store Student node keys in DB
    Encode student data to bytes
    Store student data in DB
  End
  Initialise Company node
  Begin:
    Generate private and public keys for company
  End
End
```

Fig. 2. Algorithm: Initialization Phase

```
Begin:
 Company specifies eligibility criteria, sends request to Placement
   dept
 Placement Node sends email to eligible students requesting for
   data
 If student registers for company by clicking the registration link
   in mail
 Begin:
    Student's creates a new block by running PoW
    Student encrypts data and generates signature using
    RSA
    Student adds encrypted data to block and stores it in
    Buffer
    Academic Node fetches the block from Buffer
    Academic Node decrypts data, verifies and validates
    the block.
    Academic Node encrypts the data and generates
    signature using RSA
    Academic Node adds encrypted data to block and
    stores it in Buffer
    Placement Node fetches the block from Buffer
    Placement Node decrypts data, verifies and validates
    the block
    Placement Node encrypts the data and generates
    signature using RSA
    Placement Node adds encrypted data to block and
    stores it in DB
    Block is appended to Blockchain
    Company fetches the block from DB, decrypts and
    authenticates block
    Company retrieves the requested student data from
    block
  End
End
```

Fig. 3. Algorithm: Request Pipeline

Figure 1 shows the workflow of the placement system. There are 5 components in the proposed System. They are the Blockchain, Student, Company, Placement Department and Academic Department. Each node has separate endpoints for their distinctive functionality. The Student, Company, Placement Department and Academic Department nodes collectively handle the request pipeline.

Authorized licensed use limited to: Khulna Univ of Engineering & Technology - KUET. Downloaded on May 29,2022 at 06:32:54 UTC from IEEE Xplore. Restrictions apply.

The request pipeline is initiated when the company requests for the student's data. The company specifies the eligibility criteria and sends a request to the Placement Department node. The Placement Department node filters the Database to obtain the students who fit the eligibility criteria as set by the company. The Placement Department node sends an email requesting for data to the eligible students.

If the student clicks on the rejection link mentioned in the mail, then the request pipeline terminates, and action is logged in Database. If the student clicks on the registration link mentioned in the email sent by the Placement Department node then the Student node first creates a new block with its data. It runs the Proof of Work algorithm on this block. It then encrypts the data with the public key of the Academic Department node. This ensures the confidentiality of the data. It generates a signature using its own private key. It also initializes a new verification structure recording the timestamp of the creation of the block. It adds the encrypted data, signature and verification to the block and stores the block in the Buffer. It then sends a notification to the Academic Department node for its verification.

The Academic Department node gets the notification from the Student Node and fetches the specific block from the Buffer. It decrypts the student data using its own private key and authenticates by verifying the signature of the student using the public key of the student. It then proceeds to validate the Proof of Work done on the block. It runs Proof of Elapsed Time on the block. It stores the timestamp of verification of Academic Department node in the verification structure. It then encrypts the data using the public key of the Placement Department node and generates the signature using its own private key. It adds the encrypted student data, signature and verification to the block and stores the block in the Buffer. It sends a notification back to the Student node saying the Verification by the Academic Department node is successful. It then sends a notification to the Placement Department node for its verification.

The Placement Department node gets the notification from the Academic Node and fetches the specific block from the Buffer. It decrypts the student data using its own private key and authenticates by verifying the signature of the Academic node using the public key of the Academic Department node. It then proceeds to validate the Proof of Work done on the block. It runs Proof Of Elapsed Time on the block. It stores the timestamp of verification of the Placement Department node in the verification structure. It then encrypts the data using the public key of the company and generates the signature using its own private key. It adds the encrypted student data, signature and verification to the block and stores the block in the Database. It sends a notification back to the Academic node saying the Verification by Placement Department node is successful. It then sends a notification to the company registered to retrieve its data. It adds the block signifying the transfer of data from student to company to the blockchain.

The company requesting data gets the notification from the Placement Department node and fetches the specific block from the Database. It decrypts the student data using its own private key and authenticates by verifying the signature of the Placement Department node using the public key of the Placement Department node. It successfully retrieves the decrypted student data. It then sends a notification back to the Placement Department node saying it has successfully retrieved the data. This concludes the request pipeline.

VI. Conclusion And Future Research Aspects

The proposed consensus algorithm builds a Zero Trust model as no central authority can be trusted to govern the distributed system. The consensus algorithm is a hybrid algorithm which combines Proof of Work and Proof of Elapsed Time. Data Security is ensured using the RSA algorithm for authentication and authorization. The Proposed consensus algorithm is used in building a zero-trust model which is implemented in the placement system. The open issues in the current system unfold the following future research possibilities:

- Security: Network security has to be maintained using cryptography to prevent unwanted data access
- Usage Scenarios: The proposed model can be extended to Banking systems, Health Industry, etc.

Acknowledgement

The authors wish to thank the Department of Computer Science and Engineering, the Principal and the Management of Ramaiah Institute of Technology, Bengaluru for providing us the required facilities and support to carry out our research work. The authors would like to thank Raghunath Kulkarni and Subodh Gajare from Cisco for their guidance and valuable feedback throughout the course of the project.

References

[1] Al Harthy, Khoula, Fatma Al Shuhaimi, and Khalid Khalifa Juma Al Ismaily. "The upcoming Blockchain adoption in Higher-education: requirements and process." 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC). IEEE, 2019.

[2] Hazari, Shihab Shahriar, and Qusay H. Mahmoud. "A parallel proof of work to improve transaction speed and scalability in blockchain systems.

[3] 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2019.

[4] Wang, Baocheng, et al. "A Blockchain Consensus Mechanism for Educational Administration System." 2019 IEEE 2nd International Conference on Electronics Technology (ICET). IEEE, 2019.

[5] Yang, Xinle, Yang Chen, and Xiaohu Chen. "Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information." 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019.

[6] Ferdous, M.S., Chowdhury, M.J.M., Hoque, M.A. and Colman, A., 2020. Blockchain Consensuses Algorithms: A Survey. arXiv preprint arXiv:2001.07091.

[7] Ehmke, Christopher, Florian Wessling, and Christoph M. Friedrich. "Proof-of-property: a lightweight and scalable blockchain protocol." Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain. 2018

[8] Kim, Soohyeong, Yongseok Kwon, and Sunghyun Cho. "A survey of scalability solutions on blockchain." 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2018.

[9] Chen, Lin, et al. "On security analysis of proof-of-elapsed-time (poet)." International Symposium on Stabilization, Safety, and Security of Distributed Systems. Springer, Cham, 2017.

Authorized licensed use limited to: Khulna Univ of Engineering & Technology - KUET. Downloaded on May 29,2022 at 06:32:54 UTC from IEEE Xplore. Restrictions apply.

[10] Kumar, Rakesh, et al. "Challenges in Adoption of Blockchain in Developing Countries." 2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST). IEEE, 2019.
[11] Liu, Qin, et al. "Education-industry cooperative system based on blockchain." 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2018.
[12] Xue, Tengfei, et al. "Proof of contribution: A modification of proof of work to increase mining efficiency." 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). Vol. 1. IEEE, 2018.

Authorized licensed use limited to: Khulna Univ of Engineering & Technology - KUET. Downloaded on May 29,2022 at 06:32:54 UTC from IEEE Xplore. Restrictions apply.