Study of Decentralized Application for File Sharing on Blockchain

Prof. Dr. S.D. Joshi[1], Yash Chaubey[2], Hritvik Dadhich[3], Ishan Srivastava[4]
[1,2,3,4]*Department of Computer Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune*

Abstract **- In a scrutinizing bunch, data sharing is an essential step to gain maximum knowledge from the prior work. Existing data sharing platforms depend on trusted third party (TTP). Due to the involvement of TTP, such systems lack trust, transparency, security, and immutability. To overcome these issues, this paper proposed a blockchain-based secure data sharing platform by leveraging the benefits of interplanetary file system (IPFS). A Meta data is uploaded to IPFS server by owner and then divided into n secret shares. The proposed scheme achieves security and access control by executing the access roles written in smart contract by owner. Users are first authenticated through RSA signatures and then submit the requested amount as a price of digital content. After the successful delivery of data, the user is encouraged to register the reviews about data. These reviews are validated through Watson analyzer to filter out the fake reviews. The customers registering valid reviews are given incentives. In this way, maximum reviews are submitted against every file. To implement the proposed scenario, smart contracts are written in solidity and deployed on local Ethereum test network. The proposed scheme achieves transparency, security, access control, authenticity of owner, and quality of data.**

Index Terms **- — blockchain; IPFS; AES; RSA; TTP; SSS; Ethereum; smart contracts.**

I.INTRODUCTION

Data storage essentially means that files and documents are recorded digitally and saved in a storage system for future use. Storage systems may rely on electromagnetic, optical, or other media to preserve and restore the data if needed. Data storage can occur on physical hard drives, disk drives, USB drives, or virtually in the cloud.

Data storage is necessary for keeping a record of our data in case of loss of data. And in today's hectic and fast-growing technological world everyone has this facility to keep a record of their data which is nowadays a basic need.

There is a huge amount of data right now in this world. So data needs to be stored somewhere and as mentioned above data could be stored on Physical drives like hard disk, floppy drive, pen drive, different kind of USB'S but most importantly as technology is growing data is preferably stored on the cloud which is a more convenient option for people. Storing data on the cloud reduces the burden of carrying physical drives. Cloud storage is like data is gathered and stored over a single place from where we can access the data whenever we want to access that data because it's all in one place.

Actually, we are surrounded by data in today's world and everything we search or download is in the form of data. It is the data that helps us find everything we look for on Google or YouTube. Not only these but in everyday life, there is a lot of data like in the medical field, in hotels, restaurants, showrooms, and big IT firms. Data is everywhere. That's how important is data in the world we are living in.

The decentralized storage system is the Answer to the problems which we face using Centralized storage system. It is being used in the industry at a very good scale nowadays field like medical, IT companies and Vehicle manufacturing companies, etc.

A decentralized storage system allows users to store their files (and sensitive information) without relying on massive data centers, such as those run by Amazon and other cloud storage providers. An element of sharding was involved too, as files were often broken down into chunks.

Not just that it also ensures that if a server goes down, the information it stored often goes with it. But through decentralization, a file can be broken into little pieces and scattered across nodes — meaning that

there's always a backup plan if one of them goes offline.
Decentralized storage can also make it harder for malicious actors to take pieces of web content down. Instead of centralized file storage, which means there may only be one destination to target, an attacker could have thousands of nodes to contend with — making a denial- of- service attack prohibitive and close to impossible. This could also make it harder for countries around the world to restrict information to their citizens by blocking news websites and online portals such as Wikipedia. Decentralized storage ensures that security and safety.

II. RELATED WORK

Blockchain-Based Access Control Scheme for Secure Shared Personal Health Records.
Blockchain technology provides a tremendous opportunity to transform current personal health record (PHR) systems into a decentralized network infrastructure. However, such technology possesses some drawbacks, such as issues in privacy and storage capacity. Given its transparency and decentralized features, medical data are visible to everyone on the network and are inappropriate for certain medical applications. By contrast, storing vast medical data, such as patient medical history, laboratory tests, X-rays, and MRIs, significantly affects the repository storage of blockchain. This study bridges the gap between PHRs and blockchain technology by offloading the vast medical data into the InterPlanetary File System (IPFS) storage and establishing an enforced cryptographic authorization and access control scheme for outsourced encrypted medical data. The access control scheme is constructed on the basis of the new lightweight cryptographic concept named smart contract-based attribute-based searchable encryption.

Reliable Vehicle Data Storage Using Blockchain and IPFS
As the importance of vehicle data increases, it has become very important to safely store them. However, because onboard diagnostics scanners generally used to store vehicle data are IoT devices, security and capacity issues exist to store data safely and efficiently. To address this, we propose a system that stores vehicle data safely and efficiently using blockchain and IPFS. Users can access the system through DApp, an Ethereum- distributed application, and manage their vehicle data. Various experiments have been conducted to demonstrate the superior performance of this system, and the experimental results show its advantages in terms of data-processing speed and cost.

III. DECENTRALIZED APP SYSTEM MODEL

The system model has the following entities.
Owner: It may be a person or organization which owns the data to be shared among customers. It can also control the query and access of data by filtering out the requestors.
Customer: Makes a Request for buying the data from the system. After receiving the desired content, the customer downloads the file from IPFS server by reconstructing the hash and registers his reviews about data on the review system.
Workers: It is the passive entity of system, provides decryption services on behalf of the customers. Authenticates the new customers through signatures and query the smart contract for requested data by customers.
Arbitrator: A trusted entity is responsible for solving disputes between the buyer and seller regarding the downloading of requested content. Based on the decision of arbitrator, a customer may be refunded the deposited amount.

IV. MODEL WORKING

This Decentralized model is bind up of major three functionalities and are as follows:

DATA SHARING
Before everything, the owner initiates the digital datasharing by way of generating the metadata of the original file. Metadata could include facts including the name of the file, type, description, and size. Once the metadata is prepared, its miles uploaded to the ipfs alongside a complete file of data. The snippet of file uploading to ipfs is given next.

```
//upload the plain file meta
 ipfs . files . add ( buf , function ( err , meta _ result ) {
if ( err ) {
console . log ( err ) ;
return res . send Status ( 500 ) ; }
```

```
Console. log ( meta _ result ) ;
res . json ( { " meta_hash " : meta _ resul t [ 0 ] . hash
, " file _ hash " : fileMeta . hash ,
 "address " : recipient _ addr ,
 "email " : recipient _ email } ) ;
 } :
```

Once the file is uploaded to IPFS, hashes of that data are generated by IPFS and returned back to the owner. When the owner receives the hash, SSS algorithm is used to split the IPFS hash of file into k number of shares. In response to these shares, owner decides the n number of random keys to be used for encryption. Once all the shares are encrypted, they are stored in the blockchain along with other important information such as; authorized recipient for the file.

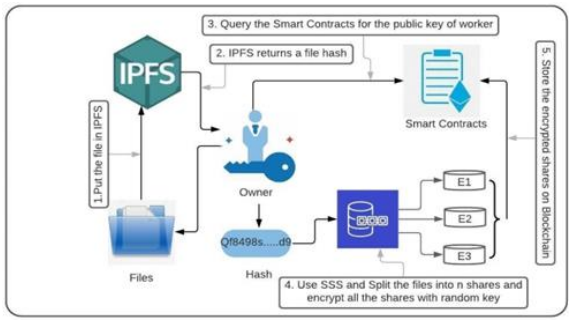


Fig 1: Data Sharing on IPFS by owner

DATA RETRIVAL

A detailed system model for customers asking for the digital content is shown in figure shown below Purchaser-first examines the existing review of data by using previous clients so that the best data can be nicely verified before depositing the ethers.

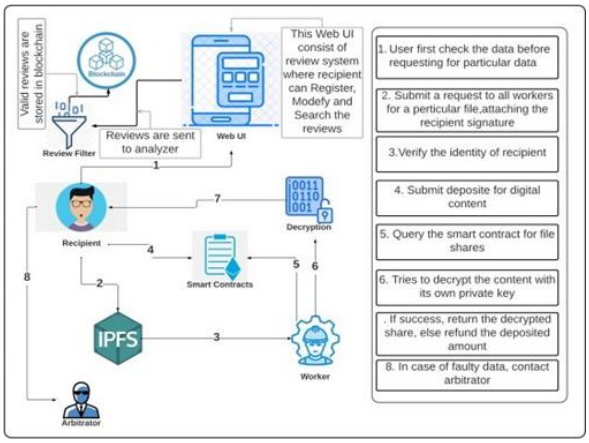


Fig 2: Data request by recipient

Data review system:- For data trading between owner and customer, a reputation system is available to update data being traded. Note that reviews, ratings and reputations are used differently in this work. First, the review system provides ratings or scores provided to customers, who already use the data. Based on these updates, new customers can check the quality, reliability, and integrity of the data. The consistency of the review is verified using the blockchain because the data disrupts the evidence in the blockchain. After looking at the ratings, the new customer decides whether the data should be purchased or not. After that, a request is sent to the workers for specific details according to the review. Once the customer is satisfied with the updates, the request is sent to the workers to get the desired digital content.

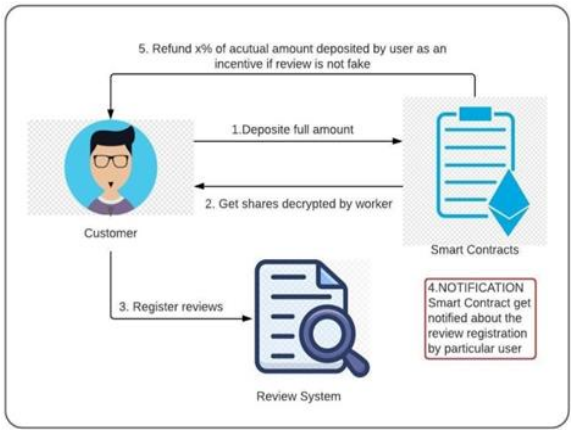


Fig 3: Incentive for user registration review

SMART CONTRACT DESIGN

Three special variables are most commonly used in this paper:

Msg.sender: Message or transaction sender (current call). The contract address associated with the content creator, whenever a contract is entered into.

Msg.value: Wei value associated with the message, cost per dollar ($) when number of wei fixed. One ether is equal to 10^18 wei.

Tx.origin: Accounts call for a smart contract.

IPFS STORAGE CONTRACT: -

This contract provides the following services:

addFile: The owner or contractor can do this work. The event begins when a new file is uploaded to the IPFS server, which returns the IPFS hash to the owner and is stored in a smart contract. Uploaded content is requested only by a valid applicant other than those, which are blacklisted by the owner.

//Add f i l e function addFile (bytes32 id , bool is Visible)

```
public { require ( ! b l a c k l i s t [msg. sender ]
&&FileMap [ id ] . timestamp == 0 ) ;
.emitconfirmFileIndexID(F i l e L i s t . length −1, id);}
```

deletefile: This operation is performed only when the owner wishes to delete a specific file from the server. When file deletion is required, reference and address issues are referred to this function.

```
// File deletion
function deleteFile( uint index , bytes32 id , address [
] memory addr ) public {
File List [index] = 0;
emit confirmFileDeletion ( index , id ) ;
 }
```

setRecipient: When data requested by a user, it is searched and mapped to the application. If the information you want is available, then the list of recipients is kept by a smart contract to distribute digital content.

```
//Search content function setRecipients( bytes32 id ,
bytes32 [ ] memory newShares ) public {
 for( uint  j  =0; j<addr . length ;      j ++)
{
FileMap[ id ] . recipients [ addr [ j ] ]=value ;
 }
 }
```

V. MODEL WORKING

SMART CONTRACT

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met.

There are many benefits of using smart contracts such as Speed, efficiency and accuracy. Once a condition is met, the contract is executed immediately. Because smart contracts are digital and automated, there's no paperwork to process and no time spent reconciling errors that often result from manually filling in documents. Trust and transparency because there's no third party involved. From Security point of view Blockchain transaction records are encrypted, which makes them very hard to hack.

DAPPS(DECENTRALIZED APPLICATION)

A Dapps has its backend code running on a localized peer-to-peer network. Distinction this with an app wherever the backend code is running on centralized servers. A Dapps will have frontend code and user interfaces written in any language (just like an app) that may buildcalls to its backend. Moreover, its frontend is hosted on localized storage like IPFS. A decentralized application (Dapps) is an application designed on a localized network that mixes a smart contract and a frontend program. Dapps will run on a P2P network or a blockchain network.

DApps can run on a P2P network or a blockchain network. For example, BitTorrent, Tor and Popcorn Time are applications that run on computers that are part of a P2P network, whereby multiple participants are consuming content, feeding or seeding content, or simultaneously performing both functions

ETHEREUM

Ethereum is a blockchain platform with its very own Cryptocurrency, referred to as ether (eth) or Ethereum, and its very own programming language, known as solidity. As a blockchain community, Ethereum is a decentralized public ledger for verifying and recording transactions. The community's customers can create, put up, monetize, and use programs on the platform, and use its ether Cryptocurrency as payment. Insiders call the decentralized applications at the community "dapps".

IPFS(INTERPLANETARY FILE SYSTEM)

The Interplanetary File system (ipfs) is a protocol and peer-to-peer community for storing and sharing records in a distributed report file system. Ipfs makes use of content material-addressing to uniquely identify every document in an international namespace connecting all computing devices.

Ipfs permits users to host and obtain content material in a way just like bit torrent. As opposed to a centrally placed server IPFS is built around a decentralized system of user-operators who hold a portion of the overall data, growing a resilient device or report storage and sharing. Any user in the network can serve a file via its content material address, and different peers in the network can find and request that content material from any node that has it using a distributed hash table (DHT).

The gain of ipfs is that users in a neighborhood network can communicate with every other, although

the huge region network is blocked for some reason. Considering that no servers are required, creators can distribute their paintings without any cost. Information masses quicker as it has higher bandwidth. To sum up, it in all fairness safe to say that ipfs offers a sustainable technique to the prevailing challenges in web. With its censorship resistance, high pace, information security, and a resilient backbone for a network. Ipfs is absolutely a progressive "key" to every problem inside the net today.

VI. RESULT

After Succesfully Deploying Our Smart Contract in real-time we observed data sharing and storing done through the decentralization as shown in the figure below:

Functions	Transaction Gas	Execution Gas	Actual Cost (ether)
Contract creation	1,808,235	1,338,219	0.00361647
Add file	67,512	53,948	0.000107896
Delete file	29,206	19,034	0.000058412
Set receipient	34,098	30,231	0.000060462
Set blacklist	31,290	14,203	0.000028402

Table 1: Smart contract cost test (IPFS storage: gas price = 2 Gwei), 1 ether = 150 USD

Functions	Transaction Gas	Execution Gas	Actual Cost (ether)
Contract Creation	1,723,531	1,277,355	0.003447062
Customer Payment	70,190	47,510	0.00014038
Download Results	30,373	30,412	0.000060746
Confirm flle Server Results	54,428	76,930	0.000108856

Table 2: Smart contract cost test (Proof of delivery: gas price = 2 Gwei), 1 ether = 150 USD.

To add a review system to a data sharing environment, a separate smart contract is entered into. The user needs to set up an account, stealing user ID to view updates about the data. To register for new updates, the sign up button must be clicked by the user to fill in fields such as Metadata, comments, and ratings. In the same way, updates can be searched by a new user by clicking the search button and adding a query.

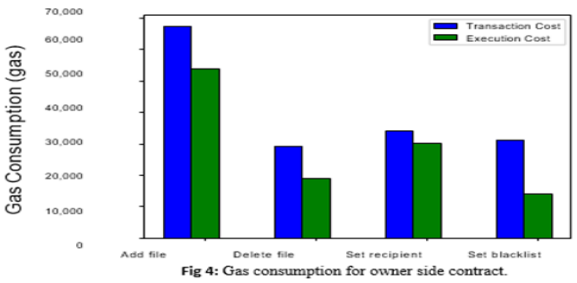


Fig 4: Gas consumption for owner side contract.

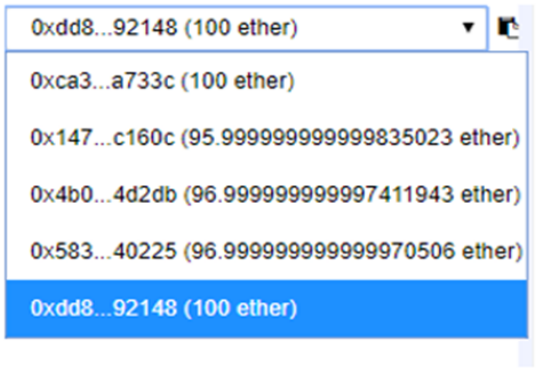


Fig 5: Money deposit from recipient.

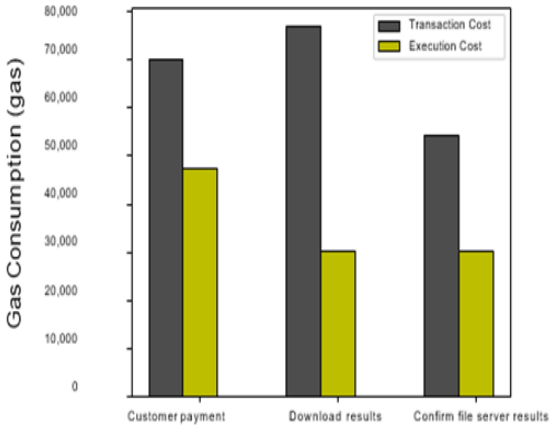


Fig 6: Gas consumption for recipient side contract.

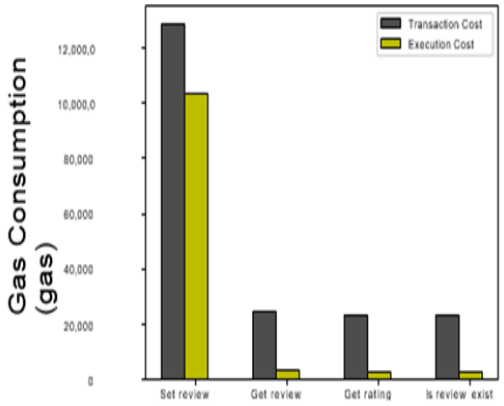
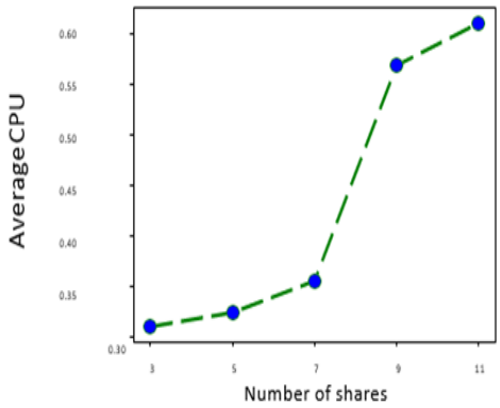


Fig 7: Gas consumption for review system.

It is clear from the graph that as the number of shares increases, the average CPU timegreatly increased. In this system, when k = n, the shares are generated by whose polynomial promotion of qualifications with all the extra k in the system. The highest calculation time is labeled as 0.66 ms where k is equal to 11 shares and 0.32 ms is the lowest calculation time when the number k is 3.



SSS is used in our case to separate and encrypt hashes of file uploaded to IPFS Comparison between two encryption schemes, namely, advanced encryption standard (AES) 128 and AES 256.

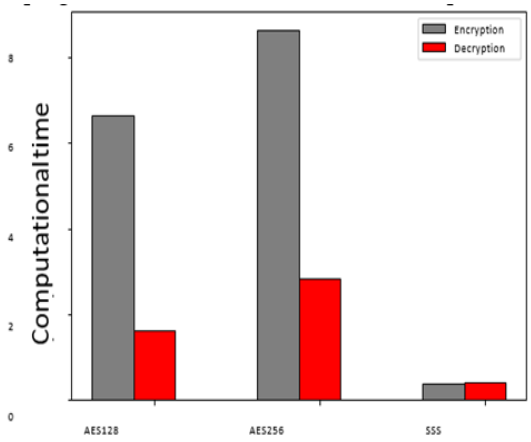


Fig 8: Computational time for different encryption schemes.

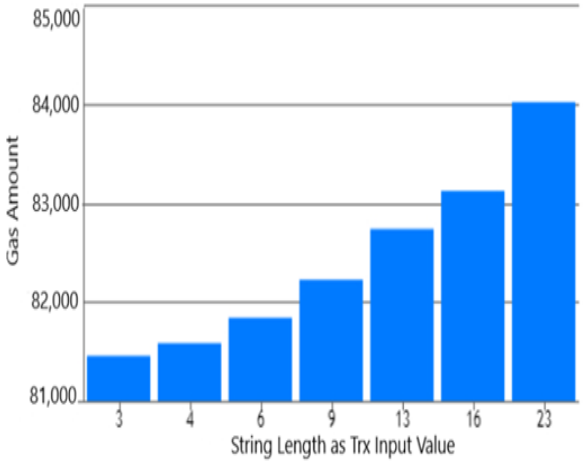


Fig 9: Change of amount of gas consumed with different input lengths of transactions

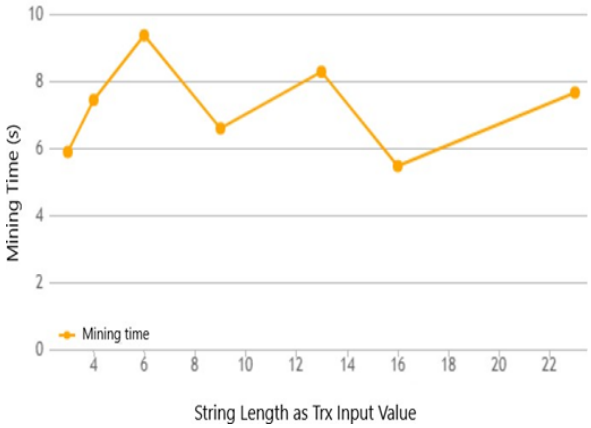


Fig 10:Change of mining time with different input lengths of transactions

VII. CONCLUSION

In this project, a blockchain-based secure data sharing and delivery of digital assets framework is presented. The main aim of this proposed scenario is to provide data authenticity and quality of data to customer as well as a stable business platform for owner. A decentralized storage IPFS provides the solution for bloating problem at owner's end. Data hashes returned by the IPFS are encrypted using SSS, so that a customer who has not deposited digital content price, cannot access the data. In this way, owner is satisfied from any type of hash leakage to unauthorized customer. Data authenticity is ensured by adding a review based system, where customers can record their comments and rating about the data. In this way, new customers can judge the quality of data, therefore money can be saved at customer's end. Different smart contracts are designed for various purposes; such as, owner smart contract for uploading the file on IPFS and encrypting the hashes. The other smart contract is for user side. A user can access the file hashes from smart contact after authentication from worker nodes. Finally, the review system smart contract can help new and old customers to search and register reviews. Simulation results are performed for gas consumption and cost analysis of these smart contracts. Each function consumes different gas value depending upon the logics and complexity of operations being performed in each function.

REFERENCES

[1] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitco.in/pdf/ bitcoin.pdf(accessed on 6 April 2019).
[2] Shamir, A. How to share a secret. Commun. ACM 1979, 22, 612–613.
[3] Li, J.; Wang, X.; Huang, Z.; Wang, L.; Xiang, Y. Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing. J. Parallel Distrib. Comput. 2019, 130, 91–97.
[4] Fukumitsu, M.; Hasegawa, S.; Iwazaki, J.; Sakai, M.; Takahashi, D. A proposal of a secure P2P-type storage scheme by using the secret sharing and the blockchain. In Proceedings of the 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), Taipei, Taiwan, 27–29 March 2017; pp. 803–810.
[5] Guo, R.; Shi, H.; Zhao, Q.; Zheng, D. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access 2018, 6, 11676–11686.
[6] Assets. Arab. J. Sci. Eng. 2019, 44, 3849–3866.
[7] Hasan, H.R.; Salah, K. Proof of delivery of digital assets using blockchain and smart contracts. IEEE Access 2018, 6, 65439–65448.
[8] Chen, Y.; Li, H.; Li, K.; Zhang, J. An improved P2P file system scheme based on IPFS and Blockchain. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11– 14 December 2017; pp. 2652–2657.
[9] Park, J.S.; Youn, T.Y.; Kim, H.B.; Rhee, K.H.; Shin, S.U. Smart contract- based review system for an IoT data marketplace. Sensors 2018, 18, 3577.
[10] Truffle Suite. Available online: Https://truffleframework.com/tutorials/configuring-visual-studio-code (accessed on 23 April 2019).
[11] Truffle Suite. Available online: Https://truffleframework.com/docs/ganache/overview (accessed on 23 April 2019).
[12] MetaMask. Available online: https://metamask.io/(accessed on 23 April 2019).
[13] Reliable Vehicle Data Storage Using Blockchain and IPFS by (Ms. Hyoeun Ye and Prof. Sejin Park) 9292/10/10/1130/htmhttps://www.mdpi.com/2079-
[14] Know Your Customer (KYC) Implementation with Smart Contracts on a Privacy-Oriented Decentralized Architecture by (Mr. Kapsoulis, A. Psychas, Georgios Palaiokrassas, Achilleas Marinakis, AntoniosLitke, Theodora Varvarigou)https://www.mdpi.com/1999-5903/12/2/41/htm
[15] Blockchain-Based Access Control Scheme for Secure Shared Personal Health Records over Decentralised Storage (Mr. Hassan Mansur Hussien, Dr.Sharifah Yasin, NurIzuraUdzir, MohdIzuan Hafez Ninggal) https://www.mdpi.com/1424-8220/21/7/2462/htm
[16] Decentralizing Supply Chain Anti-Counterfeiting and Traceability Systems Using Blockchain Technology (Mr. Neo C.K. Yiu)https://www.mdpi.com/1999-5903/13/4/84/htm