A decentralized blogging cum messaging application built on top of ethereum platform

Vignesh Varadarajan
Georgia State University
vvaradarajan1@student.gsu.edu

Sohan Sathyan
Georgia State University
ssathyan1@student.gsu.edu

Kiruthiga Sekar
Georgia State University
ksekar2@student.gsu.edu

***Abstract*—The first ammendment of the United States constitution provides freedom of speech as one of the fundamental right. But in todays world, many of the powerful entities are controlling the communication medium and this has put our right to freedom of speech in danger.In this project paper, we have propsed a multipurpose decentralized ethereum based application that allows the users to exchange their ideas without the fear of being censored or tracked.The app allows the authors to securely publish their blog.In addition to the blog, the application also enables the users of the application to have a private conversation. Finally to monetize the authors of the blog without having to display the annoying advertisements,the readers are provided with an option to applaud/like the blog.Doing so will trigger a transaction over the blockchain network, which will transfer a particular amount of money from the reader to the author of the blog.**

I. Introduction

In today's digital world, the internet is most significant medium of mass communication. Ideally, people should be able to express themselves freely, but the powerful entities like a government institution or a large corporation often create hindrance to your ideas from reaching the common mass by either censoring your blog or by deleting your blog altogether. In addition to this, currently available platforms pay the bloggers for the advertisements that are displayed in their blogs and not for the blog itself.

We are tackling these problems by building a decentralized blog application using smart contracts that runs on top of the Ethereum blockchain. The main features of our application are: (1) It is decentralized, (2) It provides a way to incentivize the author without having any advertisements and (3) Provides a messaging system which eases the communication between the author and the readers of the blog.

The decentralized nature of the application ensures that there is no central authority or a powerful entity to control the activities on the application. As the application runs on Ethereum blockchain, we observe that the system is resistant to censorship such that once an author has control over his blog.

This application allows the readers to incentivize the author if they enjoy reading the article. Whenever an article is applauded, a new transaction is initiated, which will transfer bitcoins from the reader to the author. This will avoid the advertisements, that are irrelevant to the blogs.

This application also provides a messaging system wherein any two users can communicate with each other to exchange their ideas in a secure environment. This messaging system would help the readers to get more insights about the article by interacting with the author. This messaging system can be used by any users of the platform to communicate with one another.

The sole intention of this project is to develop a secure environment for people to express their thoughts with no government or any other organization controlling the activities of the bloggers and censoring any articles, based on a criticized topic.

II. Related Works

This section briefly surveys some of the blogging and chat platforms currently available

A. Medium

Medium is a centralized online platform for publishing blogs. As part of its content creators, Medium has a hybrid collection of professionals and amateur people who publish articles in their platform. Medium pays the authors based on a formula that depends on factors like how much time a reader spent on the article, how much claps or likes the article has received. A blog can be clapped up to 50 times, which potentially describes the quality and the likeliness of the post. Some of the problems that we see with Medium are:

1) Medium being a centralized organization, it is prone to censorship from either the government or from the people calling the shots in the company. For Ex: In April 2016, Medium was blocked in mainland China after information from the leaked Panama Papers was published on the site. This would not have been the case if Medium was run on a blockchain.
2) Medium does not provide a private messaging system in its platform. Any two users of the platform can only communicate with each other in the open through the comments section.
3) A user can clap a blog only up to 50 times to show their appreciation to the story.

B. Steemit

Steemit is a blockchain based blogging and social media platform that rewards people with cryptocurrencies for publishing high-quality content. This concept is similar to Medium, but it uses the blockchain for the reward system.

As people upvote any post, the authors are rewarded with STEEM Dollars, which can later be traded for Bitcoins or Ethereum.Even though Steemit solves the problem of censorship as it is a decentralized platform, Steemit comes with its share of problems:

1) There are multiple reports that claim that Steemit has a flawed payment system.
2) Like a medium, even Steemit does not have its own messaging system.

C. *Whatsapp*

WhatsApp Messenger is a freeware and cross-platform messaging and Voice Over IP(VoIP) service owned by Facebook. The main selling point of WhatsApp is the claim that each message in their platform is encrypted and only the users who belong to the conversation can decrypt the messages and read them. But as WhatsApp is not open sourced, there is no way to confirm this claim. The other issues with WhatsApp are:

1) As it is a centralized organization, it is prone to censorship.
2) There is no blogging platform in WhatsApp where people can share their ideas.

III. Implementation

The Ethereum blockchain based application SpeakItOut was implemented using the solidity programming language for the backend and ReactJS for the front end. The other technologies that were used to build this application are listed below.

A. *Technologies used*

a) Solidity: Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs which govern the behavior of accounts within the Ethereum state. We have used Solidity version 0.5.0 in our project.

b) Truffle: Truffle is a development environment, testing framework and asset pipeline for Ethereum, aiming to make life as an Ethereum developer easier. We have used truffle to compile and deploy our smart contracts. We have used Truffle version5.0.7 in our project.

c) Ganache: Ganache is a personal blockchain for Ethereum development that can be used to deploy contracts, develop your applications, and run tests.We have used Ganache version 2.0.0 in our project.

d) Metamask: A google chrome extensions that allow us to run Ethereum dApps right in the chrome browser without running a full Ethereum node. We have used Metamask version 6.4.1 in our project.

e) ReactJS: ReactJS is a javascript library for creating user interfaces.

f) web3.js: The web3.js library is a collection of modules which contain specific functionality for the Ethereum ecosystem. Among the collections, we use

1) The web3-eth is for the Ethereum blockchain and smart contracts
2) The web3-utils contains useful helper functions for DApp developers.

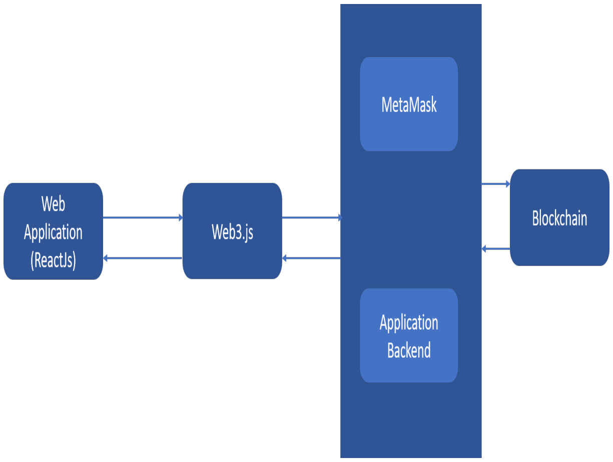


Fig. 1: Design of our application-SpeakItOut

B. *Detailed Implementation*

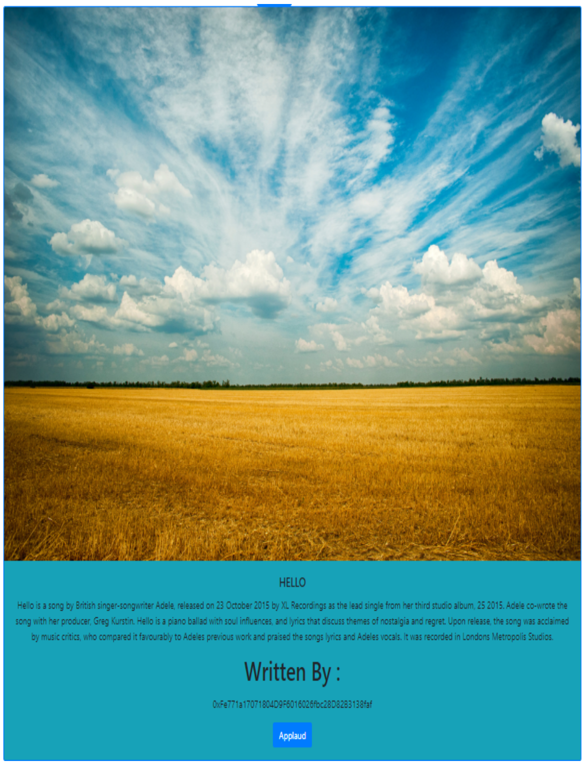
a) Blog: For blogs, we have used mapping to store the generated ID of the blog which the key and it's contents as the value which is the blog itself. Each Blog itself is saved as a struct, a data structure in the solidity that allows us to group all properties of a particular object. A mapping is used to structure value types, such as booleans, integers, addresses, and structs. It consists of two main parts: Key and a Value

b) Chat: For implementing the chat application, we have made use of events. Hence the all the messages are stored in the blockchain, but instead of storing it in the smart contracts it is stored in the logs of the blockchain. And to retrieve the messages, we just query the logs. To achieve all these, we had to index the sender and receiver addresses in the events(This allows us to query the messages on the logs based on sender and receiver address).Even though it costs us some gas to retrieve the message from the logs, it is significantly cheaper than storing the message in the smart contract. The blockchain is a list of blocks which are fundamentally lists of transactions. Each transaction has an attached receipt which contains zero or more log entries. Log entries represent the result of events having fired from a smart contract. In the Solidity source code, to define an event, you mark it by preceding it with the event keyword (similar in usage to the function keyword). You then call or fire the event in the body of whatever function you wish to cause to generate the event. You may fire events from any function using the emit keyword. Now, using web3.js which provides functions to filter and retrieve appropriate logs and fetch the chats from there

c) Profiles: Each profile is saved as a struct. Here we save the first name, last name as part of the struct. Each profile is uniquely identified by its address. This relationship is provided using maps in solidity.

d) Applaud: This feature provides a way to transfer ethers between two accounts. When an author selects a particular blog and chooses to applaud it, the sender and receiver accounts are captured, and one ether is transferred from sender to receiver.

All the transactions that update the blockchain would require gas as part of each transaction. Gas is a unit of measuring the computational work of running transactions or smart contracts in the Ethereum network. Hence, the accounts that make any of the transactions must have sufficient balance in their account.


HELLO

Hello is a song by British singer-songwriter Adele, released on 23 October 2015 by XL Recordings as the lead single from her third studio album, 25 2015. Adele co-wrote the song with her producer, Greg Kurstin. Hello is a piano ballad with soul influences, and lyrics that discuss themes of nostalgia and regret. Upon release, the song was acclaimed by music critics, who compared it favourably to Adeles previous work and praised the songs lyrics and Adeles vocals. It was recorded in Londons Metropolis Studios.

Written By :

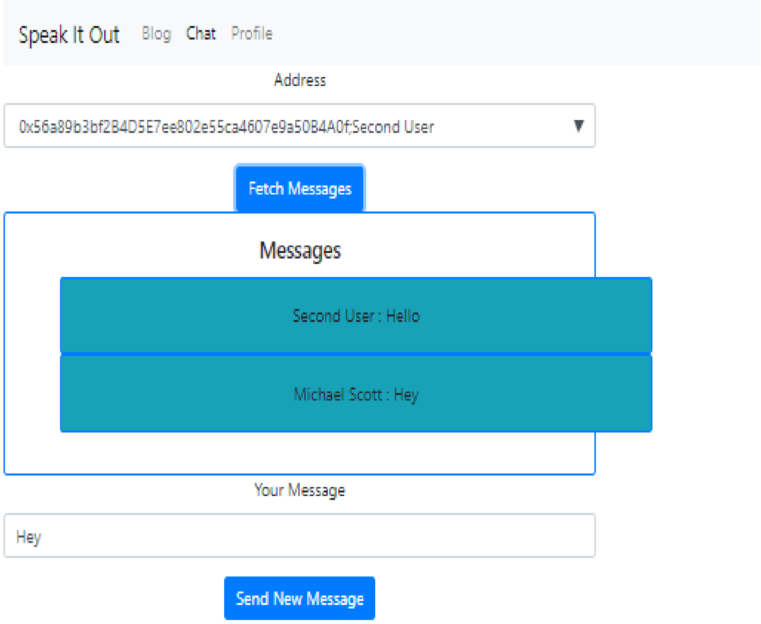
0xFe771a17071804D9F6016026fbc28D82B3138faf

Fig. 2: UI for displaying the Blog

IV. Conclusions

In this paper, a decentralized blogging cum messaging app running on the ethereum platform was developed. Developing the application on the ethereum blockchain makes sure that no single person has control over the platform and prevents a powerful entity from censoring the contents published. In our approach, we have used the blockchain to save the blog data and the message data(message data is saved in the logs). Doing so has its own set of advantages and disadvantages. The advantages being that no single person can delete the blog or erase the conversations that happened in our platform. But the major drawback of using this approach is that writing data into the blockchain incurs a cost in terms of gas and as the price of ethereum increases, the cost to write a blog and to send messages also significantly increases for the end user. One more thing that we used for the messaging feature of our application is that the messages are not directly stored in the blockchain. Instead, they are stored in the blockchain in the logs as it is much cheaper to store things in logs as compared to contract storage. What surprised us about events was the fact that anyone in the ethereum blockchain can query the logs. Finally, as part of the future work of the project, we would like to do two things:

1) Explore the possibility of storing the blog data outside the blockchain.
2) Encrypt the message when a user is sending it and decrypt the message when he or she wants to retrieve it.



Address: 0x56a89b3bf2B4D5E7ee802e55ca4607e9a50B4A0f;Second User

Second User : Hello

Michael Scott : Hey

Your Message: Hey

Fig. 3: UI for chat application

References

[1] https://solidity.readthedocs.io
[2] http://www.dappuniversity.com/
[3] https://cointelegraph.com/news/blockchain-network-takes-on-flawed-steemit-by-offering-lifetime-earnings-to-creators
[4] https://web3js.readthedocs.io/en/1.0/