Vel Tech
Rangarajan Dr. Sagunthala
R&D Institute of Science and Technology
(Deemed to be University Estd. u/s 3 of UGC Act, 1956)

Department of Information Technology
Major Project Review 1

FORGERY DATA DETECTION FOR NATIONAL SECURITY USING BLOCKCHAIN

SUPERVISED BY

Mrs. JAYANTHI. K
M.Tech
Assistant Professor

PRESENTED BY

Yugandhar Surya (VTU 12278)

FORGERY DATA DETECTION FOR NATIONAL SECURITY USING BLOCKCHAIN

ABSTRACT

One of the most important outlets for exchanging information between social groups is social networking. Not only real news, but also rumours and fake news, are widely disseminated via social media. Users benefit from online platforms since they can simply get news. However, this provides a chance for cyber thieves to distribute bogus news via these channels. Readers read the news and begin to believe it before verifying it. Detecting false news is a significant difficulty since it is not a simple process. To address this issue, blockchain is being utilised to control the spread of misinformation. The suggested system records and analyses disseminated material, limiting the amount of fake news and user manipulation. The system also includes a real-time alert panel that uses user votes to determine the truth of the news.

Once the threshold value is achieved, the news status is continually monitored and adjusted. The false word data collection may be used to identify misleading phrases and stop fake news from spreading. To reduce the consequences of rumours and their uncontrolled spread, all news that reaches the public eye must first be cross-verified by intellects. With the use of block-chain, the proposed initiatives might give governmental entities the capacity to check material and decide whether or not it is authentic enough to be spread among everybody. Because, unlike traditional methods, blockchain tends to share copies of the same data to every individual with hash codes in the system, the certainty that the data cannot be hijacked or corrupted is strong. Along with various characteristics that protect data from cyber-attacks, blockchain technology has the potential to grow service in all areas while maintaining total transparency and intelligence.

Guided by

Mrs. JAYANTHI. K

M.Tech

Assistant Professor

Presented by

Yugandhar Surya (VTU 12278)

INTRODUCTION

Blockchain is basically an storage or electronic ledger which safegaurds the digital data, information, content or currencies with locks in terms of hashes that changes each time if any change in information takes place anywhere in the chain. Change in the hash code keeps all the participants updated with new updates. In near future, Blockchain technology is likely to bring advancements in all sector including banks and online transactions, automobile, automotive, food supplies etc. Smart contract plays very crucial role in the field of blockchain. Smart contracts are similar as contracts but in e-format. Every participants of each chain are connected with each other through smart contracts.Blockchain re-evaluated the requirement of third-parties in trading or transactions and eliminated them which resulted in making the whole process de-centralized and secure.

Forgery in any kind of data or information becomes quite simple, nowadays technology like GANs is being used to generate deep fakes and fake images. The bitter truth is to be captured here is, these thing is being used in creating child sexual abuse material, bullying, financial fraud, revenge porn, fake news, etc.

The main reason behind these forgery data is the invisibility of the creator, mutable data, and insecurity on web2.0. At a saturated level machine or deep learning fails to identify the deep fakes and also to achieve high accuracy, these algorithms need data in bulk to train with, and to store big data high computational database is needed which will cost higher. Using blockchain the data will be transparent, secured, immutable and so the authenticity of data increases.

LITERATURE SURVEY

1. L. Zhang et al.(2021).”Peer-to-Peer Networking and Applications” To take action against news and online curated content on the internet which could be inimical to the sovereignty of any nation, the proposed solution being implemented by smart contracts may have the capacity to identify and flag such contenton websites and social media. According to L. Zhang et al.(2021)[1]Fake news, press freedom disputes, advertising fraud, difficulty in digital rights management, flaws in content creation methods, and rumour spreading exacerbated by social media are all challenges that content producers and social media must deal with.All of the difficulties stated above are mostly caused by centralized servers or, to put it another way, management and all of the conceivable decisions made by a single person, allowing anybody to modify data as they choose.Blockchain technology, characterized by decentralization, security, and tamper-proof, offers a brand-new perspective on the above problems.

2. P. Fraga-Lamas and T. M. Fern´andez-Caram´es (2020)”Fake News, Disin- formation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality”, fake news raises worries about the Internet and social media’s role in modern democratic countries, which might result in large economic losses or national security problems.This study attempts to investigate the potential of distributed ledger technologies (DLTs) to prevent digital deception by defining the most relevant applications and identifying the main problems they face. Blockchain and other distributed ledger technologies (DLTs) guarantee the provenance and traceability of data by providing a transparent, immutable, and verifiable record.

3. S.Cho and C.Jeong (2019) ”A blockchain for media: Survey”, In their study they have stated that We can assure that any type of content is fully secured using blockchain.In their paper, they looked at how to characterise blockchain in digital subjects like media and interactive media as media blockchain. They also stated that a network is made up of devices that are lightweight, such as low storage space and computing performance, and that these issues degrade network security performance. It can be used for tracing and managing right information on content delivery platforms.

4. S. E. Haddouti, et.al, 2019, ”Analysis of Identity Management Systems Using Blockchain Technology,”. They have investigated and gives us analysis of the most popular Identity Management Systems using Blockchain: uPort, Sovrin, and ShoCard. It then evaluates them under a set of features of digital identity that characterizes the successful of an Identity Management solution.The comparison analysis findings are provided in a clear and straightforward manner, allowing readers to quickly determine which systems meet which standards, allowing them to choose the best system for a given scenario.

5. Shilpashree B N, et al.(2021),“Counterfeit Detection of Documents using Blockchain” it’s shown that InterPlanetary File System [IPFS] protocol and also a peer-to-peer-network for storing and sharing data in a distributed file system and can make a system that will be more secure and efficient for digital certificate validation.They advocated using blockchain technology to solve the problem of document counterfeiting.The blockchain technology offers the user’s documents with the authentication, authorisation, privacy, secrecy, and ownership that are required attributes of digital documents.

6. Shovon Paul, Jubair Islam Joy et al.(2019),”Fake News Detection in Social Media using Blockchain,” We'll talk about how to detect fake news in social media using the benefits of Blockchain's peer-to-peer network concepts.According to them, use of the concept of decentralization, Ethereum smart contract and use BFS algorithm for calculating proimity of an user.Whenever news has been created, it will be broadcast through the chain by the transaction. Here, we will review only those particular news’ which have surpassed a certain limit of virality. The news will spread over the chain. General users may also get the news, but initially, this news will have no rating. As time passes by, validators will provide their reviews, and then the news will pop up with a rating to the users. This rating represents the correctness/authenticity of particular news.

7. M. Torky, Emad Nabil, Wael Said,2019, “Proof of Credibility: A Blockchain Approach for Detecting and Blocking Fake News in Social Networks.”Blockchain as a powerful technology can provide a miraculous solution to overcome validating information credibility and reliability for social network platforms due to its immutability, security, tamper-proof, and P2P design.It offers Proof of Credibility (PoC), an innovative blockchain approach for detecting bogus news and preventing its spread on social media. On two datasets of newsworthy tweets obtained from various news sources on Twitter, the PoC protocol's functionality was simulated.

8. Yazed Alsaawy et al.(2021), ”Lightweight Chain for Detection of Rumors and Fake News in Social Media”, they proposed modifying the Blockchain's structure while keeping its core properties. This was accomplished by combining a custom blockchain with the Text Mining (TM) algorithm to generate a Light Weight chain that was updated (LWC). The verification process will be sped up thanks to LWC, which uses proof of good history to assign weights to nodes based on prior posts. They created a basic model to replicate the suggested LWC for detecting fake news while maintaining the standard Blockchain's properties and functionalities.Because of the widespread availability of the internet and social media in recent years, false information has travelled faster than ever before. Fake news can be more appealing than actual news in some instances. As a result, individuals become misled.

9. Cohen, K.,(2018),"Before paying with Bitcoins", The report provides a high-level summary of how blockchain technology works. It also discusses current applications of blockchain technology and possible future applications – in both the context of private transactions and public records. Finally, the report addresses some of the possible economic opportunities connected with blockchain technology as well as risks associated with both the technology and its uses. L. Liu et al.(2021)[2] proposed "Peer-to-Peer Networking and Applications" to take action against news and online curated content on the internet which could be inimical to the sovereignty of any nation, the proposed solution being implemented by smart contracts may have the capacity to identify and flag such contenton websites and social media.

EXISTING SYSTEM

Existing system runs with the help of Machine learning and natural language processing and it tries to aggregate the news and later determine whether the news is real or fake using Support Vector Machine. It has higher data set. The ML based system has centralised access to the data, and it can be easily manipulated by anyone.Because of the multi-dimensional nature of fake news, the recognizing the category of news is not so easy.The proposed strategy is completely made out of Artificial Intelligence which is basic.

PROPOSED SYSTEM

The proposed system tracks and analyzes the news that is shared, thus restricting where it is fake or user manipulated. The system also proposes a real-time alert panel that aims to find out the reality of the news by taking user's votes. The news status is constantly tracked and then eventually modified once the threshold value is reached. The fake word data set can be used to spot misleading terms and prevent the fake news.

Pros:

- Decentralized structure and Trust
- Immutability
- Transparency

FEASIBILITY STUDY

A feasibility study is a test of a system proposal according to its work ability for impact organization, to meet user needs and effective use of resources. The objective of a feasibility study is not to solve only the problem, but to acquire and sense of its scope. During the study, the problem definition is crystallized and the aspects of the problem to be included in the system are determined. After the initial investigation of the system that helped to have in-depth study of the existing system, understanding its strength and weaknesses and the requirements for the new proposed system.

Economic Feasibility:

Economic feasibility deals about the economic impact faced by the industry to implement a brand new system. The proposed system provides an efficient outcome. The whole setup is processed with ethereum based transactions. Cost per usage is least and it provides an safe digital transaction.

- It’s very economical as it doesn’t need more infrastructure.
- There is some cost for every transaction a user makes which will make it more effecient and effective.

Technical Feasibility:

Technical Feasibility centers on the existing computer system. It can support the proposed system in addition proposed system IPFS database used for easily accessibility of data, ReactJs is used for SPA(Single Page Application) and it is a user friendly application.

Social Feasibility:

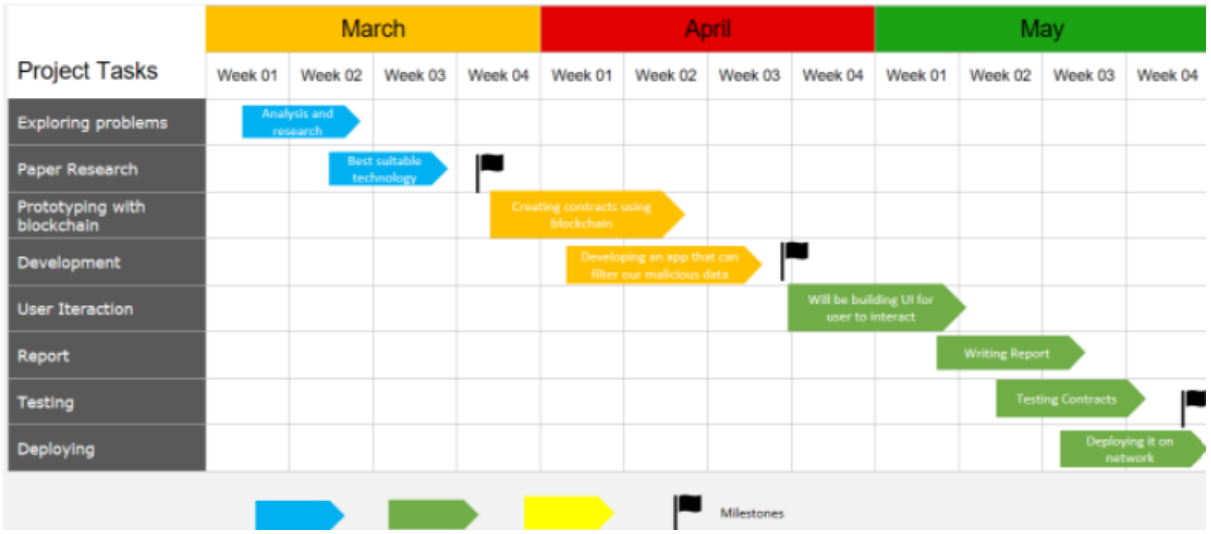
The aspect of social feasibility is to test the amount of acceptance of the system by the user. The project has software installations that are easily accessible and operational to common user. It is an asset to eradicate spread of fake data along web. It is user-friendly after a briefing on the system connections.

Market Feasibility:

The application would be free of cost for users. Prediction and estimation of the budget will be based on size, server, and project maintenance costs. A statistical analysis of the no. of consumers and participating retailers would decide the market scope of the application.

- Type of Software Project: Mobile Application.
- Software Development – a new software, involving custom development.
- Size – Medium
- Time Frame – 3 Months

Scheduling feasibility:



Hardware Specification:

- SSD :- 256GB
- RAM :- 4GB DDR-SDRAM

Software Specification:

- Operating System: 64bit operating system, x64-based processor
- VScode, Ethereum IDE, Ganache, Metamask
- JavaScript, Solidity, ReactJs, JSON

SYSTEM DESIGN

Architecture diagram:

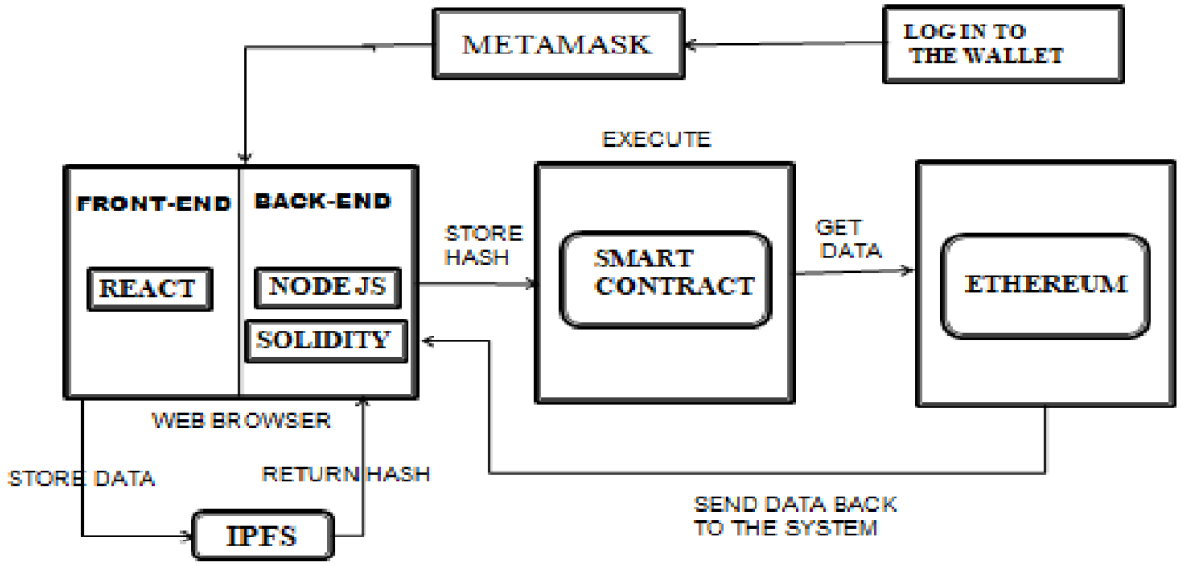


Fig 1: Architecture diagram

Given architectural diagram is pictorial representation of step-by-step procedure that we followed to receive desired output.The proposed system has a transactional architecture. It works on the block chain framework.The system uses ganache that provides counterfeit currency to be used in local host and metamask for smart contract based transactions. Ethereum is used for the transactional functioning. The front end is procured using ReactJs and the back-end is managed by solidity. Metamask is the web extension that helps in logging to the crypto wallet and it is used for getting the data and sending it back to the system.

Dataflow diagram:

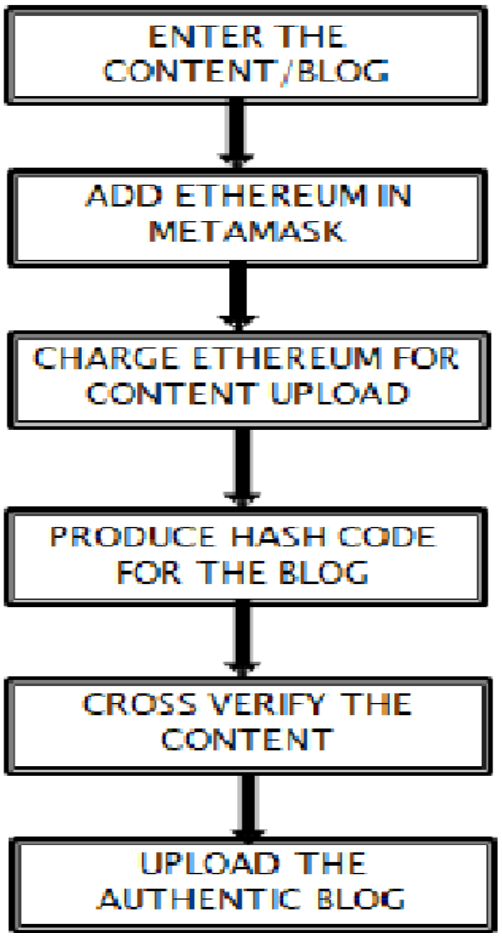


Fig 2: Dataflow diagram

This flow diagram illustrates our overall strategy for data transfer and receiving. Once the required software's are installed a block chain based application is created. Before uploading the contents that are to be published user has to sign the smart contract proceedings. Official verification is done and the contents are proportionally filtered. Once done the filtered contents are published along the platform.

Use case diagram:

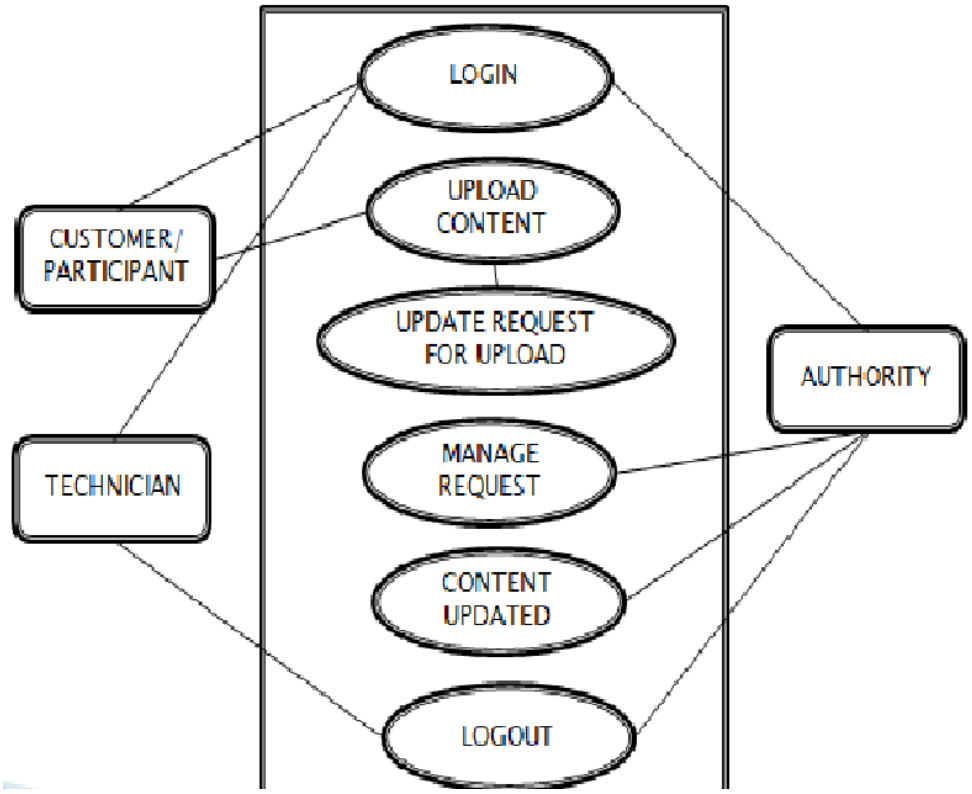
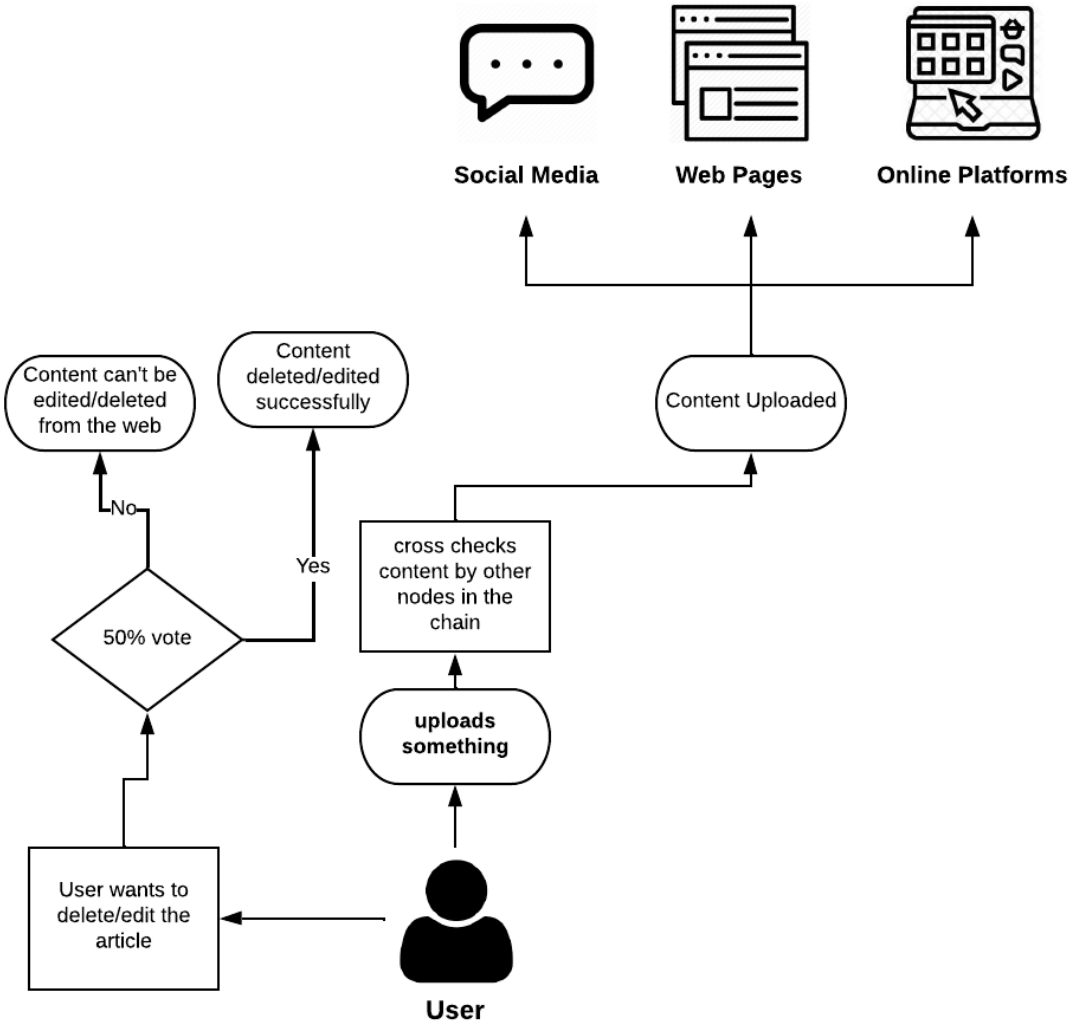


Fig 3: Use Case diagram

The project fully look into eradicating forgery data across web. When the user uploads a content into any online platforms or social media websites the system cross checks the content by other nodes in the chain.Only then its finally uploaded. Also if the user wants to delete/edit this content based o the proportional filtration the system intakes an 50 percentage vote to confirm whether the article can be altered or not.

Activity diagram:

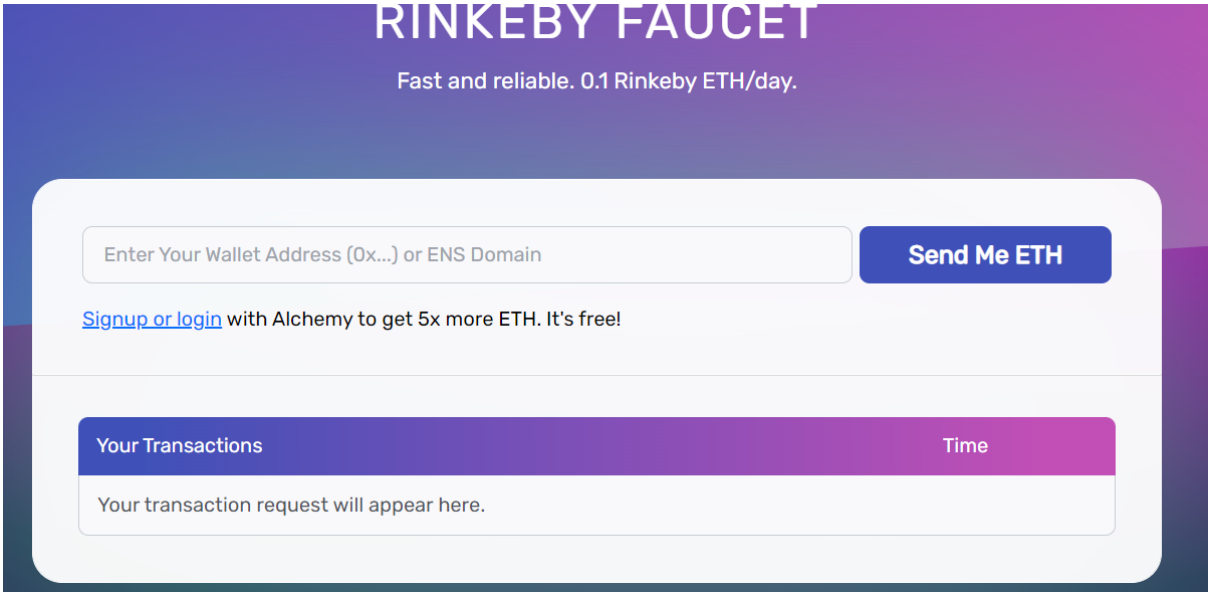


The project fully look into eradicating forgery data across web. When the user uploads a content into any online platforms or social media websites the system cross checks the content by other nodes in the chain. Only then its finally uploaded. Also if the user wants to delete/edit this content based o the proportional filtration the system intakes an 50 percentage vote to confirm whether the article can be altered or not.

MODULE DESCRIPTION

Module 1: Initializing the project and connect with rinkbey test networks

- This project have three different application which is then integrated with one another.
- Firstly, I have to install a ReactJs project then to connect with any blockchain network, I have installed contracts using hardhat(i.e. a compiler to compile smart contracts).
- Later we need IPFS file system for that I have used sanity.io.



Module 2: Planned and created the smart contract using solidity

- Here the functional and class based components are created in VS Code using solidity and define the working of respective components.
- By running this set of code, token IDs are assigned to each content that are supposed to uploaded.

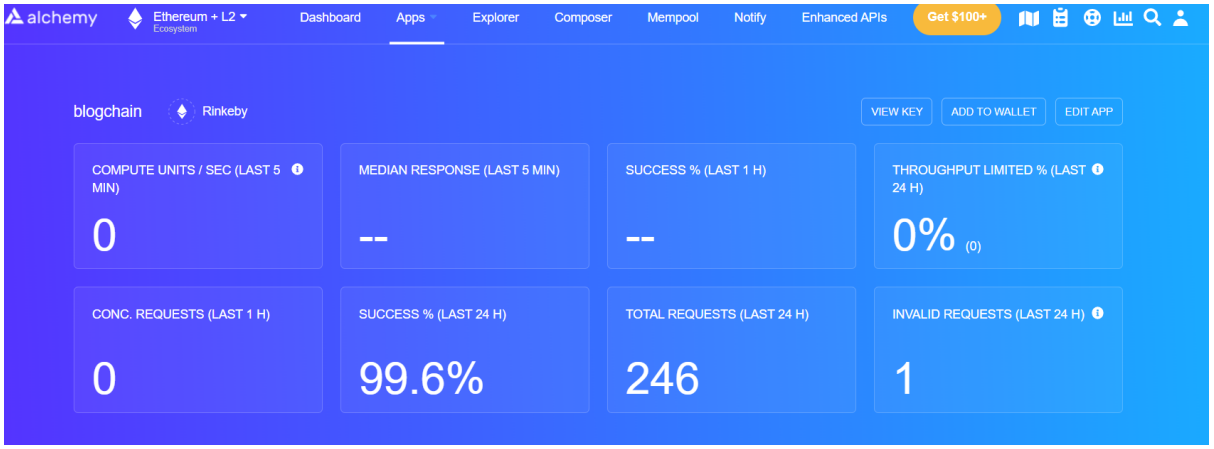
```
function _setTokenURI(uint256 tokenId, string memory _tokenURI) internal {
    _tokenURIs[tokenId] = _tokenURI;
}

function tokenURI(uint256 tokenId) public view virtual override returns (string memory) {
    require(_exists(tokenId),"URI not exist on that ID");
    string memory _RUri =  _tokenURIs[tokenId];
    return _RUri;
}

function getAlltoken() public view returns (RenderToken[] memory){
    uint256 latestId = _tokenIds.current();
    RenderToken[] memory res = new RenderToken[](latestId);
    for(uint256 i = 0; i  <= latestId ; i++){
        if(_exists(i)){
            string memory uri = tokenURI(i);
            res[i] = RenderToken(i,uri," ");
        }
    }
    return res;
}
```

Module 3: Deployment of code on ethereum network

- Each post requires ethereums network. After paying for the post, it goes through the verification.
- Adding any article will cost handsome amount, therefore many will avoid sharing fake data uselessly.Authorized and authentic posts next gets selected for getting displayed in the front-end.



Module 4: Integration of back-end and front-end

- Connect to metamask through any specified network.
- Fetch all the data from the IPFS file system \textit{i.e} Sanity database.
- Display those dynamic data on the front-end.
- Addition of data from front-end which will then pushed to the IPFS file system.

CONCLUSION

A new system is proposed to detect and avoid further spreading of fake news and validate the information from origin. The proposed systems make use of block-chain technology for verifying the source and content of the news. Using block chain makes it secure, transparent, smart and efficient as it identifies the user's malicious intent (if any) and hence prevents it from spreading fake news. It also restricts any further change in the content ones uploaded and reduces the chance to escape after creating a havoc. RTAP (Real Time Alert Panel) keeps track of the live news and constantly updates news status. Block chain based forgery data detection preserves the interest and sterility of the readers.

FUTURE ENHANCEMENT

This research looked into the current state of the block chain technology landscape. This included a general review of block chain technology as well as a more in-depth look at existing research publications and potential study fields. As a result, the goal of this project was to improve understanding of the technologies, as well as to spur further research and uncover knowledge gaps. From our perspective, the future of block chain technologies is incredibly promising, but there are issues and obstacles that must be addressed before widespread adoption. For example, 51 percent attacks, authentication, data malleability, latency, throughput, size, and bandwidth are all difficulties in security. But also in terms of personal privacy, personal data, the right to be forgotten. In its initial form, block chains are also incredibly energy inefficient. We need to use various forms of consensus and byzantine fault tolerance instead of POW. There are also issues on the developer side, as there is now no clear front runner among the various products available. There is also no agreement on the usefulness of block chains, developer support, end user support, or how they should be linked into other systems. This causes problems with chain versions, forks, numerous chains, side chains, and so forth. Finally, block chain systems rely heavily on hash puzzles and asymmetric encryption that are now available. If one of these fails, or if a flaw is revealed, the chain becomes untrustworthy and useless.

REFRENCES

1. Liqun Liu, Weihan Zhang, Cunqi Han,2021, ”A survey for the application of blockchain technology in the media”, Peer-to-Peer Networking and Applications, Issue 5, May 2021

2. P. Fraga-Lamas and T. M. Fern´andez-Caram´es, 2020, ”Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality,” in IT Professional, vol. 22, no. 2, pg no. 53-59, Issue March-April 2020.

3. S. Cho and C. Jeong, 2019, ”A blockchain for media: Survey”, 2019 International Conference onElectronics, Information, and Communication (ICEIC), Issue Jan 2019, pg no. 1-2.

4. S. E. Haddouti and M. D. Ech-Cherif El Kettani, 2019, ”Analysis of Identity ManagementSystems Using Blockchain Technology,” 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), Issue April 2019, pg no. 1-7.

5. Shilpashree B N, Rohini Krishna Mohite, Sahana S, Rajesha, Rakesh K R, 2021, “Counterfeit Detection of Documents using Blockchain”, International Journal of Engineering Research Technology,Volume 10, Issue 07 ,July 2021.

6. S. Paul, J. I. Joy, S. Sarker, A. -. A. -. H. Shakib, S. Ahmed and A. K. Das, ”Fake News Detection in Social Media using Blockchain,” 2019, 7th International Conference on Smart Computing Communications (ICSCC), pp. 1-5, September 2019.

7. M. Torky, Emad Nabil, Wael Said,2019, “Proof of Credibility: A Blockchain Approach for Detecting and Blocking Fake News in Social Networks.” International Journal of Advanced Computer Science and Applications (2019),Vol. 10, Issue No. 12.

8. Yazed Alsaawy, Ahmad Alkhodre, Nour Mahmoud Bahbouh, Adnan Abi Sen, Adnan Nadeem Al Hassan, 2021, ”Lightweight Chain for Detection of Rumors and Fake News in Social Media”,International Journal of Advanced Computer Science and Applications, August 2021.

9. Cohen, K.,2018,"Before paying with Bitcoins", Retrieved from FTC Consumer Information Theory, 22(6),644-654, June 22, 2019.

10. McKinsey & Company, 2019,"Beyond the Hype: Blockchains in Capital Markets",Corporate & Investment Banking / No 12,March 2019.