International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 6, December 2020, pp. 6399~6411
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i6.pp6399-6411

A decentralized consensus application using blockchain ecosystem

Chetana Pujari, Balachandra Muniyal, Chandrakala C. B.
Department of Information and Communication Technology, Manipal Institute of Technology,
Manipal Academy of Higher Education, India

Article Info

Article history:

Received Aug 3, 2019
Revised May 9, 2020
Accepted May 27, 2020

Keywords:

Blockchain
Consensus
DApp
Ethereum
Security

ABSTRACT

The consensus is a critical operation of any decision-making process. It involves a set of eligible members; whose decision need to be honored by taking their acknowledgment before making any decision. The traditional consensus process follows centralized architecture, the members need to rely on and trust this architecture. The proposed system aims to develop a secure decentralized consensus application in the untrusted environment by making use of blockchain technology along with smart contract and interplanetary file system (IPFS).

Corresponding Author:

Chandrakala C. B.,
Department of Information and Communication Technology,
Manipal Institute of Technology, Manipal Academy of Higher Education (MAHE),
Manipal, Karnataka, India.
Email: chandrakala.cb@manipal.edu

1. INTRODUCTION

A decision-making system is designed to make decision based on the consensus from the eligible participants as per the rules/regulations. An example of a decision system is a voter system used during the election, where the eligible participant can cast vote to the candidate of their choice and the one with the majority of the vote is declared as a winner. The same mechanism is used to take a consensus when a new rules and regulations are proposed in any industry or organization.

The simple decision-making system is designed by adapting a client-server architecture, and most of the data processing and storage are handled at the server-side. Due to this centralized architecture, the current decision-making system suffers from following limitations:

- Availability: As the data is managed at the centralized server, if the server goes down. The data will no longer be available to support decision making.
- Integrity: Due to centralized storage there is a possibility that the data can be manipulated by one who owns the centralized server.
- Data Provenance: Lack of trust in tamper-resistant in data provenance is one of the concerns.

To address these issues a decentralized application can be designed on top of the blockchain technology. It follows a peer to peer architecture, hence instead of storing the data in a centralized server, the data is stored at every node in the network and the data is secured cryptographically. In this model, the important properties of any decentralized applications are:

- Authority: Due to its distributed storage, the issues concerned with centralized authority can be avoided.
- Availability: Availability of the data is ensured even if one of the nodes fails to operate.
- Integrity: The hashing concept used to store transactions, ensures data integrity.

- Conflict Resolve: Secure data provenance is ensured using a cryptographical concept, which helps to resolve conflicts in a short time.

The proposed work aims to build a decentralized consensus application using a blockchain ecosystem, where the users are identified based on their login credentials and account address, each transaction is secured by encrypting them using the private key. The data is stored in the smart contract storage which ensures data integrity and provenance. The front end/ client-side application is hosted in the IPFS network. The proposed work addresses the issues identified in current decision-making systems. The data availability is guaranteed by making use of a decentralized network, where each node in the networks maintains a copy of the data. The user is authenticated by his account number and login credentials. The data confidentiality is ensured by using public-key cryptosystem and finally, the data integrity is ensured by using a hashing algorithm. The paper is organized as follows. Section 2 presents an overview of blockchain technology and its ecosystem. In section 3, the problem with an emphasis on objectives, research gap and rationale are described. Section 4 gives the methodology for the realization of a decentralized application for consensus. The result section gives an insight into the outcomes. The conclusion section concludes the paper.

2. BLOCKCHAIN

2.1. Blockchain overview

Blockchain is a secure distributed ledger technology. It consists of transactions, grouped to form blocks. These blocks are linked cryptographically, hence, it is called blockchain. The blockchain is distributed to every node in the peer to peer blockchain network. The blockchain technology, therefore, ensures decentralized and tamper resistance behavior [1].

2.1.1. Why blockchain?

As most of the developing countries have started a movement from cash to cashless and going digitized, the secure micropayment, online transaction, and secure digital communication are essential factors to consider. Currently, distributed systems are used for digital communication. They are prone to issues like data integrity, data confidentiality, data provenance and lack of ownership [2-4]. The blockchain technology can be used to address issues related to data confidentiality, integrity, and non-repudiation.

Banks and financial organizations are governed by central or federal authorities. The rules imposed on transactions, such as transaction fees and transaction limit changes with share market and government policies, hence, there is a need to navigate to a decentralized system like blockchain wherein people involved in a system can make a contract and validate every transaction by taking a consensus from every other member in the system.

Frauds and hacking related to confidential data like internet banking, credit/debit card data, health records, data generated by monitoring systems like video surveillance, electronic appliance usage data and sensor data are challenges for any digital and IoT based applications. Using blockchain with applied cryptography, most of the above-mentioned challenges can be addressed to some extent.

2.1.2. Blockchain usecase

Blockchain can be used in a variety of applications like cryptocurrency, cloud service, land registration, voting system, law enforcement and IoT based applications [5, 6]. Let's consider the usecase of the land registration application. The application must identify the user and authenticate them before selling or buying the land. It must also ensure, secure record management, verify and validate the uploaded documents. Blockchain ecosystem can be used to address these requirements by providing an interface to upload documents related to user identity and land details, enable tracking transactions and verifying documents. Blockchain ecosystem also ensures the protection against land-fraud and record tampering [7].

2.1.3. Building blocks of a blockchain

The three building blocks of a blockchain are shown in the Figure 1.

- Encryption and cryptography: These ensure security services such as authentication, authorization, non-repudiation and confidentiality [8, 9].
- Consensus mechanisms: These are the algorithms used to decide, whether, a new block of validated transactions should be added to the chain or rejected.
- Timestamp and hashing of the previous block: These ensure data integrity. The blockchain structure helps to track back to a specific transaction, due to consistent and immutable data provenance.

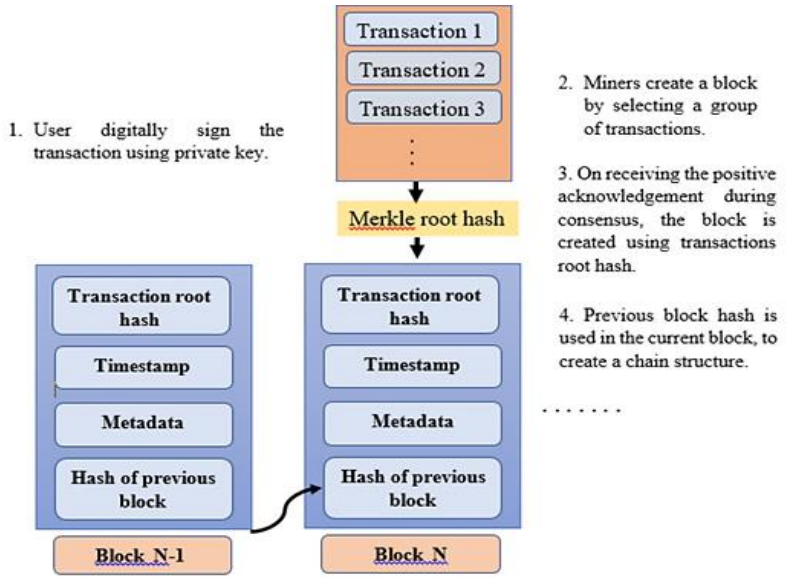

Figure 1. Blockchain building blocks

2.1.4. Blockchain working

Blockchain technology uses a linked list data structure as shown in Figure 2. Transactions are validated by the participant nodes in the blockchain [10]. A group of the valid transactions is stored in a block and confidentiality is maintained by hashing each block. Each block stores the hash generated by the previous block to form a chain of blocks which resembles a linked list structure. Every block maintains a ledger of a valid transaction. If any hacker tries to tamper the data, it affects the hash value significantly. Adding a new block to chain requires a consensus from every other node in the chain hence ensuring validation of each block [11].

The two major roles of any participants in the blockchain are discussed below:

- Initiate transaction: In order to have active blockchain or to initiate a blockchain, the participant must initiate a transaction. The transaction is then verified by other participants in the blockchain network.
- Participant can play the role of miners and can do a task like verifying and broadcasting transaction competing to add a block, broadcasting a new block and confirming the transaction.

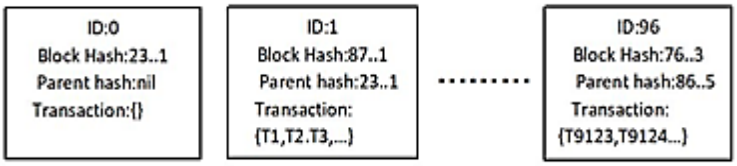

Figure 2. Blockchain example

Blockchain technology is divided into private and public blockchains.

- Private Blockchain: It is also known as a permissioned blockchain, here one needs to have permission to perform read, write and update operation. The distributed property of blockchain is with respect to the ledger.
- Public Blockchain: Anybody can participate in a public blockchain as it is public. It does not deal with access management and anybody can be part of the consensus. Validation is done by the nodes connected to the network.

2.2. Consensus mechanism

The consensus mechanism is the decision making process through which any new valid or verified block is added to the blockchain, which in turn improves the trust level. The two most prominent consensus mechanism is proof of work and proof of stake.

- Proof of work: In this mechanism, any new transaction in the blockchain network is broadcasted to every other node in the network via gossip protocol. The miner nodes select a group of the transactions to form a block. All the selected transactions are verified and are hashed along with the nonce. This hashing process is repeated for the different nonce until the difficulty is met. Once the block is created it is broadcasted to every other node. The block is then verified at each node using the given nonce. The miner who creates the block and receives a positive consensus from other nodes will be rewarded and the miner's block is added to the network [12]. If two miners create a block at the same time, both blocks will be added to the network forming two branches of the chain, based on where the next block is added the additional block is discarded. This proof of work consensus mechanism is currently used in bitcoin, Ethereum, and many other blockchain platforms.
- Proof of stake: In proof of work mechanism, huge computation power is required to create a block that satisfies the difficulty level, and also the miner with the highest computation power is generally the winner. To overcome this problem a new mechanism called proof of stake came into existence. In this mechanism, the miners are known as validators, and they need to deposit some coin as a stake in the network. The validators are selected in some pseudorandom order. Once selected the validator has to verify the transactions and create a block. This block is then broadcasted to other nodes who then verify the block created and send a positive consensus for the valid block [12].

3. RELATED WORKS

The following research review is done to understand the existing approaches used in decision making, and some papers are studied to know the importance of blockchain technology and its decentralized applications. Supeno et al., [13] have proposed a design for a secure electronic voting system. SHA-256 hashing and the RSA algorithm are used in the proposed design to ensure data security and integrity. All the data collected are stored in the centralized server, hence if the server goes down, the data would not be available. The data is maintained by the centralized authority; hence its reliability and trustworthiness are a matter of concern. These issues can be overcome by using blockchain technology.

Shahzad et al., [14] have proposed a framework for the electronic voting application using blockchain technology. Blockchain technology is used to ensure data security, verifiability, and privacy, due to its irreversible, distributed ledger property. In the proposed system SHA-256 hashing used is the only security aspect considered to safeguard business logic. Including a smart contract, which has business logic in it can provide better security. Kshetri et al., [15] have discussed, how blockchain can be used to ensure tamper resistant votes. Blockchain platform also ensures that the data is stored accurately, permanently and transparently. As the blockchain technology is still in the development stage, technology immaturity is the only matter of concern.

Irham et al., [16] have proposed an e-voting system, based on hashing and public key infrastructure. In this system, the key generation process depends on a central authority. In the voting process, the central authority needs to encrypt the ballot with the corresponding public key of each voter, who then need to decrypt the ballot to cast vote. The proposed system depends on central authority at every stage of the voting process, using blockchain's distributed ledger property and the smart contract a better solution can be provided.

Hao et al., [17] have proposed an end to end verifiable classroom voting system, without any intermediate tallying authority. Fiat Shamir transformation and DRE-i protocol are used to ensure concealing, revealing and self tallying property in the system. The security of the system can be further improved by managing the identity of the voter. Abou et al., [18] have discussed the applications of blockchain in a different domain. This work helps to understand the prominent features of blockchain like privacy, immutable, decentralized and confidentiality. It also assists in comprehending how these features can be used to provide a solution to the various business problem in today's world.

Yining et al., [19] have proposed a payment scheme, using the Ethereum blockchain platform. The scheme aims to ensure reliable service over the unreliable network. Blockchain's distributed ledger feature guarantees distributed verification. The smart contract includes business logic for service management. As in Ethereum, smart contracts are treated as a transaction, its security is ensured.

Kumar et al., [20] have recommended a method, using a modified RSA algorithm to provide data security. The main focus of this method was to ensure data confidentiality but using blockchain technology, we can ensure both the confidentiality of data but also data integrity. Adamu et al., [21] have proposed a framework for securing an electronic medical record system. This work involves comparing different PHP frameworks with respect to its security features. The web application for the electronic medical records was developed, using Lravel PHP framework. The focus of this work was on user authentication. The IPFS, together with blockchain technology can improve the security requirement of the application.

3.1. Research gaps

In the literature survey, existing approaches used for decision making, and the importance of blockchain are discussed. Based on which, the following research gaps are identified, which needs further investigation:

- Identity management in the decision-making application.
- Securing the business logic, which includes rules and constraints to be used in decision making.
- The trustworthiness of transactions in decentralized decision-making applications.
- Void Type: Theory application void is observed in the literature survey.

3.2. Problem statement

Research shows that ensuring the trustworthiness of the data and identity management are the key requirements of any decision-making process. Blockchain technology powered with IPFS ensures the availability and reliability of any data [12, 22]. This work undertakes a descriptive study to understand the Ethereum blockchain ecosystem. The problem identified in this work is to develop a decentralized application for decision making using the blockchain ecosystem. Transactions in the application, must adhere to rules and constraints defined as a business logic. Following are the research questions identified for the given problem.

- How to secure the data from tampering?
- How to ensure the security of the business logic?
- How to ensure identity management in the decentralized application?
- What are the activities involved in formulating Consensus application?

3.3. Objective and rationale

- Objective: Develop a secure decentralized consensus application using the Ethereum blockchain ecosystem.
- Rationale: Data tampering and identity management are a major concern for any application used for decision making. The proposed work aims to overcome the above discussed issues by developing a decentralized application, where user can rely on the trustworthiness of the data and business logic. Which, in turn, helps to build the trust on the consensus mechanism used.

4. RESEARCH METHOD

The overall description of the methodology that is followed for development of the decentralized consensus application is discussed in this section.

4.1. Decentralized consensus application architecture

The Figure 3 represents, the architecture diagram for decentralized consensus application proposed. The client-side application, i.e, the front end is built using HTML, CSS, and Javascript and is hosted in the distributed network using IPFS. At the backend, Ethereum blockchain network is used to ensure distributed server architecture, wherein each node in the blockchain network maintain the copy of the ledger and smart contract. In the proposed work, Ganache is used which provides us with 10 test accounts and a private key for each account. The business logic of consensus application is written in a smart contract using solidity language. As a smart contract, once deployed cannot be changed, hence test cases are written using solidity/ javascript language to test smart contract before deploying. In order to ensure proper organization of the application and it's smooth working a truffle framework is used, which ensures proper structuring of the proposed work along with the facility to compile, migrate, test and deploy the smart contract. Once a smart contract is built, the generated JSON object is used by the web3 object, to ensurea smooth interaction between the blockchain node and the client-side application. Finally, the Metamask is used as an add-on for the browser which acts as an interface between the web application and the blockchain node.

The Figure 4 depicts, the overall use-case diagram for a consensus application. The consensus application consists of two actors requester and responder. The requester is the one who once authenticated can add suggestion and can view the suggestion status. On the other hand, the responder can view the request list and give a response, i.e, the authenticated responder can accept or reject the suggestion.

The Figure 5 represents, the flowchart for consensus application. In this application, once the requester adds the suggestion, the requester is authenticated. If the requester is an invalid user, a custom message is displayed, whereas, for the valid requester, the suggestion added is broadcasted to all the responders in the network. On receiving the request the responder can accept or reject the suggestion. Once all the responders give their consensus, the suggestion is accepted or rejected based on the condition that, if the count of acceptance is greater than the count of rejection, then the suggestion is accepted else it is rejected.

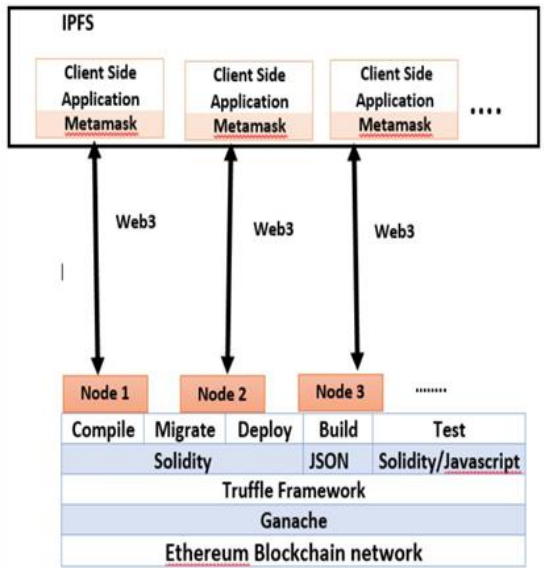

Figure 3. Decentralized consensus application architecture

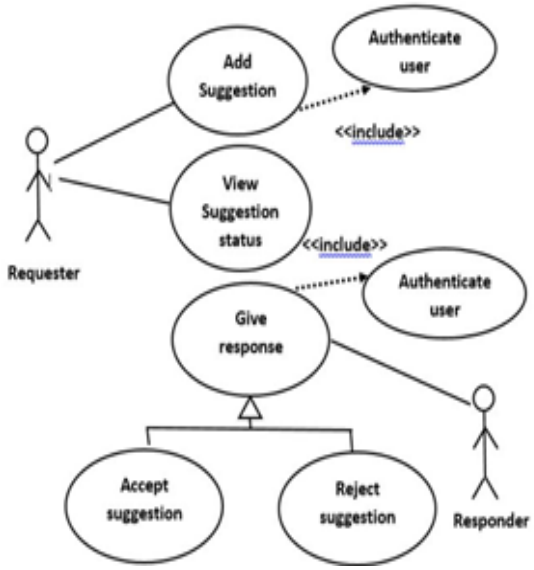

Figure 4. Usecase diagram for consensus application

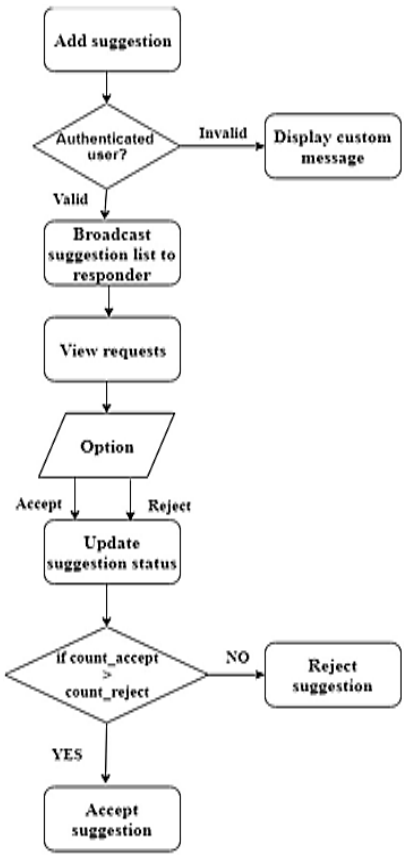

Figure 5. Flowchart for consensus application

The Algorithm 1, depicts the flow of events during the decision-making process. Once the blockchain ecosystem is set up, The member is authenticated using the credentials and his/her ethereum account is verified. On successful authentication, the member can post his suggestion and the decision is made based on the response of other members involved in decision making.

Algorithm 1 Consensus Application

```
Require: Ethereum account, blockchain ecosystem
Ensure: Authentication, confidentiality and data integrity
 1: Host client application in IPFS network
 2: if memberName = = username AND memberPassword = = password then
 3:   if validEthereumAccountANDbalance > transactionFees then
 4:     if choice is newsuggestion then
 5:       addSuggestion
 6:     else {choice is viewDecision}
 7:       if rejectCount ≥ acceptCount then
 8:         RejectDecision
 9:       else
10:         AcceptDecision
11:       end if
12:     end if
13:  end if
14: end if
```

4.2. Implementation details

The blockchain ecosystem used with an emphasis on different tools/utilities/technologies for the development of proposed application is described in the following subsections.

4.2.1. Blockchain ecosystem used

The Fgure 6, represents the overview of the peer to peer blockchain network, where each node act as a peer at the server-side. The client application can communicate with the ethereum server using the web3 library.

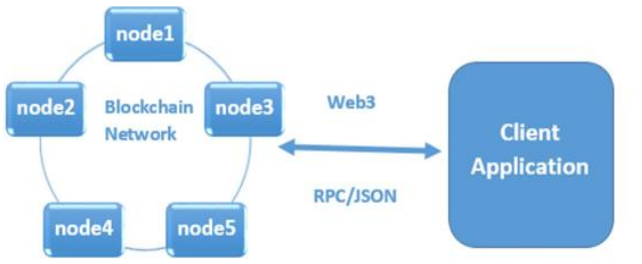

Figure 6. Decentralized application architecture

a. Ethereum

Ethereum is the open source, distributed blockchain protocol. It provides Ethereum Virtual Environment also called EVM. EVM enables us to compile and deploy the smart contract to the blockchain. Ethereum is a protocol used to develop a decentralized application with the power of smart contracts. Currently, Etherum uses proof of work for consensus [12].

b. Solidity

Solidity is the object-oriented programming language used exclusively to write a smart contract for Ethereum. It is the combination of javascript and java language. Solidity enables us to write rules, constraint, and business logic into the smart contract. The smart contract serves as an agreement among different stakeholders and once it's deployed into the blockchain, all the nodes in the blockchain network adhere to the smart contract. The remix is the most popular IDE used to write a smart contract. It enables to execute a smart contract in the test environment and also to deploy it in the blockchain networks [12]. Figure 7 depicts the remix interface. The left side is the project explorer. The center area is to write solidity program and the area at the right side contains options to compile, execute and deploy a smart contract.

c. Truffle

Truffle is the framework used to develop a decentralized application based on Ethereum platform. It provides the environment for compiling, testing and deploying a smart contract. It also provides an interface to link the smart contract with external web, mobile or a console based application. Figure 8 depicts the truffle structure. All the smart contracts to be used in the application will be stored in the contract folder, where the contracts are written using solidity language. Once the smart contract is compiled, the generated JSON file will be stored in the build folder. The migration folder consists of Migration.sol file, which consists

of all necessary artifacts to deploy the smart contract. Before the smart contract is actually deployed, it is first tested using test cases specific to the contract and the test cases are written in .js or .sol language. These test cases are stored in the test folder, and finally, all files related to front end application like HTML, CSS or js files are stored in the src folder. Using truffle framework enables a developer to follow a systematic approach while developing a decentralized application [12].

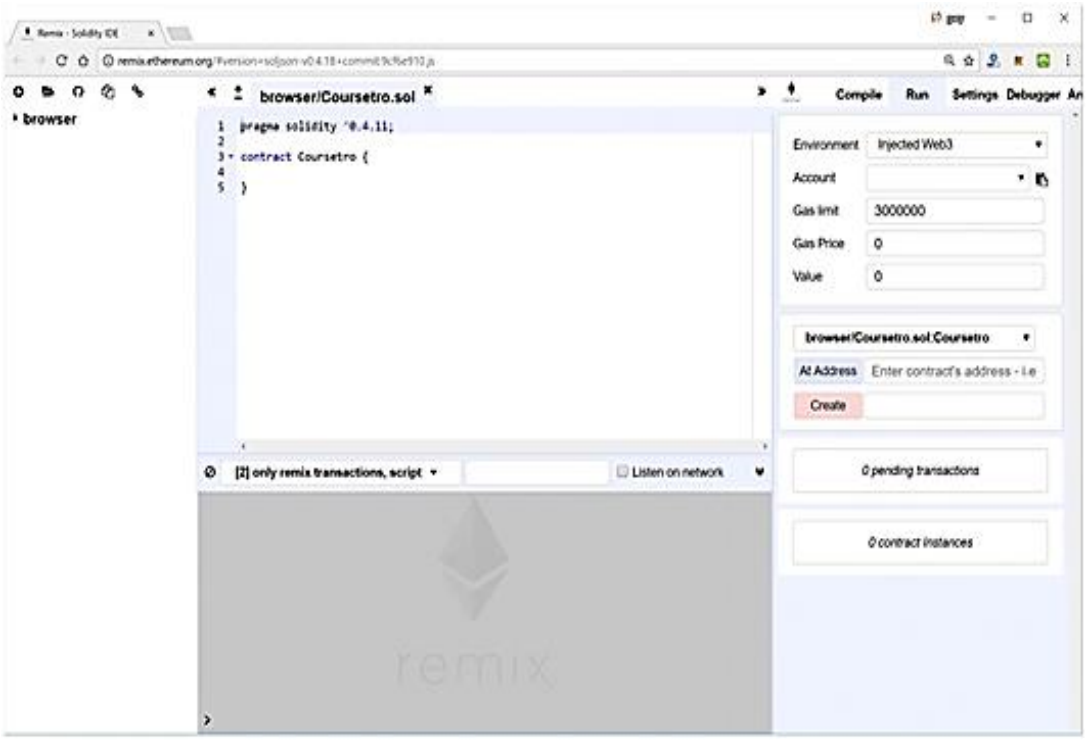

Figure 7. Remix IDE

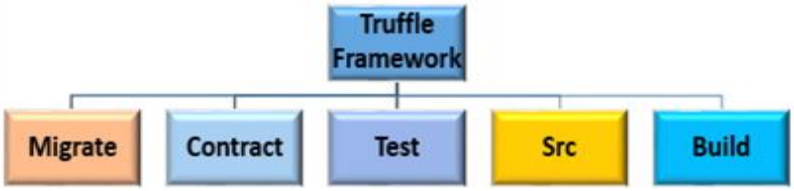

Figure 8. Truffle structure

d. Ganache

Ganache is the test Ethereum blockchain which provides 10 test Ehereum accounts with a private key and each account with the balance of 100 ether to start with. Ganache enables a developer to test the smart contract by deploying it to the test blockchain. Ganache is GUI based, hence developer can view when the smart contract is deployed and transactions are executed. Once the application is tested successfully in the local test blockchain, it can then be deployed to the actual network [12].

e. Decentralized application (DApp)

It is similar to the traditional application to some extent but it is tamper resistant and more trustworthy. Just like a traditional web application, the DApp also has a front but instead of the centralized backend in DApp the nodes in a distributed blockchain network are used as backend. The interaction between the front and the backend is enabled using powerful web3 features [12, 22, 23]. Figure 6 depicts the overall architecture of decentralized application.

f. IPFS

A centralized system usually managed by a single company, hence the user has to depend on this company to gain access to the data. To avoid this dependency one can use interplanetary file system (IPFS). IPFS helps to make the web application completely distributed. It works similar to bit torrent. IPFS uses content-based addressing instead of location-based addressing. In content-based addressing, a user just needs to specify what content is required whereas, in location-based addressing, the user needs to specify the IP address or the domain address from where the content is to be downloaded. In IPFS, hashing is used to address the content hence ensure a tamper-resistant content [23].

Figure 9 depicts the IPFS structure. Up to 256KB of data can be stored in each IPFS object. If the size exceeds, then data can be split up and stored in different IPFS object, and a new empty IPFS object is created with a link to a different part of the data. IPFS uses a Merkle tree structure to store data. Similar to the blockchain once data is stored it cannot be changed, instead versioning is used to refer to new data.

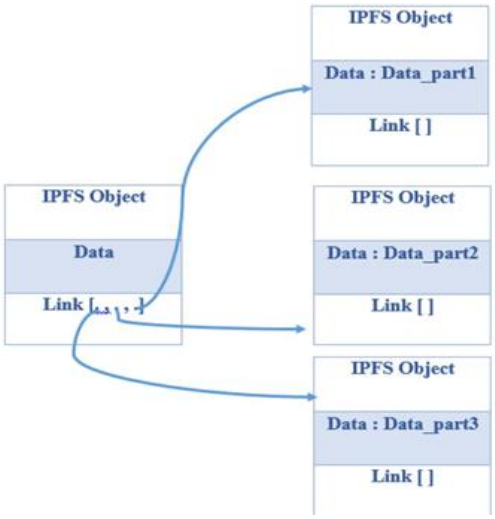

Figure 9. IPFS structure

g. Metamask

Metamask acts as a bridge between the decentralized web application and Ethereum blockchain node. It is included as an addon in chrome, firefox, and other browsers. Once configured, it can be used to identify the blockchain account holder and enables a user to sign the transaction using the private key.

5. RESULTS AND DISCUSSION

As mentioned earlier in the paper, Ganache is used in order to develop an application using test blockchain. Figure 10 represents, 10 test accounts with its private key, which can be used to test an application. Ganache also provides us with the GUI, to view transaction status, block creation status, and event logs as shown in Figure 11, Figure 12. The private key assigned for each account is used for digital signing the transaction. The user is authenticated based on the account address. Figure 13 represents, the GUI to add a suggestion. Once the requester adds a suggestion, the transaction is executed as shown in Figure 14. For each transaction, a fee is calculated based on instructions to be executed, each transaction is verified and validated by the miner before it is executed, and once the consensus is reached it is locked in the blockchain. Hence, this process ensured the validity and integrity of the transactions.

On viewing the request list, the responder can accept, reject or keep the request in the pending state as shown in Figure 15. Once responded a transaction is executed to update the changes. All the changes done to the data are stored as transactions in the blockchain, hence ensure data provenance. This helps to resolve the conflicts in the future and overcomes the problem of non-repudiation.

The existing decision-making system, rely on a centralized server or a third-party server. The users participating in decision-making need to trust the one who owns this server [24]. If the owner was compromised then the data in the server may have tampered [25]. In the proposed system, the trustworthiness and data integrity is ensured by the primary property of the blockchain technology.

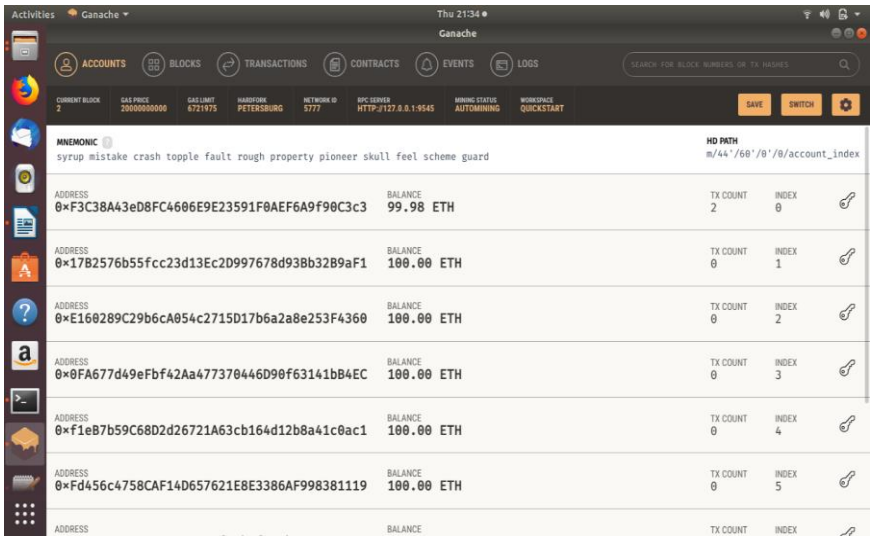

Figure 10. Ganache test account

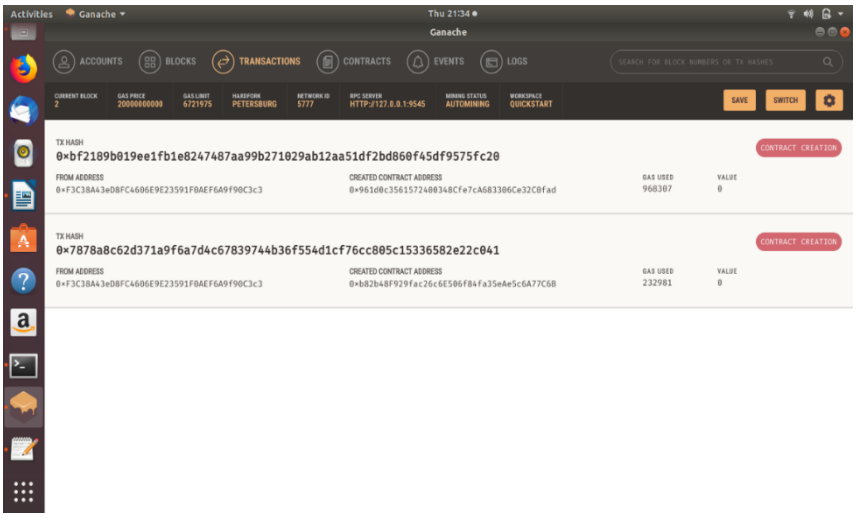

Figure 11. Transaction status

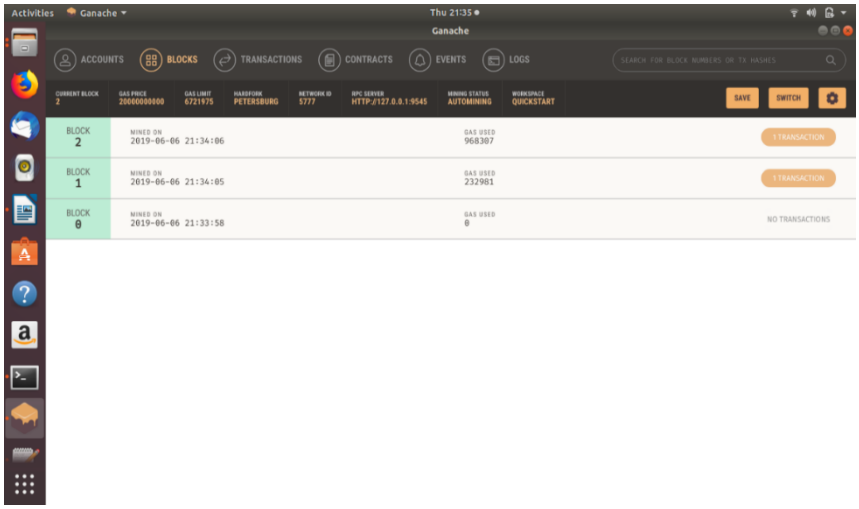

Figure 12. Block creation status

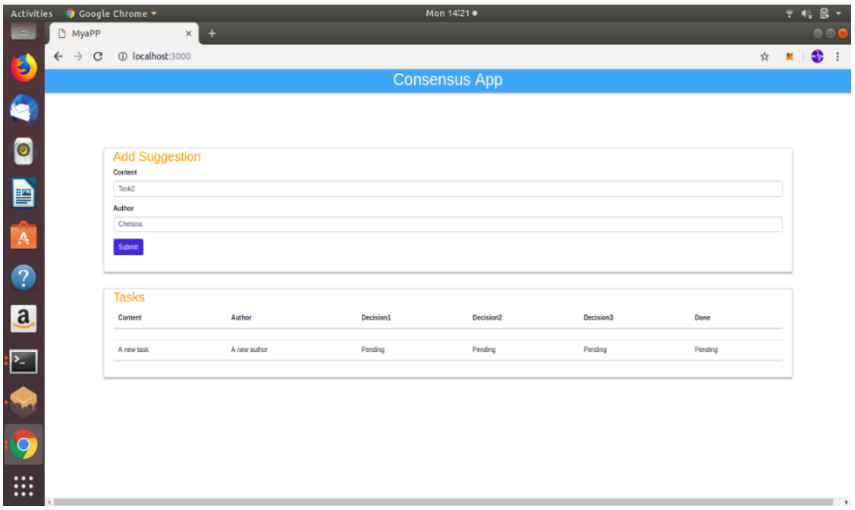

Figure 13. GUI to add suggestion

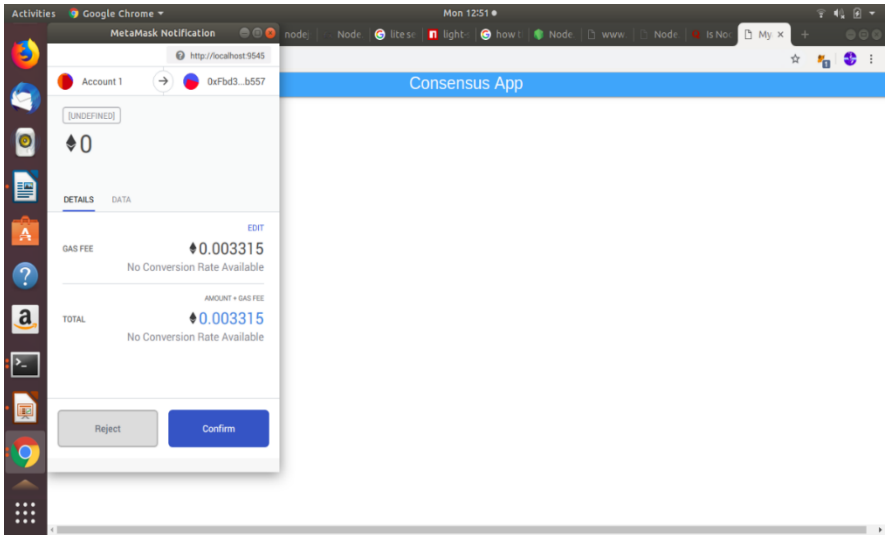

Figure 14. Transaction executed using Metamask

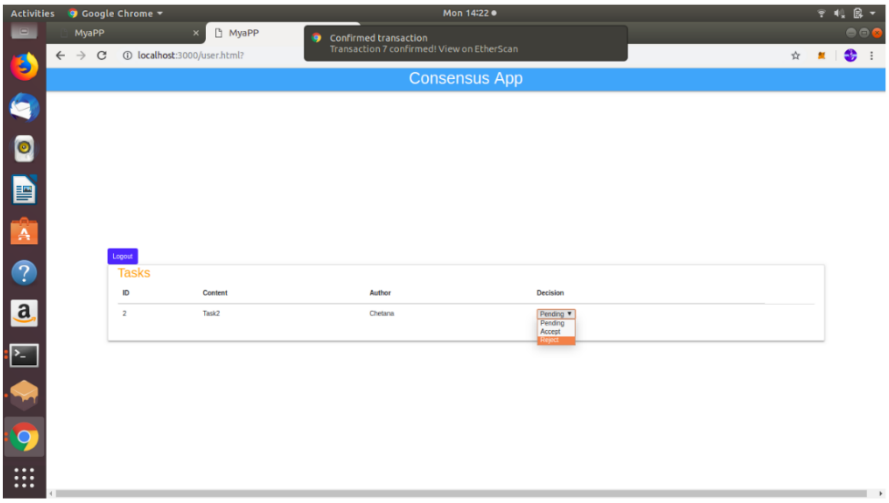

Figure 15. GUI for responder

6. CONCLUSION

In the proposed work, a decentralized consensus web application is developed using IPFS and Ethereum blockchain network. Both IPFS and blockchain along with smart contract ensures that the developed application is trustworthy and reliable. The proposed work can be further extended. Instead of storing all the data in smart contract storage, only confidential data like user credentials are stored in a smart contract. The remaining data concerning the consensus mechanism can be stored in IPFS.

REFERENCES

[1] T. T. A. Dinh, et al., "Untangling Blockchain: A Data Processing View of Blockchain Systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366-1385, 2018.

[2] T. Aste, et al., "Blockchain Technologies: The Foreseeable Impact on Society and Industry," *Computer*, vol. 50, no. 9, pp. 18-28, 2017.

[3] B. A. Scriber, "A Framework for Determining Blockchain Applicability," *IEEE Software*, vol. 35, no. 4, pp. 70-77, 2018.

[4] Vidya M. S and M. C. Patil, "Reviewing effectivity in security approaches towards strengthening internet architecture," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 3862-3871, 2019.

[5] N. Kshetri and J. Voas, "Blockchain in Developing Countries," *IT Professional*, vol. 20, no. 2, pp. 11-14, 2018.

[6] H. Zhao, et al., "Efficient key management scheme for health blockchain," *CAAI Transactions on Intelligence Technology*, vol. 3, no. 2, pp. 114-118, 2018.

[7] Edureka, "Blockchain Technology," 2017. [Online], Available: https://www.edureka.co/blog/how-blockchain-works/.

[8] A. E. Omolara and A. Jantan, "Modified honey encryption scheme for encoding natural language message," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 3, pp. 1871-1878, 2019.

[9] A. E. Omolara, et al., "Fingereye: improvising security and optimizing atm transaction time based on iris-scan authentication," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 3, pp. 1879-1886, 2019.

[10] J. Kang, et al., "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154-3164, 2017.

[11] D. Tosh, et al., "CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud," in *2018 IEEE 11th International Conference on Cloud Computing*, pp. 302-309, 2018.

[12] Bina Ramamurthy, "Blockchain Specialization," *Coursera*, 2017. [Online], Available: https://www.coursera.org/specializations/blockchain.

[13] S. Djanali, et al., "Design and development of voting data security for electronic voting (E-Voting)," in *2016 4th International Conference on Information and Communication Technology (ICoICT)*, pp. 1-4, 2016.

[14] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," *IEEE Access*, vol. 7, pp. 24477-24488, 2019.

[15] N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," *IEEE Software*, vol. 35, no. 4, pp. 95-99, 2018.

[16] I. M. Rodiana, et al., "Design of a Public Key Infrastructure-based Single Ballot E-Voting System," in *2018 International Conference on Information Technology Systems and Innovation (ICITSI)*, pp. 6-9, 2018.

[17] F. Hao, et al., "Verifiable Classroom Voting in Practice," *IEEE Transactions on Nuclear Science*, vol. 16, no. 1, pp. 72-81, 2018.

[18] J. A. Jaoude and R. G. Saade, "Blockchain applications – usage in different domains," *IEEE Access*, vol. 7, pp. 45360-45381, 2019.

[19] Y. Hu, et al., "A delay-tolerant payment scheme based on the ethereum blockchain," *IEEE Access*, vol. 7, pp. 33159-33172, 2019.

[20] Y. K. Kumar and R. M. Shafi, "An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 530-537, 2020.

[21] J. Adamu, et al., "Security issues and framework of electronic medical record: A review," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 9, no. 2, pp. 565-572, 2020.

[22] Savjee, "IPFS: Interplanetary file storage!," [Online], Available: https://www.youtube.com/watch?v=5Uj6uR3fp-U.

[23] G. McCubbin, "The Ultimate Ethereum Dapp Tutorial (How to Build a Full Stack Decentralized Application Step-By-Step)," 2019. [Online], Available: http://www.dappuniversity.com/articles/the-ultimate-ethereum-dapp-tutorial.

[24] O. W. Purbo, et al., "KawalPilpres2019: a highly secured real count voting escort architecture," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 17, no. 6, pp. 2834-2841, 2019.

[25] M. Awad, et al., "Security vulnerabilities related to web-based data," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 17, no. 2, pp. 852-856, 2019.

BIOGRAPHIES OF AUTHORS

Chetana Pujari is Research Scholar and working as Assistant Professor-Senior Scale in the Department of Information and Communication Technology, Manipal Institute of Technology, MAHE, Manipal, India. She has completed her graduation in B.E(Information Science and Engineering) and postgraduation in M.Tech(Computer Science and Engineering). She is currently pursuing her Ph.D. in Information Security.

Dr. Balachandra Muniyal, received his B.E degree in Computer Science and Engineering from Mysore University and M.Tech and Ph.D in Computer Science and Engineering from Manipal Academy of Higher Education, Manipal, India. He carried out his M.Tech project work in T-Systems Nova GmbH, Bremen, Germany. His research area includes Network Security, Algorithms, Operating systems. He has more than 30 publications in national and international conferences/journals. He was deputed to Manipal International University, Malaysia for 1 year in 2014. Currently he is working as the Professor and Head in the Dept. of Information and Communication Technology, Manipal Institute of Technology, Manipal. He has 25 years of teaching experience in various Institutes.

Dr. Chandrakala C B is currently working as Associate Professor-senior in the Department of Information and Communication Technology, Manipal Institute of Technology, MAHE,Manipal, India. Her research areas are Distributed Computing, Ad-hoc networks, Software Engineering. She has around 20 years of teaching experience.