BLOCK CHAIN BASED DECENTRALISED TWITTER DAPP

Valeti Deepika, 2D. Lalitha Bhaskari
1M.Tech Student, Department of Information Technology,
2Professor, Department of Computer Science and Systems Engineering,
Andhra University College of Engineering (A), Andhra University, Visakhapatnam, AP, India.

Abstract:

The block chain is an innovative technology which opened doors to new applications for solving numerous problems in distributed environments. In this work, we design a block chain based data storage and access framework Twitter application to remove its total dependence on a centralized repository. We use the public block chain and tools like Ganache, Metamask, Truffle and Ethereum IDE for deploying the contracts. In the proposed work, metadata of the files are stored on the block chain and we use the networks like Ropsten and Rinkebey for occurring the Transactions using a peer-to-peer networks. This will provide decentralized storage, distributed processing, and efficient lookup capabilities.

Key Terms—Public block chain, Distributed ledger Technology, Decentralized system.

1) INTRODUCTION

The block chain is a peer-to-peer distributed ledger in which records called blocks are linked and secured using a cryptographic hash. By design, block chains are decentralized, secure, immutable and extremely fault tolerance making them suitable for record management activities i.e., financial transactions, identity management, provenance and authentication. Block chain can be deployed as permissionless (e.g., Bitcoin or Ethereum) or permissioned blockchain e.g., Hyperledger Project by The Linux Foundation. In permissionless or public block chain the actors in the system are not known. Anyone can join or leave the block chain network at any time, which may raise security risks in the network. However, in permissioned or private blockchain only known and identifiable set of participants are explicitly admitted to the blockchain network. This reduces the presence of malicious actors within the network. As a result, only authenticated and authorized actors can participate in the network which increases the security of the system as required by the enterprise applications. The interesting non-financial areas that leverage the opportunities of permissioned blockchains include health, government services, supply chain management, Internet of Things, peer-to-peer cloud storage and many more. The P2P cloud storage is an interesting application of blockchain as it provides a decentralized data storage facility without involving any trusted third party or a clientserver architecture. The decentralized data storage will help to eliminate the most traditional data failures and outages by increasing the security, privacy, and control of the data.

2) RELATED WORK:

Blockchains are write-only data structures with no administrative permissions for editing or deleting of the data. The data structures are known as blocks and are distributed in a P2P network. Each block contains the cryptographic hash function of the previous block and is used to develop a link between them. The linked blocks form a complete chain, hence the term blockchain. The hash function maintains the security, integrity, and immutability of the blockchain.

Figure 1: Block Chain structure
i) Transactions & Blocks: The record of an event, cryptographically secured with a digital signature, that is verified, ordered, and bundled together into blocks, form the transactions in the blockchain. Thus, each block is composed of transaction data along with the timestamp, cryptographic hash of the previous block (parent block) and a nonce. A nonce is a random number or bit string which is used to verify the hash. The hash values are unique and help to maintain the integrity of the entire block chain from the first block (genesis block) to the last in the network.

ii) Smart Contracts: They are the computer programs that run automatically when certain criteria are met within the system. They are used to transfer value of any kind between the peers in a blockchain without the service of the trusted third party [18]. Today, the Ethereum smart contracts are designed to run on all nodes of the Ethereum network. Similarly, Hyperledger Fabric5 smart contracts are called chaincode. They enable the user to create transactions in the shared ledger of the network.

iii) Ethereum: It is a decentralized open source block chain featuring smart contract functionality. Ether is the native cryptocurrency token of Ethereum platform. It is the second largest cryptocurrency behind Bitcoin. Ethereum provides a decentralised virtual machine called as EVM, which can execute scripts using an international network of public nodes.

iv) Solidity: It is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various block chain platforms mostly in Ethereum. Solidity is compiled to byte code that is executable on the EVM.

3) PROPOSED WORK

Decentralized Twitter Dapp is an application where the users can create accounts on twitter and able to add the tweets, delete the tweets and able to send the messages from one account to another. As Block chain is decentralized technology and occur all the transactions with the help of ethers, we use networks like Ropsten and Rinkebey with ethers for occurring each and every transactions. In this paper, we used tools like Ethereum IDE, truffle and Ganache and Metamask for deploying the contracts.

Methodology:

In this paper, deployed the smart contract using Linux operating system. The tool named as Truffle is used for deploying the smart contract in Ubuntu (Debian) OS. The project we proposed is more secured compared to normal twitter app. Decentralised application which provides more security and integrity. Only the authorized users can create accounts in Twitter and can able to send messages from one account to another account and also able to add and delete tweets. Ethers are main tokens used to perform each and every transactions in the Block Chain. Gas is the computational unit used in Ethereum for occurring the transactions. Compilation and migrations of smart contracts is the first step for deploying the contracts.
From the above figure, it is clear that TweetBook smart contract is deployed using the Ropsten network. The network id for Ropsten is 3 and it has certain gas limit.

From the above figure, it is clear that the contract has been deployed and contract address for TweetBook has been generated.
Metamask is the tool used to connect the smart contract with the particular network whether to confirm that the transactions should occur with this network or not.

![Image of Metamask connecting contract with network]

From the figure it is confirmed that TweetBook smartcontract has been connected with Ropsten Network. Through this network we can perform all functions which are include in smart contract with the cryptocurrency called Ethers.

Account is created within the Ropsten network / Rinkebey network to perform the transactions according to the smart contract. Each and every account state has four components:

- **Nonce**: Number of transactions sent through the particular account from the contract address which has been generated while deploying the contract.
- **Balance**: Number of Ethers that particular contract address contain. It can be in the form of Ethers/Wei.
- **Code Hash**: Initially the hash value is 0. After occurring the transaction, the details of that transaction is stored in the form of hash in tree like structure.
- **Storage root**: Each and every hash value is stored in tree structure called as Merkle Tree. The root of the tree is used to check from which block the data has been stored.
4) RESULTS

After deploying the contract need to run that particular smart contract with the help of lite-server having the local host as 3000. The contract runs and it opens in the browser and are able to perform the functions like creating an account in twitter, adding and deleting the tweets, sending messages from one account to another account.

![Creating account](image1)

![Sending messages](image2)

Figure 1: Creating account

Figure 2: Sending messages
Figure 3: Adding Tweets

Figure 4: Deleting Tweets
5) CONCLUSION AND FUTURE WORK:

In this work block chain based decentralized twitter application has been implemented which provides more integrity and security compared to the traditional application. The proposed frame work eliminates the need for centralized repository. This approach decentralizes the Twitter framework and removes the project dependence upon centralized computing resources for storing, processing and uptime. This block chain based decentralized technology can also be implemented to other social media applications like Facebook, Whatsapp and LinkedIn etc. This, in turn, will help in improving the performance monitoring of the Internet needed to maintain the quality-of-service required for present day and future technologies of the Internet.

REFERENCES: