

NATIONAL INSTITUTE OF TECHNOLOGY SILCHAR

Cachar, Assam

B.Tech. VIth Sem

Subject Code: CS-382

Subject Name: Introduction to Blockchain

Topic:

Implementation of dApp for Document Management System

Submitted By:

Students of Computer Science and Engineering:

- | | |
|---------------------------|-----------|
| 1. Ankur Upadhyay | - 1912117 |
| 2. Nazibul Omar | - 1912118 |
| 3. Sukh Dev Suthar | - 1912119 |
| 4. Prottay Kumar Adhikary | - 1912157 |
| 5. Subhojit Ghimire | - 1912160 |

Under the Guidance of:

Dr. Malaya Dutta Borah

Assistant Professor

Department of Computer Science and Engineering

TOPIC: IMPLEMENTATION OF DAPP (DECENTRALISED APPLICATION) FOR DOCUMENT MANAGEMENT SYSTEM.

AIM:

1. TO IMPLEMENT A DECENTRALISED DOCUMENT MANAGEMENT SYSTEM.
2. TO DRAW THE ARCHITECTURE OF DAPP AND SHOW THE DATA FLOW.
3. TO IMPLEMENT SECURITY PROTOCOLS IN FILE SYSTEM.

UNDERSTANDING DECENTRALISED APPLICATION (DAPP):

Decentralised Applications (dApps) are such applications that run on a blockchain network of computers instead of relying on a single computer or a server. Since dApps are decentralised, they are free from the control and interference of a single authority. They are typically built on Ethereum and aim to give users more control over their finances and data.

In general, the term *decentralise* or *decentralisation* refers to the process by which the activities of an organisation, particularly those regarding planning and decision making, are distributed or delegated away from a central, authoritative location or group. A decentralised system is a systems theory in which lower level components operate on local information to accomplish global goals.

Decentralised application is an application that can operate autonomously, typically through the use of smart contracts, that runs on a decentralised computing- the blockchain system. In today's digital world, dApps in finance, arts and collectibles, gaming and technology are on rise. Decentralised finance, for example, are applications that focus on building out finance services using cryptocurrencies.

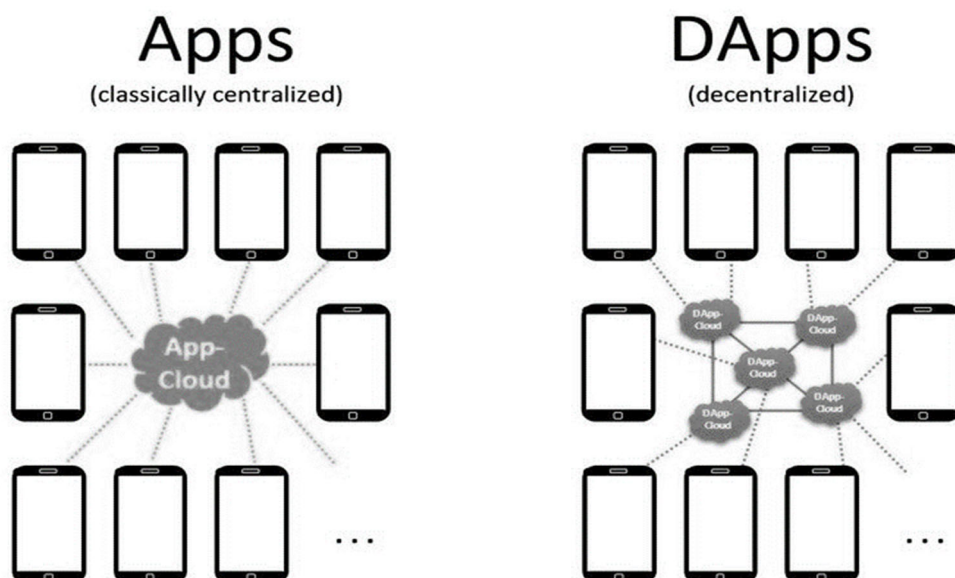


Fig.: Centralised Application Network (left) and Decentralised Application Network (right)

MECHANISM OF DAPPS:

dApps have their backend code (smart contracts) running on a decentralized network and not a centralized server. They use the blockchain for data storage and smart contracts for their app logic. Once dapps are deployed on the blockchain network, no individual can change them. dApps can be decentralized because they are controlled by the logic written into the contract, not an individual or a company.

FEATURES OF DAPPS:

- They run on blockchain.
- Their code is made open-source.
- They generate DAPP tokens to provide value to their contributing node.
- Users are granted access to them in exchange for tokens.
- Miners are rewarded with tokens when they successfully contribute to the ecosystem.

UNDERSTANDING SMART CONTRACT:

A smart contract is like a set of rules that live on-chain for all to see and run exactly according to those rules. For example, a vending machine: if one supplies it with enough funds and the right selection, they'll get the item they want. And like vending machines, smart contracts can hold funds much like a cryptocurrency account. This allows code to mediate agreements and transactions.

UNDERSTANDING DOCUMENT MANAGEMENT SYSTEM:

A document is a recorded information or object which can be treated as a unit (ISO 12651-2). Document Management System (DMS), also known as Record Management System, is a system or process used to capture, track and store electronic documents such as PDFs, word processing files and digital images of paper-based content. It helps to reduce and thus automate the entire document management. It makes the entire process paperless.

CHALLENGES OF TRADITIONAL DMS:

1. Traditional DMS saved files, folders, documents and images in a single location, such that it was impossible to retrieve the files at times of need easily.
2. It was time-consuming to manually search every folder one by one.
3. In addition to time consuming, it was cost ineffective to maintain after some usage.
4. The flexibility in naming and linking the related documents was not possible.
5. Duplicate information was often impossible to detect which would eventually lead to massive disorganisation that puts the security of the data at risk, along with damaging the productivity of a company. This also includes risk of having the data tampered with.

UNDERSTANDING BLOCKCHAIN AND ITS FUNCTION IN DMS:

Blockchain is a digital mechanism that enables two stranger parties to engage in trusted transaction with full confidence in the integrity of the assets being exchanged. Blockchain uses a distributed record-keeping system called a *ledger* that keeps track of changes to assets within the chain. This ledger is not centralised, instead distributed to all the computers in the chain, making it decentralised.

ADVANTAGES OF DECENTRALISED DMS:

1. Recognition of Documents
2. Classification and Data Indexing.
3. Data Validation guaranteeing integrity.
4. Increased Document Security and Control.
5. Better Search and Knowledge Management.
6. More reliable backups.
7. Fraud Control.
8. Processing using AI Algorithms.

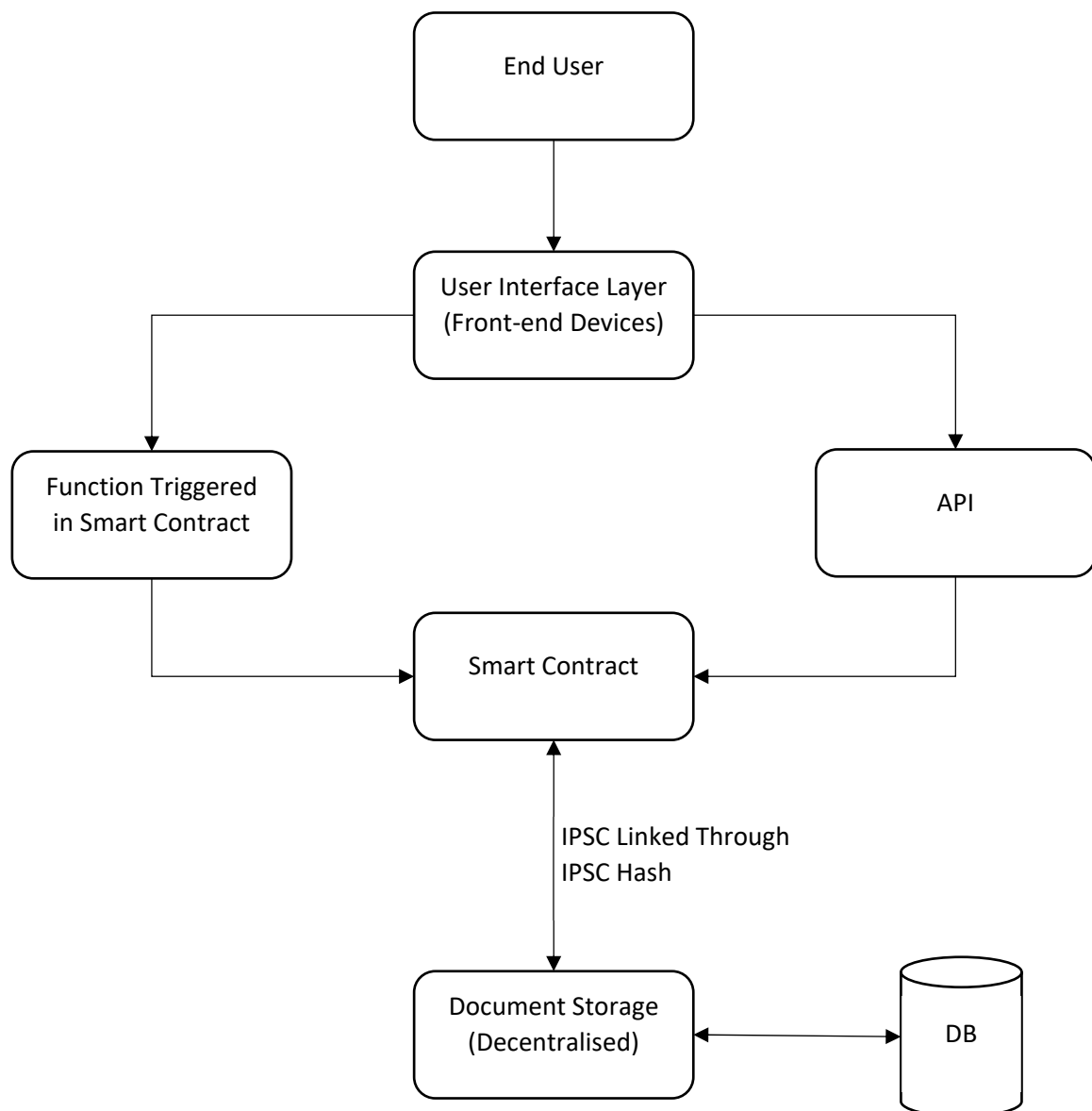
RELATED WORKS:

1. Lee, David Kuo Chuen. *Fintech Tsunami: Blockchain as the Driver of the Fourth Industrial Revolution*. Economics of Networks eJournal (2017): Blockchain enhances collaboration and provides a safe space for the distrusting parties to work together efficiently in a decentralised and innovative environment. These powerful crowd-sourcing and harnessing features make blockchain the main driver for the fourth industrial revolution.
2. Martiri, Edlira and Gentjana Muca, *DMS-XT: A Blockchain-based Document Management System for Secure and Intelligent Archiva*. RTA-CSIT (2018): DMS-XT is a document verification system. It stores the encrypted information in the blockchain, which, later, will be used for ownership verification. This system aims at providing a safe space for the diploma of bachelor and master students to publish and store their works without feeling insecure about their work being stolen or against fraud.
3. Vashistha, Mohit and Ferdous Ahmed Barbhuiya. *Document Management System using Blockchain and Inter Planetary File System*. Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure (2020): The underlying platform is built on the Ethereum platform with the smart contracts for various events written in Solidity. This paper also introduces various encryption techniques to provide additional security to the document in transition. The IPFS storage provides the distributed storage with content-based hashing, which makes the storage system more secure, resilient and immutable.
4. Shriyash Shingare, Neel Khalade, Raghav Saoji, Avadhoot Dhanve, Dr.Uma Pujeri. *Document Management using Private Permissioned Blockchain*. IRJET (2021): A blockchain-based DMS system will provide secure storage along with availability of e-document as and when required

by the owner of that particular e-document. A complete solution truly based on the digital information can be built with blockchain technology in DMS.

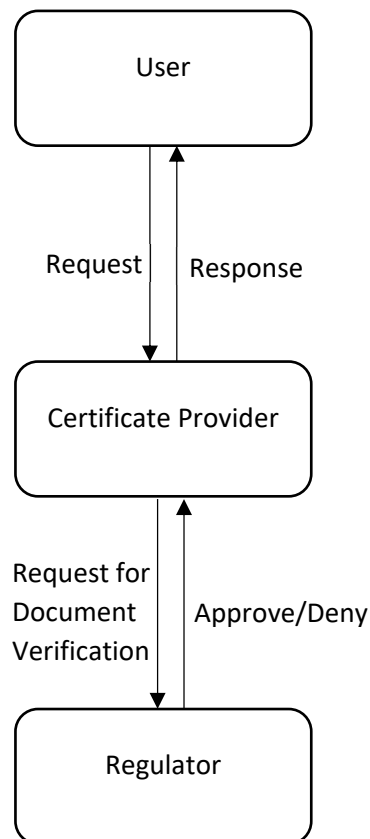
5. Mr. S. Choudaiah, Mr. U. Chandraselhar, *Blockchain Based Document Management System*. Journal of Engineering Science (2021): Data scalability, availability and integrity are all improved using Blockchain technology. Since blockchain application do not have a single point of failure, they are more resistant to DDoS attacks. Therefore, instead of using a big database stored in an extremely powerful server, the solution provided allows users to access their data through P2P network in which all participants are responsible for controlling and supervising the data.

BRIEF ARCHITECTURE:



Firstly, the user interacts with the frontend. Similarly, the frontend interacts with the API. Then, the smart contract meant for the specific task is called, which processes the request and does the necessary. The smart contracts query the distributed storage. The decentralised storage splits up the workload and processes that query and return the requested data or document.

DATA FLOW DIAGRAM:



Firstly, if a User wants to apply for a particular certificate, then they need to fill out an application regarding information related to that particular document. Then, this application is passed to the Regulator for verification and its further processing. If the application is verified by the Regulator, then they will check whether there is any balance available in the wallet or not. If the User gets a positive response after completing all the proceedings, they can issue or download the certificate.

STAKEHOLDERS:

1. **User:** The User applies for certificate in dApp by bringing their respective record or information to the Certificate Provider. If the request gets denied, the User has to reapply for the certificate after making corrections provided by the Certificate Provider. If the request gets approved, the User has to wait for certificate arrival.
2. **Certificate Provider:** The Certificate Provider provides the certificate to the User and even though from the User's perspective, it is the Certificate Provider that approves or declines their certificate request, it is in fact the Regulator that does that. The Certificate Provider

forwards the User's certificate request to the Regulator. If the Regulator declines the request, the Certificate Provider notifies the User about this cancellation and the reason behind their cancellation, so that the User can reapply after making correct changes. If the certificate gets approved, the Certificate Provider will take necessary steps to provide the User their certificate at the earliest possible.

3. **Regulator:** The Regulator is the one who either approves or declines the certificate request. The Certificate Provider sends the records of the User to the Regulator for certificate verification. If the Regulator is not satisfied with the certificate request for some reason like malicious record or faulty record, they notify the Certificate Provider of the decision taken along with reason. If the Regulator is satisfied with the certificate request, they send positive acknowledgement to the Certificate Provider.

SMART CONTRACT DESIGN TO AUTHENTICATE USER IN DAPP:

1. **Authentication Smart Contract:** This smart contract lets the user register or login themselves on the DMS.
2. **Document Management Smart Contract:** This smart contract lets users manage their documents on the DMS. Specifically, it allows users to upload, delete and get all the documents.

AUTHENTICATION CONTRACT:

1. State Variables

```
struct userDetails {  
    address addr;  
    string name;  
    string password;  
    bool isUserLoggedIn;  
}  
  
mapping (address => userDetails) public user;
```

2. Member Functions

```
// USER REGISTRATION FUNCTION  
function register (  
    address _address,  
    string memory _name,  
    string memory _password  
) public returns (bool) {  
    require (user [_address].addr != msg.sender);  
    user [_address].addr = _address;  
    user [_address].name = _name;  
    user [_address].password = _password;  
    user [_address].isUserLoggedIn = false;
```

```

        return true;
    }

    // USER LOGIN FUNCTION
    function login (
        address _address,
        string memory _password
    ) public returns (bool) {
        if (keccak256 (abi.encodePacked (user [_address].password))
            == keccak256 (abi.encodePacked (_password))) {
            user [_address].isUserLoggedIn = true;
            return user [_address].isUserLoggedIn;
        }
        else {
            return false;
        }
    }

    // USER LOGIN CHECK FUNCTION
    function checkIsUserLoggedIn (
        address _address
    ) public view returns (bool) {
        return (user [_address].isUserLoggedIn);
    }

    // LOGOUT FUNCTION
    function logout (
        address _address
    ) public {
        user [_address].isUserLoggedIn = false;
    }

```

DOCUMENT MANAGEMENT CONTRACT:

Member Functions

```

    // UPLOAD FUNCTION
    function upload (
        string memory bookB64
    ) public {
        user [msg.sender].files.push (bookB64);
    }

    // GET ALL DOCUMENTS FUNCTION
    function getDocument (
        string memory bookB64,
        address _address

```



```

) public {
    string [] memory newArray = user [_address];
    for (int i = 0; i < newArray.length; ++i) {
        if (bookB64 == newArray [i]) {
            return (user [msg.sender].files (newArray [i]));
        }
    }
}

// DELETE FUNCTION
function removeDocument (
    string memory bookB64,
    address _address
) public {
    string [] memory newArray = user [_address];
    for (int i = 0; i < newArray.length; ++i) {
        if (bookB64 == newArray [i]) {
            user [msg.sender].files.pop (newArray [i]);
            break;
        }
    }
    user [_address] = newArray;
}

```

SUMMING UP:

In this dApp, frontend will interact with user and will connect it to blockchain based backend. This will overcome the limitation of conventional DMS. When compared to the conventional DMS, block-based DMS would be more secure, and hence, more viable option. Here, metamask wallet is used for cryptocurrency to operate system functionalities over blockchain.

BIBLIOGRAPHY

Research Paper/Case Study/Journal References:

1. Lee, David Kuo Chuen. *Fintech Tsunami: Blockchain as the Driver of the Fourth Industrial Revolution*. Economics of Networks eJournal (2017)
2. Martiri, Edlira and Gentjana Muca, *DMS-XT: A Blockchain-based Document Management System for Secure and Intelligent Archiva*. RTA-CSIT (2018)
3. Vashistha, Mohit and Ferdous Ahmed Barbhuiya. *Document Management System using Blockchain and Inter Planetary File System*. Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure (2020)
4. Shriyash Shingare, Neel Khalade, Raghav Saoji, Avadhoot Dhanve, Dr.Uma Pujeri. *Document Management using Private Permissioned Blockchain*. IRJET (2021)
5. Mr. S. Choudaiah, Mr. U. Chandraselhar, *Blockchain Based Document Management System*. Journal of Engineering Science (2021)

Website References:

1. Document management defined
[<https://www.ibm.com/topics/document-management>]
2. What is DMS or Document Management System?
[<https://mobileappdevster.medium.com/traditional-vs-modern-document-management-system-f898af1a9c54>]
3. How dApps work
[<https://ethereum.org/en/dapps/>]
4. Traditional Document Management Software
[<https://mobileappdevster.medium.com/traditional-vs-modern-document-management-system-f898af1a9c54>]
5. Modern Document Management Software- Major Advantages
[<https://mobileappdevster.medium.com/traditional-vs-modern-document-management-system-f898af1a9c54>]
6. What is Document Management (DMS)?
[<https://www.aiim.org/what-is-document-imaging>]
7. What is Blockchain and why should Records Management Professionals Care
[<https://www.ironmountain.com/resources/general-articles/w/what-is-blockchain-and-why-should-records-management-professionals-care>]
8. Top 8 Blockchain Application for Documents You Need to Know
[<https://originstamp.com/blog/top-8-blockchain-applications-for-documents/>]
9. Smart contracts defined
[<https://www.ibm.com/topics/smart-contracts>]
10. Using Smart Contract Code
[<https://medium.com/coinmonks/how-to-do-authentication-in-decentralized-application-dapp-d9bc66b6249c>]
11. Dapp Authentication
[<https://github.com/Zaryab-Programmer/dapp-authentication>]