Blockchain Based Course Feedback System

Atharv Chandratre
Student, Dept. of Computer Science
BITS, Pilani - K.K. Birla Goa Campus
Goa, India
f20170009@goa.bits-pilani.ac.in

Shubham Garg
Student, Dept. of Computer Science
BITS, Pilani - K.K. Birla Goa Campus
Goa, India
f20160028@goa.bits-pilani.ac.in

***Abstract*—The Blockchain Technology is an innovative tool which can be used for tracking objects in the digital world.This project explores the usage of the Blockchain Technology as a Course Feedback System to track the feedback given by the students taking a course. This is to be done by implementing a smart contract on the Ethereum Blockchain which will accept the feedback given by students. This feedback will be recorded by a Survey Management System and then will be pushed onto the Blockchain for immutability and enhanced trackability. The system should be able to support creation of a survey by the professor who is in charge of the course. The system will then have to create a matching smart contract to support the survey questions decided by the professor. After the survey goes live, the system will store the data collected during the survey and push it to the blockchain, as a complete Feedback object file or as a hash of the values entered by the student in the review.**

I. Introduction

A. Motivation

The conduction of scientific and unbiased surveys is extremely difficult. The complete survey pipeline is riddled with opacity of review collection. The hiding of the identities of the candidates taking part in the survey is of massive importance whenever a survey is conducted, so as to prevent any biases in the final analysis of the collected data. The aim of any survey is to accurately capture a participant's true sentiments. Also, traditional systems of surveys prone to manipulation of collected data. We are looking to try to find a solution to these problems by utilizing the Blockchain framework and in the process, present a model which can be used to exhibit the properties of a perfectly unbiased, relatively transparent, more reliable and completely private survey system. By using the Blockchain framework for this project, we can utilize a system which has persistent data storage, trackability, retrieval, and identity safeguarding in built into the system. This will allow us to enhance the transparency of the survey process as the candidate filling out the survey will always be allowed to track their survey response, allowing them to know whether it was counted towards the final result of the survey or not. This system will also aim to improve the fundamental privacy provided to its users as the users on the blockchain can be issued completely randomly generated identities to fill out their surveys. This will allow for eradication of any unnecessary biases from creeping into the feedback system. Finally, this blockchain based system will allow for an increase in the overall reliability of the stored data, as it is stored on a decentralized platform, so every node on the network will have a copy of the ledger. This will prevent any manipulation to the collected data.

B. Aims and Objectives

Many applications proved that the Blockchain Technology can be used in any process that requires a trusted third-party validation and it solves the issue of a single point of failure of the centralized applications. The Blockchain can bring a variety of benefits to different business processes. Some of these benefits are:

- Data preservation and integrity.
- An immutable decentralized database with no single point of failure.
- System provenance and governance, where the input and output of each process are validated and stored on every node on the network.
- Validation of a transaction through a customized automated validation procedure known as a "Smart Contract".
- Transparency and availability since all records are shared and validated by every node on the network.

Despite all these benefits, the Blockchain Technology has many limitations such as scalability and not all processes can be implemented to be validated on the Blockchain. The aim of this project is to investigate the benefits and the shortage of using the Blockchain technology to authenticate survey systems and implement one locally for a Course Feedback System.In order to achieve the aim of this project, there are some objectives and requirements that have to be fulfilled. These requirements are:

- Understanding the Blockchain technology as a tool from a technical perspective, away from the cryptocurrencies and its trading.
- Understand the current survey system and check how the presently available tools can be used in our Course Feedback System.
- Investigate the usage of other tools and technologies that support the Blockchain technology.
- Create and develop the suitable design structure for the Course Feedback System that can be implemented based on the characteristics of the framework and the requirements of the Blockchain technology.
- Develop a simple DApp to observe the behavior of the Blockchain and create a list of test scenarios that can

show the benefits of using this technology and the Course Feedback System.

C. Advantages and Benefits

These are the advantages and benefits which we feel our system will add to the currently prevalent blockchain-less Course Feedback Systems.

- **Data preservation and Availability:** The distributed nature of Blockchain ensures the Course Feedback System and resources are always available and findable for every client in the network. This supports the idea of open and unbiased surveys. These technologies protect the resources from the risk of the single point of failure, since all data will be shared on every node equally and verified using the consensus mechanism.
- **Feedback Tracking and Management:** The ease of management and tracking of the gathered feedback is especially simple in blockchain. This was useful when implementing the function which was allowing users to check if their feedback had been counted or not. This trackability and the ease of its implementation is one of the major advantages of blockchain.
- **Secure Sharing of Feedback:** The cryptographic power of the Blockchain adds more security to the stored data, therefore any modification of the data in any node on the network will cause the rejection of the node and mark it as "untrusted". Thus, the Blockchain technology can encourage feedback hosts to use the DApp to validate and store their feedback.

II. An Introduction to Blockchain

The Blockchain is a protocol that provides a high level of integrity using cryptographic operations in a distributed network to make sure that every node holds the correct data. [1]. Blockchain is considered a data structure that forms an append-only database, where the records of this database are shared between all nodes. This protocol forces the validation of the data stored on every node using a consensus mechanism. The most popular consensus mechanism is the Proof of Work (PoW) that requires every node to calculate the hash value of all transactions.

A. Types of Blockchains:

Blockchain can be developed with different permissions to perform read, write, and validate operations on the records that are shared between nodes. Below are the different types of networks that can be created using the Blockchain protocol:

- **Public Permissionless Blockchains:** any node can join the network, and every node is able to read and insert new transactions. In addition to that, all nodes have to participate in the consensus mechanism. Public Blockchains need to offer an incentive for the nodes that perform the validation. In cryptocurrencies, the network offers an amount of its currency depending on the amount of data that has been validated.

- **Private Blockchains:** recording new transactions is restricted to a centralized organization and the validation of records is done by the predefined nodes while reading permission can be public or private depending on the network design. Usually, no incentive is awarded to nodes that participate in the consensus mechanism.

- **Consortium Blockchain:** sending transactions is restricted to a predefined set of nodes, such that not all nodes have to validate the transactions since only the majority of the network is doing the validation. The right to read processed records can be permissioned or public based on the design. Consortium Blockchains allow the usage of different consensus mechanisms which makes validating the transactions more efficient than public Blockchains and relatively more scalable.

B. Existing Blockchain Platforms:

There exist many Blockchain platforms that enable the creation of decentralized applications. Following are the three most popular platforms -

- **Ethereum:** often defined as the "World Computer" is one of the Blockchain platforms that provide the ability to create Smart Contracts, using Solidity. Ethereum provides the ability to customize different consensus mechanisms other than PoW.

- **Hyperledger:** is a project developed by the Linux Foundation, it provides APIs that facilitate creating private Blockchains. Hyperledger supports the development of Smart Contracts using different programming languages, such as Go and Node.js.

- **Corda R3:** is an open-source project that provides the ability to create financial services on top of a Blockchain. In Corda, records are shared only between parties that are interested in using or validating the transactions to ensure the privacy of data. This makes this platform more scalable than any other Blockchain.

III. Design Choices

Different choices have to be made with respect to what technologies should be used before implementing the experiment of using the distributed technology with the Course Feedback System. In order for the feedback values to be shared and validated on a Blockchain network, the following design questions have to be answered:

- **What type of Blockchain should be implemented?** The characteristics of the Course Feedback System force the choice of a public Blockchain network with a testchain, since it provides public access to the validated transactions, and it can be customized to have the transactions validated by a specified number of clients

on the network.

- **Which Blockchain platform should be used?**
  Ethereum is the most preferred platform to build a consortium Blockchain for the Course Feedback System. The Hyperledger implementation is used for private Blockchains with the PBFT consensus mechanism, and the Corda development team consider any non-financial project "out-of-scope".

- **Where should the data be stored?**
  In this project, the Ethereum nodes will only contain the cryptographic hash values of the feedback received, whereas the complete feedback will be stored as a JSON package "off-the-chain" on a main database. This approach makes the application more efficient and scalable since the large data is stored off the chain and the Blockchain ledger only contains references to the values on the network.

IV. Design Overview

The Course Feedback System is different from a traditional cryptocurrency model as there will be a single commit transaction from each user as the submitted feedback. However, the Blockchain Technology can be implemented in different ways not only as a distributed ledger that contains transfer actions of cryptocurrencies. This section discusses the constraints and requirements of building a Blockchain protocol that can be utilized as a part of this Course Feedback System. These constraints can be identified as the following research questions:

- What part of the feedback structure should be validated by the smart contract?
- What are the changes that have to be made in order to make feedback ready to be registered on the Blockchain?
- What are the authentication services we will be building into the smart contract?

In addition to that, this section explains the design architecture of a DApp that uses the Ethereum Blockchain and the storage to validate and store Feedback Structures and the role of each technology in the developed application.

A. Involved Parties

In terms of the parties involved, which will be the actors in our DApp, we have majorly identified three actors. Their descriptions with their major roles in the Feedback process are as follows:

- **Administrator:** The administrator is the actor who will initiate the feedback system. He will be given two major roles, firstly that of creation of the survey to be filled by the client nodes, in our case, the students and he will be given the sole authority to add a new client to be allowed to give feedback. This is important as the administrator, who in our case will be the course Instructor in Charge, should be able to selectively allow only the students enrolled in his course to give the feedback.
- **Client:** The client nodes will be the nodes filling in the feedback initiated by the administrator. They will be first checked as to whether they have been given permission to vote. Then only will they be allowed to give the feedback for that course.
- **Blockchain Framework:** This is the Blockchain Framework on which we will be storing the results of the feedback system, to be retrieved and analyzed later. We have already discussed in depth about the Ethereum Framework, the blockchain framework of choice for this project.

B. System Operation Phases

The Course Feedback System will work in majorly in three phases. They are described below:

1) **Survey Creation and Student Registration Phase:**
   In this phase, the administrator will first create the Feedback form. After this, he will create a list of students to be permitted to give the feedback. Once that is made, those names will be committed to the Smart Contract. The student credentials will first be sent to the smart contract by the admin. There will be a check in place to make sure that the person sending this message is indeed the administrator. After this, a student object will be created and will be added to the list of students. Failure at any check point will result in the end of this phase for that particular attempt to give add a student.
2) **Student Feedback Recording Phase:**
   In this phase, the feedback form will be made open to receive feedback from the registered users. In that, the first check will be if the student has been registered to give feedback. Then the smart contract will check if the student hasn't previously voted. After these checks are passed, the feedback will be taken and a feedback object will be generated. A check to see if invalid arguments aren't being passed will also be in place. Finally, that Feedback Object will be published to the blockchain and the block number onto which the object was committed will be returned. Failure at any check point will result in the end of this phase for that particular attempt to give feedback.
3) **Final Feedback Collection, Analysis and Verification Phase:**
   After the feedback recording phase has been completed, the feedback will then be gathered from the committed feedback objects on the blockchain. The feedback can be collected from there and used for further analysis and draw inferences about the sentiment of the surveyed clients. One more feature which will be provided to the client will be that of the ability to check if his/her feedback has been counted or not. This will be done by having the clients end a hash of the feedback object generated, and having it checked if it matches the block value in the chain.

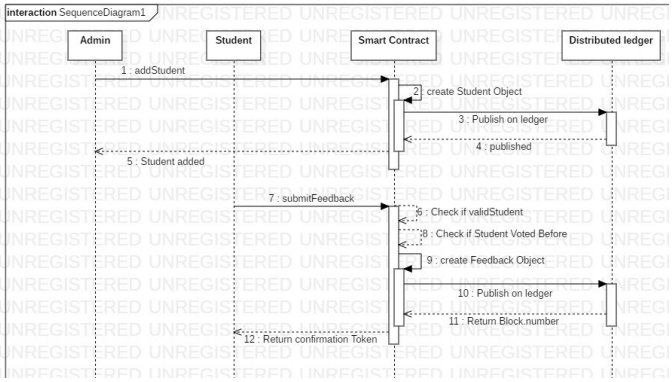

Fig. 1. Timeline Diagram of the System Operation Phases.

V. Implementation

This section focuses on the actual implementation of the code in the form of the smart contract. We discuss the tools we used for this project and then the description of the code written of the smart contract.

A. Tools Used

Multiple tools will be used in order to accomplish the objectives of this project and develop a DApp prototype for this project. There exist many APIs developed in different languages to interact with the Ethereum. The reason for that to make these technologies used by a wide range of developers. Our project will be developed in Solidity, the reason behind taking this approach is to use the stable distribution of each tool and to use a language which is deeply integrated into the Ethereum ecosystem. Following is the list of the tools that will be used in this project with the version of each tool:

- **Solidity:** Solidity is a object-oriented programming language. It is mainly used to write smart contracts on the Ethereum Blockchain. Solidity enables programmers to write the business logic of their smart contracts in an easy to understand form, which runs efficiently on the Ethereum Virtual Machine.
- **Truffle:** Truffle is the most popular development framework for Ethereum. It is a simple development environment, testing framework and asset pipeline combined into one for blockchains using the Ethereum Virtual Machine (EVM).
- **Ganache:** A personal blockchain for Ethereum development which can be used to deploy contracts, develop decentralized applications, and run tests. It is available as both a desktop application as well as a command-line tool (as Ganache-cli from NPM). It is a cross platform tool.
- **MetaMask:** MetaMask is a bridge that allows a user to visit the blockchain services in your browser. It allows the user to run Ethereum DApps right in the browser without running a full Ethereum node. MetaMask includes a secure identity vault, providing a user interface to manage user identities on different sites and sign blockchain transactions.
- **Remix:** Remix is a powerful, open source tool that helps users write Solidity contracts straight from the browser. Remix supports both usage in the browser and locally. Remix also supports testing, debugging and deploying of smart contracts.

B. Deployment

As of writing, the smart contract has been deployed to the Rinekby test chain, a sister chain of the Ethereum blockchain specifically used for testing smart contracts before deploying them to the actual Ethereum Blockchain. The address of the newly deployed contract is 0xc2745c0b2ca628ab34f903b0b4b564ce5191dd8a . The code is available at the following link: https://github.com/AtharvChandratre/CourseFeedbackSystem

VI. Scope for Further Improvement

These are some of the limitations we came across with our current setup, where we have observed scope for improvement, which can be implemented in the future:

- First of all, we are treating the blockchain as a single source of truth. The first approved data will be taken as a fact and cannot be changed; this is a general issue for most of the Blockchain applications. This immutability, which is one of blockchain's most important qualities, can also be one of its flaws in our use case, because if a person wants to go back and change his feedback, he will not be able to do so. Likewise, the process of recording transactions will be signed by the uploader and registered with his EOA. The Blockchain ensures the integrity of the recorded data, but, it cannot validate the source of data before it is recorded on the public ledger.
- Secondly, scalability is the main challenge of the Blockchain technology. This issue is not only caused by the replication of records on every node on the network. The continuous computing of the cryptographic hash of all transactions and chaining them to what was previously recorded in order to generate the proof of work (PoW) is the major cause of this scalability problems. The growing size of data needs to be encountered with a more scalable consensus mechanism such as the PBFT.
- Finally, smart contracts are deployed only once. The EVM generates an address to the Smart Contract when deployed and every record stored is only accessible by this Contract. This raises the concern whether a future update is needed to the Smart Contract. For this reason, the DApp needs to have a plan to transfer the recorded data from a contract to another.

Acknowledgment

The success and final outcome of this project required a lot of guidance and assistance from many people and we are extremely privileged to have got this all along during the progression of my project. All that we have done is only due

to their supervision and assistance. We are extremely grateful to Dr. Vinayak Naik, Head of Department, Department of Computer Science, BITS - Pilani, K.K. Birla Goa Campus, for his guidance as our mentor and for providing us such amazing support while taking time out of his busy schedule at regular intervals. Our appreciation also goes to our friends and colleagues who have helped us develop the project, and to all those people who have lent a helping hand with their abilities and skills. We would also like to take a moment to thank all the organizations and individuals currently working in this field, without whose prior breakthroughs, we would not have been able to bring this project to fruition.

REFERENCES

[1] N. Bauerle, "What is Blockchain Technology?," CoinDesk, [Online]. Available: https://www.coindesk.com/information/what-is-blockchain-technology.
[2] D. Dob, "Permissioned vs Permissionless Blockchains: Understanding the Differences," 2018. [Online]. Available: https://blockonomi.com/permissioned-vspermissionless- blockchains/.
[3] S. Khatwani, "What Are Private Blockchains and How Are They Different From Public Blockchains?," 2018. [Online]. Available: https://coinsutra.com/private-blockchainpublic- blockchain/.
[4] B. Asolo, "Consortium Blockchain Explained," 2018. [Online]. Available: https://www.mycryptopedia.com/consortium-blockchain-explained/.
[5] V. Buterin, "Ethereum Whitepaper," 2013. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.
[6] Hyperledger-Foundation, "About Hyperledger," 2018. [Online]. Available: https://www.hyperledger.org/about.
[7] Corda-Platform, "The Corda Platform," 2019. [Online]. Available: https://www.r3.com/corda-platform/.
[8] BlockGeeks, "What Are Dapps? The New Decentralized Future," 2017. [Online]. Available: https://blockgeeks.com/guides/dapps/.
[9] BlockchainHub, "DApps and their types," [Online]. Available: https://blockchainhub.net/decentralized-applications-dapps/.
[10] M. Pratap, "What are Decentralized Applications, DApps?," 2018. [Online]. Available: https://hackernoon.com/what-are-decentralized-applications-dapps- 3b63b4d587fe.
[11] A. Quay, "A Beginner's Guide to IPFS," 2018. [Online]. Available: https://hackernoon.com/a-beginners-guide-to-ipfs-20673fedd3f.
[12] BlockGeeks, "What are smart contracts?," [Online]. Available: https://blockgeeks.com/guides/smart-contracts/.
[13] J. Frankenfield, "Consensus Mechanisms (Cryptocurrency)," 2018. [Online]. Available: https://www.investopedia.com/terms/c/consensus-mechanismcryptocurrency. asp.
[14] Solidity, "Solidity Documentation," 2019. [Online]. Available: https://solidity.readthedocs.io/en/v0.5.3/.
[15] Truffle, "Truffle Github Documentation," 2019. [Online]. Available: https://github.com/trufflesuite/truffle.
[16] Ganache, "Ganache Github Documentation," 2019. [Online]. Available: https://github.com/trufflesuite/ganache.
[17] Metamask, "Metamask Github Documentation," 2019. [Online]. Available: https://github.com/MetaMask/metamask-extension.
[18] R. IDE, "Remix IDE Documentation," 2019. [Online]. Available: https://remix.readthedocs.io/en/latest/.
[19] D. Rosenthal, "Blockchain Solves Preservation!," 2018. [Online]. Available: https://blog.dshr.org/2018/09/blockchain-solves-preservation.html.
[20] D. Sondregger, "Blockchain In Practice: A Single Source Of Truth," 2018. [Online]. Available: https://abovethelaw.com/2018/03/blockchain-in-practice-a-singlesource- of-truth/.
[21] TSS, "A gentle introduction to blockchain scalability (Part I)," 2018. [Online]. Available: https://medium.com/sandor-report/a-gentle-introduction-toblockchain- scalability-part-i-42d477898122.
[22] T. J. Rush, "Smart Contracts are Immutable — That's Amazing... and It Sucks," 2016. [Online]. Available: https://medium.com/@tjayrush/smart-contracts-areimmutable- thats-amazing-and-it-sucks-e0fbc7b0ec16.