International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

Block chain based Application to Curb Hoaxes on Social Media using Decentralized Voting System

Parimi Shiva Kalyan, V. Kakulapati, Parimi Arvind

Abstract— Fake news on Social Media has become widespread with branching of technology over various domains and its accessibility to the general public being a major concern. Social Media hoaxes have become the new trend to gather popularity and fan base. Block chain based voting application is one such solution which is capable of curbing fake news by adapting a decentralized voting system in which knowledgeable and sound voters analyze percent of veracity behind a particular news given to vote and accordingly caste their vote on the decentralized application which in turn generates a result providing information about which news in circulation tends to be fake and which does not.

Keywords—Block chain, Voting System, Fake News, Social Media, Social media hoaxes, Decentralized application, Block chain voting system, Decentralized voting system.

I. INTRODUCTION

Social Media has always been a platform where we can observe fake news spread aiming distinct purposes, few of them being popularity and prom. These create a psychological imbalance of decision in an individual which leads to conflict in understanding what's legitimate and what's not. This phenomenon can be compared with the "Message Transfer" game where one player transfer messages into the ear of other player and the message is transferred over a chain of players and then the initial message and the final messages are compared to check whether the message still carries the same meaning or not.

Block chain [1] is the trending technology which works on decentralization which grants equal rights for everyone in the ring to vote for the authenticity of the news based on their prior knowledge about the subject. Block chain hence store details such as gas fee, and the cost of the transaction in its block.Since the platform contains the hefty amount of voters who contribute their part by voting for the authenticity, the security constraint must also be maintained. This is achieving in the system by using a cryptographic approach where a private key is using by voter to create a one-time account to cast his vote for a single time after which the account cannot be using for further transactions. This doesn't only ensure that there's relatively zero plagiarism of votes but also records the details of the voter and the key which was used in casting the process of casting the vote in order to maintain the uniqueness of the vote and authenticity at the same time.

Manuscript published on 30 April 2019.
***** Correspondence Author (s)
Parimi Shiva Kalyan*, Sreenidhi Institute of Science and Technology, Yamnampet, Ghatkesar, Hyderabad-501301.
V. Kakulapati, Sreenidhi Institute of Science and Technology, Yamnampet, Ghatkesar, Hyderabad-501301.
Parimi Arvind, Reliance Home Comfort, Kitchener, Ontario, Canada.

II. RELATED WORK

II.A. Cryptography based Voting System

Cryptographic voting system [2] is a flavour of the environment where there are various roles assigned to distinct individuals who play their roles and supervise the process of voting system. Roles include, key distributor, key generator, president and Vote recorder who play the role of distributing the generated keys to the voter, generate distinct key based on cryptography methods, and keep a record on the vote count respectively. These methods primarily focus on encryption and decryption of the keys in the voting process for successful registration of the vote.

II. B. Decentralized Applications

Decentralized applications are innovative application architecture that tend to work on distributed computing system [3]. Hence, it is not controlling or overlooking by a single entity, but it is overlooking by a group of individuals in the ring, thereby ensuring the transparency and trustworthiness of the transactions happening in the block chain network. Decentralized applications [4], better known as dApp, are a bit identical to the basic web application. They are written in the same front-end languages. The only non identical part of dApp is, they use smart contracts which connect a dApp to the block chain, hence making the series flow through front-end, smart contract and block chain. On decentralization comes distributed ledger, i.e. every transaction happening in the block chain network [5] is recorded in every ledger owned by the entities present in the network ring. This ensures the transparency of transactions taking place in the network between various elements in the ring.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

III. PROPOSED WORK WORKFLOW

This proposed system uses solidity as it's primary programming language with several unique frameworks such as Ganache and Node Package Manager with truffle. The voting system is designed using HTML and CSS with JavaScript validations adding authentication with smart contracts in block chain with solidity as the base. This system uses cryptography and smart contracts as a whole in order to register votes casted by the voters for the authenticity of the news. The proposed block chain decentralized application works with Node package manager and by installing different framework which define the flow of control from various sub modules of the block chain application. From security constraints to the result generation are covered in the sub modules defined below.

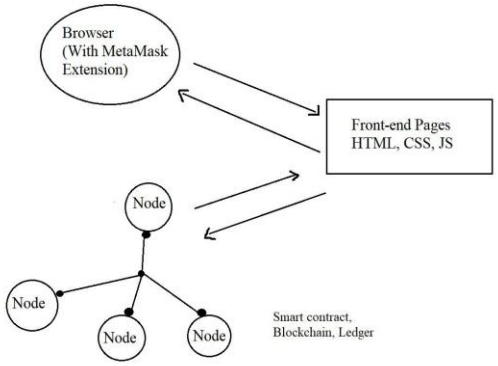

Fig. 1. Framework of our approval

This application uses a secure voting system approach, where there are multiple check-doors within every step to ensure that there's near to zero plagiarism generated by the voters i.e. no vote is casted twice with the same key under the same name. This is ensuring by importing accounts using a private key. The imported account cannot be imported again during the same session hence making it less vulnerable to plagiarism and securing the environment by the time out sessions using web3 API.

This application is programmed in solidity, the smart contracts that exist in the "Contracts" folder of the block chain files are written in Solidity with pragma header files. These smart contracts as a medium between the front-end of the application and the block chain database. Record each transaction/vote in this case with the application User Interface. The voter in this case represents an individual who has knowledge and verifies news sources from distinct sources and frames them into one single view. Using this perspective the individual tries to register the vote in the Block chain based architecture [6]

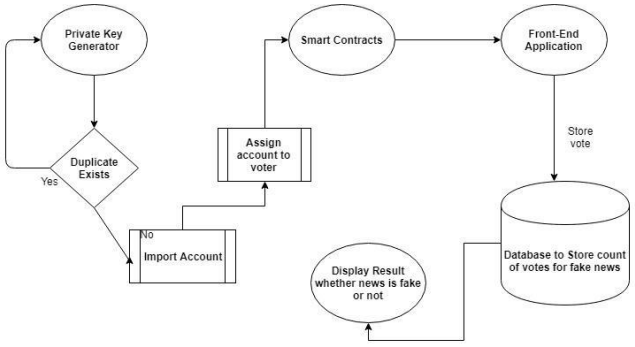

Fig. 2. Workflow

IV. A. Key Generation Functionality

The keys for the account creation on MetaMask are generated from Ganache. Every instance of Ganache from NPM has a mnemonic which can be used to generate a set of private keys and get those private keys for an individual to vote. Functions such as mnemonicToSeed (), getPrivateKey (), getPublicKey() are used to get the public string and private string in the key generation segment.

'address' : node.getWallet().getAddressString();
'privateKey' : node.getWallet().getPrivateKeyString();
'publicKey' : node.getWallet().getPublicKeyString(); To include Ethereum wallet we use
const wallet = require('ethereumjs-wallet');
const privatekey = addrnode.getWallet().getPrivateKey();

The getWallet() function is primarily responsible to return the wallet which is in association with the response obtained from the request. The getPrivateKeyString() function returns a private key String using the function. This string cannot be "Null". The private key varies accordingly with the wallet being imported. In this case the wallet being Ganache which provides Ethereum transactions over a gas fee. The getPublicKeyString() function returns a public key String, this combination of public key and the private key obtained from getPrivateKeyString() and getPublicKeyString() are used to import accounts over MetaMask.

IV.B. Smart Contracts

These are also known as Self-executing contracts are basically mere computer codes which are execute and supervising by various individuals/organizations present in the ring. This hence removes the necessity for the middleman in the block chain transactions thereby ensuring transparency and recording of each transaction happening over the net-work. In this paper, we have implemented a smart contract which is capable of recording the

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

number of votes in favour of/against a specific set of fake news. The voting system is implemented by defining a structure in the solidity file. The functions present in the Elections solidity file which is responsible for the voting process for fake news mainly consists of two basic functions, namely addFakeNewsSet () and vote (). The other functions present in Smart Contracts include keyGeneration (), keyMatch () and importAccount().

IV. C. Function addFakeNewsSet ()

The function addFakeNewsSet() takes a parameter of String array type which is a set of collection of fake news spread across Social Media gathered from different resources and groups and whose authenticity needs to be put to a test.
The function addFakeNewsSet () basically adds data i.e. the collection of fake news gathered from various different sources in an array with the structure for Election system in order for voting to take place. The Structure for adding the fake news set consists of an id, count of votes and the fake news to be displayed for the voting system, thereby creating a back-end for the voting system to bring it to reality. Every time the fake news set is updated in the array the counter value is improved to keep a count and to display the end result of how news turned out to be fake from the total number of news presented.

IV. D. Function vote ()

The function vote () takes the unique identity number given to fake news as a parameter and counts the number of votes casted for a particular identity number. The identity number is given in a back-end process, whereas in the front-end only the fake news is visible to the voter to choose and vote. This id number counter is increase every single time when a vote is casted for a specific set of fake news. The vote counter keeps track on the number of votes received for specific fake news and increments on incoming votes for the same. The private keys used in this process to the vote are also stored in the block chain network to keep a track that in the same session no voter can actually vote multiple times for the same fake news.

```
function vote(uint id)
f
//vote recording
g
```

IV.E. Importing Accounts using Private Keys

Using the generated private keys via getPrivateKeyString() method, the account on MetaMask are imported via the private key and the public string i.e. the seed phrase. These imported accounts are initialized with initial Ethereums so that the individual can vote.
Imported accounts in a session are assigned to distinct voters so that they can continue the voting process to vote for the authenticity of the news provided in the session. The results are collected and shown to the general public with maximum votes for a news results in more ”fake” content, and least votes means it is ”less fake” as compared to the other news in the set.

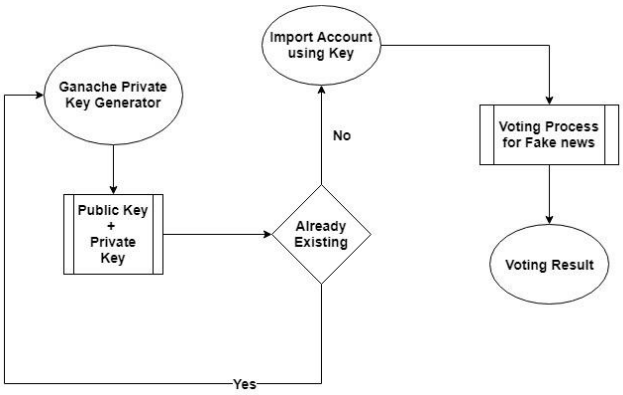

Fig. 3. Importing Account for Voting Process

Fig 3 depicts the framework involved in importing an account for the user/the individual who would vote for the authenticity of fake news being spread on Social Media.

IV. F. Front-End Voting System.

The front-end or the user end comprises of a HTML with JavaScript validated page that is responsible to show the use case of the application i.e., display the fake news via a drop-down the menu and the user gets to select one of them, which is not true. The front end is responsible to collect the user input/choice and revert the same in the database which in-turn increments the counter. This collected information is later shown with every fake news and opposite to it, the number of votes it received on”Fake scale”.

V. PERFORMANCE FACTORS & RESULTS

Fig 4 depicts the private key generated from PKG (the private key generator) which generates the private key so that the accounts to vote for authenticity of the news can be imported using the private key. And the voting process can continue.

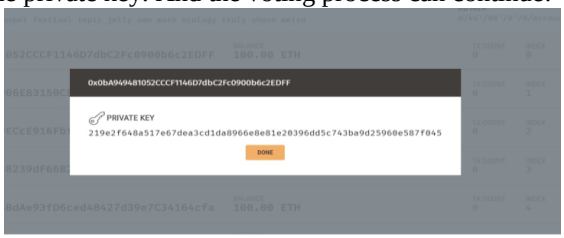

Fig. 4. Generating private keys to Import vote accounts

Fig 7 maps the result gathered after the voter/individual votes for the fake news. It shows the number of votes gained by particular news by different voters. The more the votes the more it has the score on”Fake Scale” i.e. the more votes, the more it is away from the truth. The account number of the voter is also shown below for refrence.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

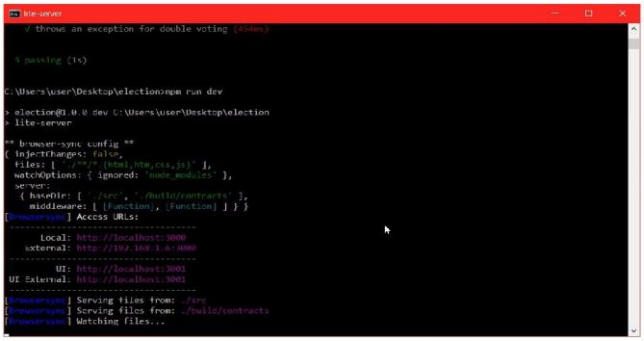

Fig. 5. Running lite-server for Front-End application

Fig 5 depicts the npm terminal running web3 lite-server. Lite server is basically a CLI that has static HTTP server which acts as a backbone to Single Page Applications. The lite-server package can be installed with the following command; npm install –save-dev lite-server

Fig. 6. Voting User Interface/Block chain Implementation

Fig 6 depicts the application where the voter votes for the fake news out of given options as seen in the image above. The user gets a chance to use his one vote to pick out fake news from the given set of fake news. Here, it is being"Rs.10 Rupee coin banned by Indian Government".

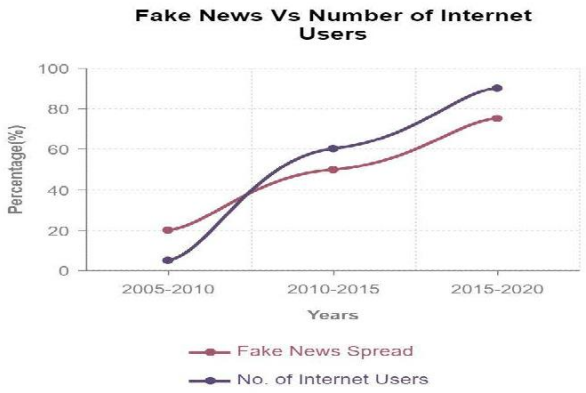

Fig. 8. Fake News Vs Number of Internet Users

Fig 8 depicts the drastic increase that can be observed in the general public using Internet over time. As the Smartphone industry occupies the top place in Electronics section, World Wide Web has also hit the top-notch. We can infer from the above graph that fake news also has increased to top levels after the general public is introduced to various different sources on the Internet, and hence the hefty variety of Fake news is being spread among the Network circle with least technology present to avoid the circulation of such fake news.

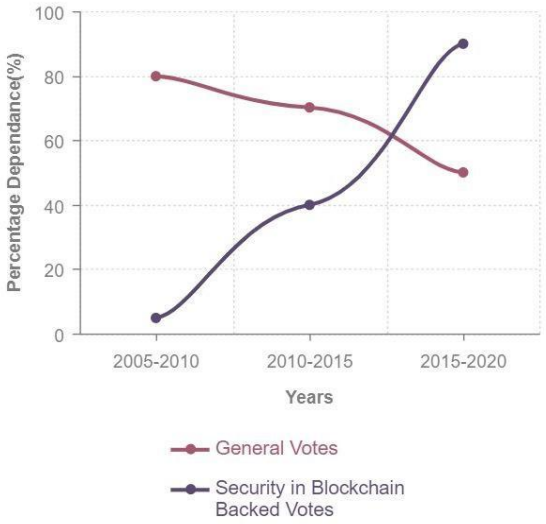

Fig. 9. Dependency on Quality Factor for Block chain Votes

As we can observe that not only the performance but other constraints such as security and ledger are added features in Block chain based voting system to curb fake news as compared to the general voting system. In the above image, we can observe that the interest of the general public in the mainstream voting system has decreased because of tampering and lot many other reasons, whereas the emerging technology "Block chain" is able to grab many eyes.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

In this system, we can say that the outcome/result can be seen as the general interest to curb fake news increases as Block chain based voting system is introduced.

VI. CONCLUSION & FUTURE SCOPE

As the count of fake news being spread on various Social platforms such as WhatsApp, Facebook, etc have increased, there's an immense need to stop the news from getting into the belief of the common public. Block chain based voting system acts as a perfect solution to these problems by creating a secure yet efficient and transparent voting system where there's distribution of power, hence decreasing the chances of monarchy and ensuring that fake news is identifying and is voting by voters to curb it. An addition to this can be a secure block chain based wallet that can give credits to the user according to the previous votes that an individual did against fake news. The individual awarded with credits can link his account with Block chain based voting system and vote for the authenticity of the news with the credits gifted from the previous transaction, hence generating enthusiasm among the public regarding curb on fake news.

REFERENCES

1. Fririk . Hjlmarsson, Gunnlaugur K. Hreiarsson, Mohammad Hamdaqa, Gsli Hjlmtsson,Blockchain-Based E-Voting System, Published in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD).
2. Rifa Hanifatunnisa, Budi Rahardjo, Blockchain based e-voting recording system design, Published in 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA).
3. Cosmas Krisna Adiputra, Rikard Hjort, Hiroyuki Sato, A Proposal of Blockchain-Based Electronic Voting System, Published in 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4).
4. Rafer Cooley, Shaya Wolf, Mike Borowczak, Blockchain-Based Election Infrastructures, Published in 2018 IEEE International Smart Cities Conference (ISC2).
5. Kejiao Li, Hui Li, Hanxu Hou, Kedan Li, Yongle Chen, Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism Consortium Blockchain, Published in 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS).
6. Emre Yavuz, Ali Kaan Ko, Umut Can abuk, Gkhan Dalkl, Towards secure e-voting using ethereum blockchain, Published in 2018 6th International Symposium on Digital Forensic and Security (ISDFS).