iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** I **Month of publication:** January 2023

DOI: https://doi.org/10.22214/ijraset.2023.48681

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue I Jan 2023- Available at www.ijraset.com

Blockchain and NFT-Based Decentralize Version of Social Media

Rishi Deo Rai[1], Janmaijay[2], Chintu Kumar[3], Asst. Prof. Kajol Dahiya[4]
[1, 2, 3]*Maharaja Agrasen Institute Of Technology, New Delhi*
[4]*Assitant Professor, CSE Department, Maharaja Agrasen Institute Of Technology, New Delhi*

Abstract: ***Major social media platforms are controlled by corporations, and a select few employees determine how these platforms should be used. This has prompted worries about conferee speech and censorship among users. The immediate objective of this research project is to create a decentralized social media platform which gives users more authority. Federated networks encourage independence without a centralized authority, in contrast to centralized social networking platforms. Censorship resistance, ownership of personal data, and enhanced control over user-generated content are all advantages. Furthermore, a user from his post, which will be in the format of a Non-Fungible Token (NFT), can earn by selling his NFT, which was tipped by his followers By using the latest Web 3.0 technologies like Blockchain, Smart Contracts, Solidity, React Js, Decentralize Storage System IPFS (Inter Planetary File Storage System).***
Keywords: Decentralize, Blockchain, NFT, smart contracts, Solidity, IPFS.

I. INTRODUCTION

DecentraSocial is a social media platform built on the Blockchain that was created with the express purpose of shielding users from censorship restrictions, fostering free speech, and providing the strongest possible data security for users. This social network is different from the rest because it operates on independent servers or nodes rather than existing on servers controlled by a central authority. DecentraSocial also often have tokens and NFTs that are used as new ways to monetize content. So DecentraSocial is not just a change to the infrastructure of centralized platforms but also a change to how social media companies make money.

A. Personal Data, Privacy, and Security

In Europe, the General Data Protection Regulation (GDPR) was created as a result of user concerns about having control over their personal data. Users are regarded as "data controllers" under the law. "Data processors" include social media companies. Users are the true data owners, according to the GDPR definition of a data controller.

Companies, at least those based in Europe, are required by law to give users more control over their personal data. Businesses that violate GDPR regulations suffer penalties.

Another solution to data privacy and security has been offered by DecentraSocial. Users do not need to link their accounts to physical identifiers like email addresses or phone numbers on federated social networks. Furthermore, rather than relying on a single entity to protect user data, these networks frequently use public-key cryptography for account security.

While there may be benefits in terms of data security, there are drawbacks as well. For instance, bootstrapped federated social networks may go offline due to a lack of funding, resulting in users losing their connections and data. Due to the fact that federated networks do not store records of personal data on servers, users are unable to easily reconnect with other users on the network in this situation. In terms of privacy, these platforms may not always encrypt data, which means that administrators may be able to see private messages.

B. Web 3.0

Web 3.0 has the potential to bring about a significant paradigm shift and be just as disruptive as Web 2.0. Web 3.0 is built on the fundamental principles of decentralization, openness, and increased consumer usefulness. The upcoming era in the evolution of the Internet is called Web 3.0, or Web 3.

Imagine a new kind of Internet that accurately translates what you type and understands what you say, whether through text, voice, or other media, and where all of the content you consume is more personalized than ever before. In the evolution of the Internet, you are about to enter a new era. It's been termed Web 3.0.

II. BLOCKCHAIN TECHNOLOGY

Blockchain is considered a ground-breaking disruptive technology which can change human life greatly. It is the underlying technology of Bitcoin, the first implementation of cryptocurrency. The origin design of Blockchain was first described in a self-published paper for Bitcoin by Satoshi Nakamoto in October 2008. As mentioned above, Blockchain is the basis of our proposed social networking architecture. Before presenting our architecture, it is necessary to introduce this technology.

A. Blockchain Architecture

A blockchain is a decentralized, distributed and public digital ledger on which transactions are anonymously recorded. The ledger is maintained simultaneously across a network of unrelated devices called nodes. A node can be any active electronic device, including a computer, a mobile phone or even an IoT (Internet of Things) device such as a refrigerator. A node is free to participate in or leave a blockchain network, as well as validate, synchronize and maintain a complete copy of a blockchain ledger. Nodes are equal so that there is no master or central node that manages others. The structure of a blockchain ledger is simply a chain of blocks in which transactions are recorded. Each block is connected to its previous block except the genesis block, that is, the first block of a blockchain. So, any involved transaction cannot be altered retroactively without the alteration of all subsequent blocks.

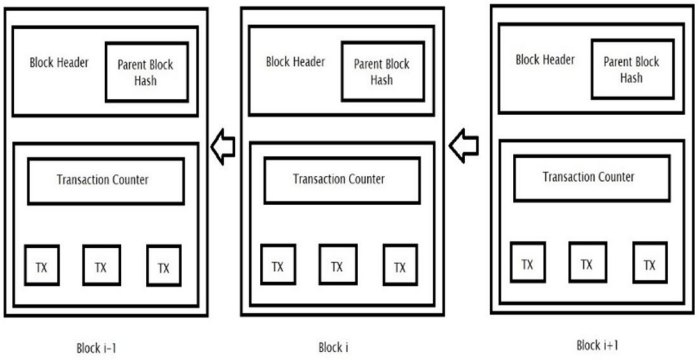


Fig. 1: Continuous Blockchain Block

Blockchain uses two key data structures:

1) *Pointers:* A variable that keeps the information about the location of another variable. Specifically, this is pointing to the position of another variable.
2) *Linked Lists:* A sequence of blocks where each block has specific data and links to the following block with the help of a pointer.

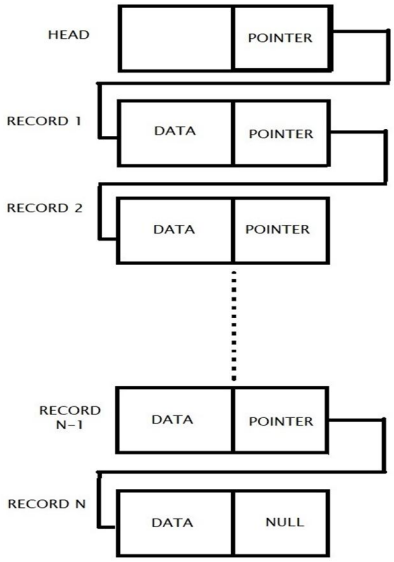


Fig. 2: Blockchain Block Diagram

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue I Jan 2023- Available at www.ijraset.com

III. NON-FUNGIBLE TOKENS (NFT)

A non-fungible token (NFT) is a consisting of digital data stored in a blockchain, a form of a distributed ledger. An NFT's ownership is documented in the Blockchain and is transferrable by the owner, enabling the trading and selling of NFTs. NFTs can be made by anyone and require little to no coding knowledge. NFTs frequently make mention of digital files like images, audio, and video. NFTs are uniquely identifiable, and they differ from cryptocurrencies, which are fungible. The market value of an NFT is associated with the digital file it references.

NFT proponents assert that NFTs give the public a public certificate of authenticity or proof of ownership, but the legal rights that an NFT conveys may not be clear. As defined by the Blockchain, an NFT's ownership has no inherent legal significance and does not automatically grant copyright, intellectual property rights, or other legal rights over the related digital file. An NFT does not prevent the creation of NFTs with identical reference files or restrict sharing and copying of the digital file that goes with it.

IV. METHODOLOGY

The smart contract of this application manages all transactions of the DApp. The user must first register once with their wallet/account address, and this user address is stored in a mapping in the smart contract. Each account in the app is linked to a single account address to avoid creating multiple accounts from the same address. This smart contract will be implemented in the Ethereum virtual machine, and the user interface will interact with the users. Thus, the whole system forms a three-tier architecture, where the UI is responsible for user interaction, while the web3 and IPFS libraries are responsible for API calls from the UI, the client interface to the Blockchain, and the IPFS storage, respectively are At the very top is the frontend UI, which is responsible for getting user input for log data, publishing data and messages, and forwarding them to the web3 library and the IPFS library. The web3 library then connects to the underlying Ethereum blockchain system for function calls, contract implementation, and fund transfers. The IPFS library is called when the user creates a post with an image or video. Images and videos are stored in IPFS data storage, and an IPFS hash is returned and stored as log data on the Blockchain. The whole system consists of three main components, namely the Ethereum backend blockchain, the IPFS storage and the frontend web UI.

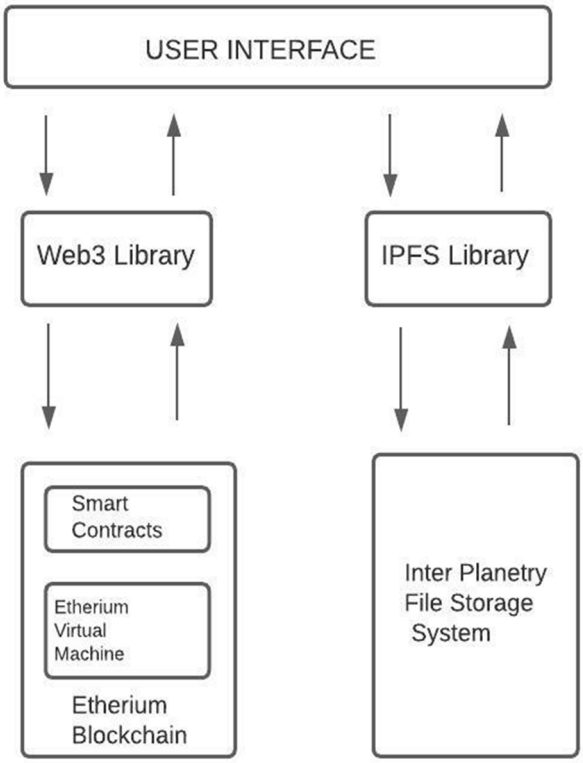


Fig. 3 Architecture of our proposed system

V. ARCHITECTURE

Fig: 3 clearly shows the architecture of our system. As with any other web application, our platform also works like a normal website, but the backend of our system is entirely different from what has been used traditionally. The front end and the user interface of our system are built using the React framework of JavaScript. The React framework makes it easy to build a web application very quickly and conveniently. So the front end of our system is built by following the normal web-development methods. But once we go deep into our system, our middleware and the backend are totally different from any traditional web application. The API we are using in our system is a JavaScript web 3.0 framework called Truffle. This framework helps in communicating with a blockchain like Ethereum or Solanum. Truffle framework is a great help to working with the Ethereum blockchain. It makes the deployment of smart contracts, the main functional unit of our system, easier. Using this framework in our system, we deploy two smart contracts that help in carrying out two important functions of our application. On the Ethereum blockchain, transactions are facilitated by smart contracts. Every Blockchain has a common digital ledger that is updated every time a transaction is made there. It's possible to say that smart contracts assist developers in carrying out transactions and adding them to the leger. The hash of the image that has been stored in IPFS is stored by one of our smart contracts. And the other help in tipping crypto coin to the content creators. The user's metamask wallet sends cryptocurrency to the content creator's wallet via this smart contract. Interplanetary File System is used to actually store the data (IPFs). A central server is not required for the operation of the peer-to-peer file-sharing protocol known as IPFS. The content-addressed storage (CAS) method is used by the web-based IPFS network to store and retrieve data based on its content rather than its physical location. IPFS employs this method to specifically identify and retrieve the requested data. Data is broken up into smaller bits, scrambled, and given a unique content identifier (CID), which serves as a fingerprint when it is uploaded to an active protocol node. Because of this, storing small amounts of data on the network is quicker and simpler.

Once the data is published to the network, other nodes in the network update their nodes to include a cached copy of the data. Similar to how the initial node did, they can also provide data. It is up to a node to decide whether to keep and keep providing this data or to discard it, for example, to conserve memory. Each fresh time data is uploaded to the network or data that has already been uploaded, a new cryptographic hash (CID) is generated, making each upload distinct and impervious to security breaches or tampering. The lengthy CID string is used by IPFS's decentralized naming mechanism to determine the file's name, which is then transformed into a more readable DNS name using DNSLink. A hash is returned after the data has been published to the IPFS by the system. The smart contracts are then used to store this hash in the Blockchain. We are storing the data in an entirely secure and uncompromisable manner by doing this. The security of the data is greatly enhanced by this. Like other social media platforms, there is no organization that owns the data here. As a result, no one uses the stored data to violate someone's privacy in the name of offering more convenient services.

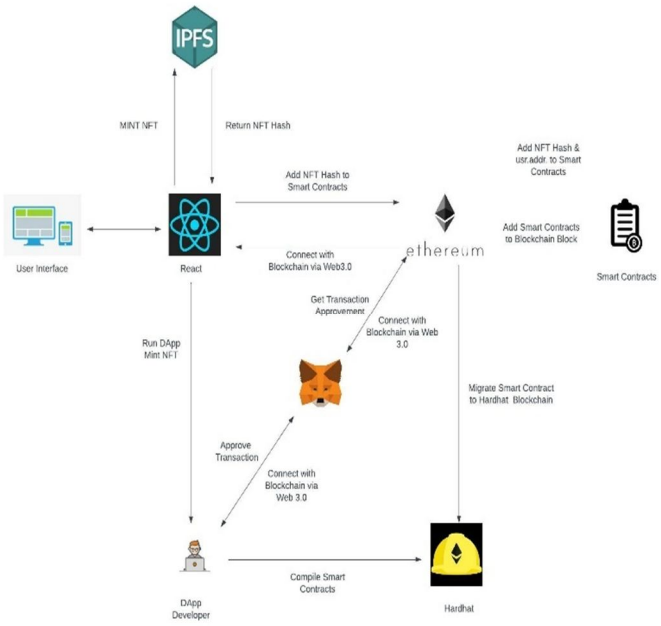


Fig. 4: Working Architecture

VI. MODULE DESCRIPTION

A. Frontend Module

Our system's front end is a website built with the React framework. The user can decide which image to use and want to upload along with a description. The user can view both their own post and other users' posts in the newsfeed. The post's popularity and the number of tips are used to order it in the newsfeed. By leaving an Ethereum tip for the author of their favourite work, the user can show their appreciation. The user can tip by clicking the tip button on the bottom right of each post.

B. Storage Module (IPFS)

We have to use MetaMask to access our website. Our social media platform allows users to upload images and descriptions. After uploading, here comes the backend of this site. When a user clicks upload, an API call will be called by this code through JavaScript. constipfsClient = require('ipfs-http-client') constipfs=ipfsClient({host:'ipfs.infura.io',port:5001,protocol: 'https'}) We use Infura.io to store the image via IPFS. They are like third-party providers for an IPFS client. They will manage everything related to the IPFS. The Infura.io IPFS client provider will give us the hash of the image that the user uploads to social media (Dapp).

C. Smart Contract to Upload Image

Our social media (Dapp) will use smart contracts to link or attach an image hash returned by infura.io to the block in the Blockchain. Then the smart contract will return a transaction request to the user to pay a gas fee (ETH) for uploading an image to social media. If the user process transaction successfully, their ETH will be transferred to the smart contract address & the photo will be uploaded. Finally, anyone who visits our social media will be able to see the uploaded image in the newsfeed. If the user didn't process the transaction successfully, the image of the hash would not be linked to the block in the Blockchain. Whether the user processes a transaction successfully or not, the uploaded image of the hash will be stored in the infura.io ipfsClient

D. Smart Contract for Transferring Crypto

To provide an incentive to the content creators, we use a tipping system where another user can donate cryptocurrency to the creator of their favourite post. To tip 0.0001ETH to the creator, the user can click the Tip button on the bottom right of each post. Now, the system calls the smart contract, and the smart contract returns a transaction request to the user. When a transaction is "done," it refers to the transfer of 0.001 ETH from the tipper's wallet to the creator of the content via a smart contract

VII. CONCLUSION

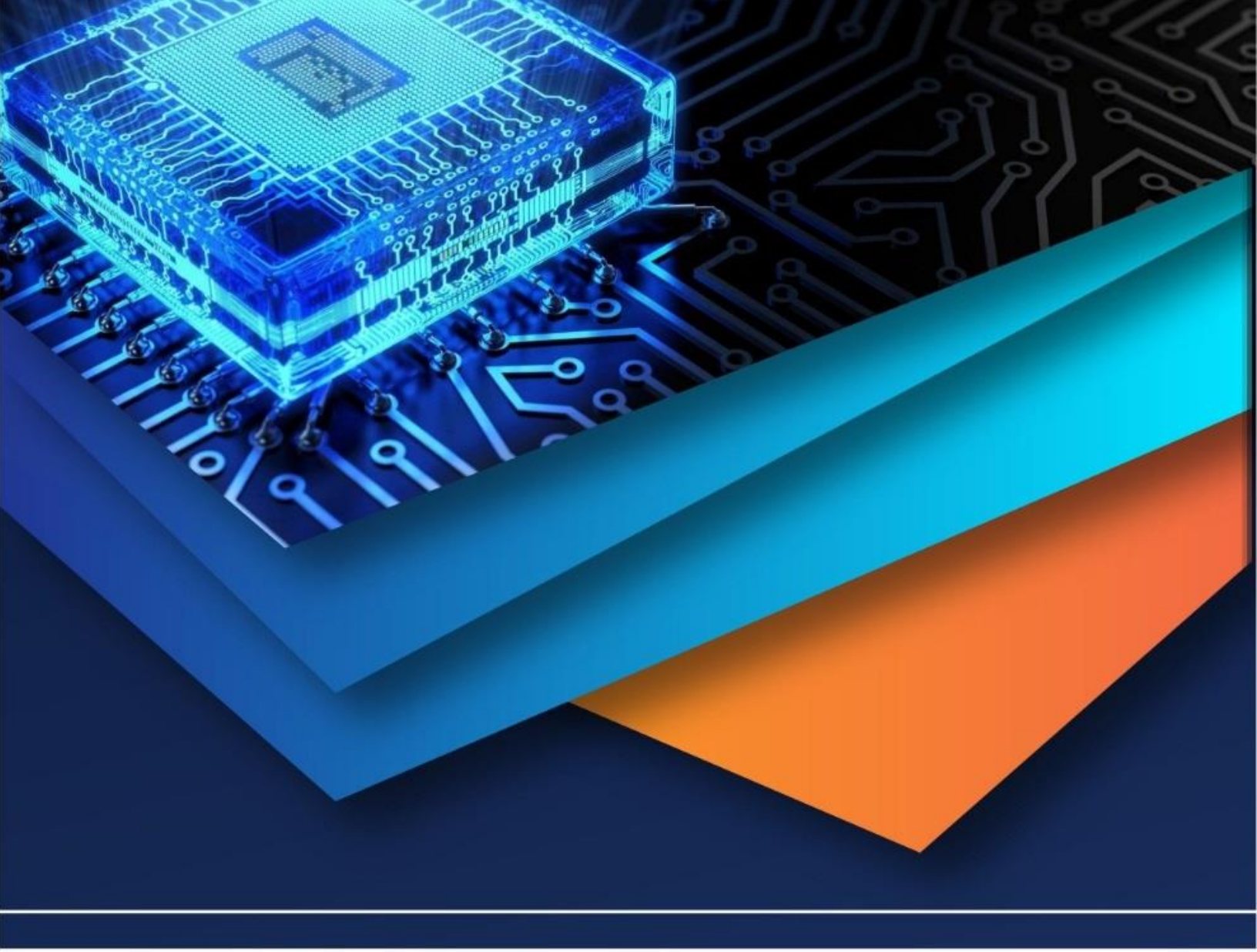
Before competing with tech giants like Facebook, Twitter, or Instagram, decentralized social media platforms still have a long way to go. However, due to the freedom and security offered, people are learning about and becoming more receptive to the concept of decentralized social networks combined with the potential of Blockchain. Many people are drawn in particular by the simple earning potential and schemes offered by participating in a decentralized, rewards-based social network.

VIII. ACKNOWLEDGEMENT

We sincerely thank our college Maharaja Agrasen Institute of Technology, for giving us a platform to prepare a project on the topic "DecentraSocial and would like to thank our HOD, Dr Namita Gupta, for giving us the opportunity and time to conduct research on the subject. We are sincerely grateful to Prof. Kajol Dahiya (CSE Department) as our guide for providing help during our research, which would have seemed difficult without their motivation, constant support, and valuable suggestion. Moreover, the complication of this research paper would have been impossible without the cooperation, suggestion, and help of our friends and family.

REFERENCES

[1] Hrishikesh Bawane1, Tanuja Shinde2, Abhishek Kadam3, Yash Budukh4, Prof. Pooja Mundhe5.Ethegram - An Ethereum and IPFS-based Decentralized Social Network System.2020
[2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Consulted, 1(2012):28, 2008
[3] Jon Evans. Bitcoin 2.0: Sidechains and ethereum and zerocash.2014.
[4] Lanier, Who owns the future?. London: Penguin Books, 2014, pp. 32-66
[5] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System (white paper)", 2014.
[6] F. Ehrsam, "The dApp Developer Stack: The Blockchain Industry Barometer", Medium, 2017. [Online]. Available: https://medium.com/ @FEhrsam/the-dapp-developer-stack-the-blockchain-industrybarometer8d55ec1c7d4.
[7] M. Qamar, M. Malik, S. Batool, S. Mehmood, A. W. Malik, and A. Rahman, “Centralized to decentralized social networks: Factors that matter,” pp. 37–54, 2016.
[8] YUAN Yong and WANG Fei-Yue, Blockchain: The State of the Art and Future Trends, ActaAutomaticaSinica, vol. 42, no.4, pp.481-494, April, 2016



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY