International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

MyDeed – A Blockchain Based Storage Solution for Official Documents

Jaymin S Chandaria, Keerthi Sai Adithiya, Harsh Mehta, Sterlin Minish T N

Computer Science – Cyber Security, Presidency Universuty, (UGC), Bangalore, Karnataka, India
mydeed.project@gmail.com

ABSTRACT—

In the age of digitalization of data, the handling and protection of secure official government documents is of utmost importance. The traditional methods of storing such data were entirely dependent on centralized databases are subjected to various threats and vulnerabilities such as tampering of data, unauthorized access, system breakdowns and so on. To overcome these difficulties, our project "myDeed" suggests a solution that uses a database storage system that uses blockchain system. This novel approach seeks to enhance the security, accessibility and storage of official documents produced by the government. Government documents are important for a nation to function and make sure the administration, and historical record-keeping are intact and are not tampered with. Blockchain technology is decentralized and uses a distributed ledger that supports cryptocurrencies and cryptographically stored data and offers a secure and transparent method to store and access data. The project utilizes the key factors of blockchain, such as decentralization, transparency, and immutability, to establish a storage medium that guarantees the integrity and confidentiality of official documents. By using cryptographic security measures, every transaction or data entry is incorporated into records that cannot be tampered with or corruption, or unauthorized intrusion. This gives a strong solution to the changing difficulties presented by digitalization and cyber risks.

Keywords—sensitive government documents, centralized databases, Database Storage System, Blockchain technology, cyber threats

I. Introduction

The rapid progress of technology has not only introduced great conveniences but has also brought up new challenges in protecting private and crucial information from evolving cyber threats and dangers. To address the issues and to present a strong and solution, "myDeed" aims to take the way in a sincere effort: a Database Storage Medium that utilizes Blockchain and it's advantages to enhance the security, accessibility, and storage of government documents.

a) Significance of securing Govt. Documents

The importance of official documents cannot be stressed, as they are the primary source of identification in terms of administration, and historical record-keeping. The traditional approaches to storing such documents, that are frequently dependent on centralized databases storage mediums, are subjected to a wide range of attacks and risks, including unauthorized access and data tampering, as well as system failures and are also subjected security breaches. To overcome these challenges, the inclusion of Blockchain brings in a revolutionary solution that not only resolves the present issues but also brings a fundamental change in how we can view and execute data storage systems.

b) Blockchain Technology as the Cornerstone

Blockchain, has shown its effectiveness in delivering crucial levels of security and transparency. "my Deed" aims to utilize the fundamentals of blockchain, including decentralization, transparency, and immutability, to establish a database storage system that guarantees the integrity and confidentiality of official documents produced by government bodies. Each entry of data, i.e., transaction will be cryptographically protected, creating a rigid sequence of records that is impermeable to unauthorized access, corruption, or tampering.

II. Key Features and Technological Aspects

a) Immutability

Immutability is a characteristic of blockchain where once data is recorded on a blockchain, it is impossible to delete it or tamper with it. It is ensured by cryptographic hashing and the decentralized structure of the blockchain where each block is linked to its predecessor making it a secure chain of critical information. This makes any record permanent and enhances the security that a system possesses. Thus, making blockchain a reliable ledger for data storage and transactions.

b) Decentralization

Decentralization in blockchain basically shifts the storage system from a centralized model to distributed model. Instead of data being stored in a single point medium, it is dispersed across a network of data nodes which have copies of the ledger entirely. Thus, security is enhanced, single point failure is omitted and centralized control is removed making the system a resilient data storage medium.

c) Transparency

Transparency in blockchain ensures a dynamic shift from the conventional database storage models. The transactions made in the blockchain is visible to all the members present, creating an open ledger system. The visibility of the transactions makes sure that the accountability of the entered data is intact and all the changes and additions to the database is visible and is verifiable to everyone on the network. This is crucial as the project requires high level of integrity and auditability.

d) Accountability

Accountability in blockchain for a database storage system enhances the traceability and transparency. Every transaction on a blockchain is recorded with a timestamp and is linked to its predecessors. This creates an immutable audit trail which will be verifiable by all parties present in the chain. Every addition or alteration is permanently recorded in the database. Thus, this ensures high level of trust and integrity in the data.

e) Enhanced Security

Enhanced security of blockchain refers to its structure and cryptographic protocols. As each transaction made is encrypted and linked to its predecessor that creates a chain that is very difficult to tamper with. The decentralized approach has data distributed data multiple nodes. This makes data resilient against unauthorized attacks and access.

III. Areas of focus

a) Secure Storage

Secure storage is achieved by dispersing data across multiple nodes in a network. Here each node is encrypted and interconnected making the risk of data tampering significantly lower. The following elements contribute to a secure storage infrastructure:

1. *Encryption: Robust encryption algorithms are being used to protect data at rest. All data stored on the blockchain are encrypted, ensuring that even if a node is compromised, the data remains unreadable without the appropriate decryption keys.*
2. *Distributed Storage: The decentralized characteristic of blockchain is used to distribute data across multiple nodes. This makes sure that there is no single point of failure and enhances sturdiness against loss of data and prevent unauthorized access.*
3. *Smart Contracts: Implementation of smart contracts to enforce access-control policies. Smart contracts define rules for data access, specifying which party can read, write, or modify data.*
4. *Consensus Mechanisms: The validity of transactions and data stored in the blockchain is through a consensus mechanism. Algorithms such as Proof of Work or Proof of Stake play a crucial role in preventing malicious activities and maintaining the integrity of the database storage system.*
5. *Private and Public Keys: The use of private and public keys for access control. Users with their respective private keys will be able to decrypt and access the required information that has been stored, thus, adding a strong layer of authentication and authorization.*
6. *Hash Functions: Unique identifiers are generated using secure hash functions. The integrity of data is measured as these hashes act as fingerprints. Alterations to the stored data will result in a mismatch, indicating potential data tampering.*
7. *Regular Audits: Audits in regular intervals are conducted to identify vulnerabilities. A detailed security stance is maintained by reviewing data and access logs along with smart contract details.*
8. *Redundancy and Backups: As data is spread over multiple data points i.e., nodes, it establishes redundancy. Additional backup is implemented in case of a node failure.*

By integrating such security measures, a blockchain-based storage medium can provide high-level of protection for stored data and transactions, making sure that the stored data remains confidential, and not tampered with. This makes sure the data is only accessible only to authorized entities within the decentralized network created.

b) Efficient Retrival of Data

Efficient retrieval of data in a blockchain-based database storage system is important for the maximum utility of the technologies implemented. There are several strategies that can be implemented to optimize the retrieval of data within this framework:

1) *Indexing and Metadata: Develop and incorporate resilient indexing mechanisms and storage systems for metadata. Linking data with pertinent metadata and establishing efficient indexes facilitates expedited and more accurate retrieval of information. This is particularly crucial in blockchain networks of significant magnitude.*

2) *Sharding: Partition the data into smaller, controllable fragments referred to as shards. Every shard has the ability to be stored on distinct nodes throughout the network. Sharding enables concurrent processing, enabling multiple nodes to retrieve data simultaneously, thereby greatly enhancing retrieval speed.*

3) *Caching Mechanisms: Implement catching mechanisms to temporarily store the frequently accessed data. Retrival time is minimized by positioning the caches in proximity to the nodes or users, enhancing the efficiency of the system.*

4) *Optimized Smart Contracts: Create smart-contracts tailored for optimal retrival of data ensuring that these contracts have defined methods for the retrival and accessing of data based on different criterias.*

5) *Peer-to-Peer Networking: Utilize peer-to-peer networking to retrive data. Here is where nodes have the capacity to communicate with one another in to request and retrieve particular data thus decreasing latency tremendously compared to conventional centralized systems.*

6) *Content Addressing: Implement content addressed storage in which unique address of data is determined by the content present. This removes the necessity of a centralized directory simplifying the retrieval of data by directly referencing the content instead of it's actual whereabouts.*

7) *Parallel Processing: Leverage the parallel processing capabilities of blockchain networks. Actively retrieve the data from multiple nodes leveraging the decentralized network architecture to optimize speeds.*

8) *Compression Techniques: Apply compression techniques to reduce the size of stored data. Smaller data blocks will lead to faster data retrieval times, especially in cases where bandwidth is a limiting factor.*

By incorporating these strategies, a blockchain-based database storage system can achieve efficient data retrieval, meeting the demands of diverse applications and user requirements while taking full advantage of the decentralized and secure nature of the blockchain architecture.

c) Scalability

Scalability is a crucial factor for a blockchain-based database storage system implemented for storing official documents produced by the government and other entities, given the importance of such data.

1) *Off-Chain Storage Solutions: Implement off-chain storage options for non essential and buffer documents. Not all data needs to be stored on the blockchain. Using off-chain solutions can alleviate burden on the primary blockchain network.*

2) *Interoperability: Ensure compatibility and seamless integration with other systems and databases. This enables the smooth incorporation of current government document management systems, eliminating the necessity for a total revamp and facilitating scalability through the utilization of existing infrastructure.*

3) *Governance Models: Create a versatile governance framework capable of adjusting to evolving demands. This encompasses the capability to enhance protocols, implement novel functionalities, and cater to growing storage requirements while maintaining the system's security and stability.*

4) *Network Upgrades: Develop and implement regular network upgrades to integrate enhancements in scalability. This proactive strategy guarantees that the storage system, which is based on blockchain technology, stays adaptable to the changing requirements of storing and overseeing government documents.*

5) *Cloud Integration: Investigate cloud-based options for storing blockchain data. Cloud platforms provide scalability advantages by enabling the storage system to flexibly allocate resources according to demand, ensuring optimal performance during periods of heightened activity.*

By addressing these scalability considerations, a blockchain-based database storage system can scale effectively to accommodate the growing volume of official documents. This ensures that the system remains robust, secure, and capable of meeting the evolving demands of digital governance and document management.

IV. Existing Services

a) The below are a few examples of the existing services that exist in the present market for solving the said issues:

1) *CarVertical: CarVertical is a blockchain-based platform that provides a transparent vehicle history registry. It leverages blockchain technology to store and verify information related to a vehicle's history, including ownership changes, accidents, and maintenance records.*

2) *VeChain - Automotive Solutions: VeChain offers blockchain solutions for the automotive industry. It focuses on providing transparency in the supply chain, anti-counterfeiting measures, and traceability of data. VeChain's blockchain technology ensures the integrity and authenticity of information related to vehicles.*

3) *IBM Blockchain for Vehicle Lifecycle and Identity: IBM provides a blockchain solution targeting the entire lifecycle of vehicles. This service covers aspects such as vehicle identity, ownership records, and maintenance history. IBM's blockchain technology enhances the security and transparency of data throughout a vehicle's lifecycle.*

4) *Carfax: Carfax is a widely used service that offers comprehensive vehicle history reports. While not based on blockchain technology, Carfax provides information about a vehicle's past, including accidents, title issues, and odometer readings.*

5) *AutoCheck: AutoCheck is a vehicle history reporting service that provides detailed information about a vehicle's history, including title information, accident reports, and odometer readings. It operates independently of blockchain technology.*

6) *National Motor Vehicle Title Information System (NMVTIS): NMVTIS is a U.S. government system that provides vehicle history information, helping to prevent title fraud and unsafe vehicle practices. It compiles data from various sources but does not utilize blockchain technology.*

7) *CarShield: CarShield is a service that offers extended vehicle service contracts and protection plans. It focuses on providing coverage for mechanical breakdowns and repairs, but it does not incorporate blockchain technology for data storage.*

8) *AutoTrader:AutoTrader is an online marketplace for buying and selling vehicles. It allows users to search for and list vehicles for sale, providing a platform for connecting buyers and sellers. AutoTrader operates without the use of blockchain technology.*

9) *Kelley Blue Book: Kelley Blue Book is a widely used service for estimating the value of vehicles. It provides information on the fair market value of cars, helping buyers and sellers make informed decisions. This service is not built on blockchain technology.*

b) Issues with the existing methods:

1) *Security Concerns: Centralized databases are vulnerable to security breaches. If the central database is compromised, all vehicle ownership records are at risk of theft or modification. Additionally, the potential for unauthorized access poses a significant threat to the confidentiality of sensitive information.*

2) *Fraud and Corruption: Centralized systems are prone to fraud and corruption. Corrupt officials may exploit their control over the database for personal gain, such as selling or leasing vehicles illegally. This creates a breeding ground for illicit activities, eroding the integrity of the entire system.*

3) *Transparency and Trust: Centralized databases lack transparency, as access to records is controlled by a single entity. This makes it challenging to verify the accuracy of ownership records. Moreover, the absence of a transparent system undermines public trust in the legitimacy of the recorded information.*

4) *Scalability Issues: Centralized databases may face scalability challenges as the number of vehicles and transactions increases, leading to slow performance. The system's inability to efficiently handle a growing volume of data hampers its scalability, impacting its overall effectiveness.*

5) *Identity Verification: Identity verification processes in centralized systems may be susceptible to manipulation or errors. Moreover, the reliance on a single point of verification increases the risk of identity theft and compromises the overall reliability of the verification process.*

6) *Privacy Concerns: Centralized databases may raise concerns about the privacy of individuals' data, especially if the central authority does not handle it securely. Furthermore, the lack of stringent privacy measures may result in unauthorized access to personal information, posing a significant threat to individuals' privacy rights.*

7) *Government Oversight: Government oversight in centralized systems may vary, and there may be challenges in enforcing regulations. Additionally, inconsistent oversight opens the possibility of regulatory loopholes, undermining the effectiveness of governance in ensuring the proper functioning of the centralized database.*

8) *Data Manipulation and Forgery: Centralized databases can be vulnerable to data manipulation and forgery, as a single point of control makes it easier for unauthorized changes to be made. This susceptibility opens the door to fraudulent activities and compromises the integrity of the data stored in the system.*

V. Objectives of “myDeed”

Discussing the primary objectives of myDeed in terms of a finished product overcoming all the drawbacks faced by the previous and presently existing services:

a) Scalability:

This objective involves ensuring that the system can handle an increasing number of transactions and users while maintaining optimal performance. This might involve employing sharding techniques, sidechains, or layer-two solutions to distribute the workload efficiently across the network.

b) Interoperability:

Achieving compatibility with existing systems and databases is crucial for a seamless transition and integration. This could entail utilizing standardized protocols or APIs that allow your blockchain system to communicate effectively with other platforms, ensuring data can be shared and utilized across different systems.

c) Regulatory Compliance:

Adhering to legal and regulatory frameworks is vital. Consider aspects like data privacy laws (e.g., GDPR), vehicle ownership regulations, and financial transaction laws. Implementing features like permissioned access and compliance checks can help meet these requirements.

d) Cybersecurity Measures:

Strong security measures are essential to protect against hacking and unauthorized access. This might involve encryption techniques, multi-factor authentication, regular security audits, and consensus mechanisms that prioritize network security.

e) Environmental Impact:

Addressing concerns about the environmental impact of blockchain involves exploring consensus mechanisms that are more energy-efficient (moving away from Proof of Work), or even integrating sustainability initiatives like carbon offset programs.

f) Web3 Integration:

Leveraging Web3 technologies can enhance transparency and security by utilizing decentralized protocols. This can involve integrating smart contracts for immutable vehicle ownership records, reducing the potential for fraud.

g) Fruad Reduction:

Implementing robust fraud detection mechanisms involves employing AI/ML algorithms to detect suspicious patterns in transactions or ownership changes, thereby safeguarding the integrity of the system.

h) Decentralized Record:

Eliminating centralized records means spreading the data across the network, enhancing security by reducing the risk of a single point of failure or attack.

i) Secure On-Chain Data:

This involves ensuring that data stored on the blockchain is secure. This can be achieved through encryption, access controls, and leveraging private/public key cryptography for secure data handling.

j) Blockchain Trilemma:

Balancing decentralization, security, and scalability is a significant challenge. Solutions might involve a hybrid approach, where trade-offs are made based on specific use cases or employing innovative consensus mechanisms that address this trilemma.

k) UI/UX Enhancement:

Improving the user interface and experience is crucial for user adoption. Streamlining design, simplifying processes, and making it intuitive can significantly enhance user satisfaction.

VI. Methodology of myDeed

Here all the modules that will be incorporated in myDeed is explained with respect to the database storage management of government documents:

a) User Interface (UI):

Develop a basic and intuitive UI using HTML, CSS, and JavaScript to allow users to submit and retrieve data easily. Ensure a responsive design for accessibility across various devices.

b) Smart Contracts:

Utilize the Solidity programming language to create a data storage smart contract on the Ethereum blockchain. Implement functions for secure and transparent data transactions, ensuring data integrity and immutability.

c) Web3 Integration:

Integrate Web3.js into the UI to establish a connection with the Ethereum blockchain. Enable seamless interaction between the UI and the Ethereum network for submitting and retrieving data.

d) Access Control:

Develop access control logic within the smart contract to manage user permissions. Specify roles and permissions to control who can interact with stored data.

e) Data Retrieval:

Create a service or API to retrieve and display data from the Ethereum blockchain. Implement efficient querying mechanisms to facilitate data retrieval based on user or application criteria.

f) Logging and Monitoring:

Implement basic logging functionalities to track system health and security events. Utilize logging frameworks for structured log data. Integrate monitoring tools for real-time tracking of system performance and potential security issues.

g) Documentation:

Develop comprehensive documentation for users and developers, including user guides for navigating the UI and interacting with the system and developer documentation covering smart contract functions, API endpoints, and integration guidelines.

h) Security:

Embed inbuilt validation and verification tests within smart contracts to ensure the integrity of data being stored and accessed. Regularly update and audit smart contracts to identify and address potential security vulnerabilities. Follow best practices for secure coding in Solidity and implement measures to prevent common attacks (e.g., re-entrancy, overflow).

A diagrammatic representation of the modules of myDeed is showcased in Fig. 2.

VII. Relatable Outcomes from myDeed

Now the outcomes of myDeed will be discussed which aims to overcome all the challenges posed to the other proprietary services and solutions that were/are instated in the present systems. Using myDeed to store and secure documents poses a ton of advantages as well as use cases.

a) General Outcomes;

- Creating a decentralized storage management system.
- Eliminating the threats of fraud and illegal transaction.
- Avoiding centralized DBMS to reduced single point of failure.
- Creating a better user UX/UI than the existing government websites. i.e., (parivahan.gov.in)
- Increasing environment sustainability by reducing the carbon footprints produced by the traditional DBMS system.

b) Specified Outcomes:

1) *Immutability and Tamper Resistance: Vehicle documents stored on the blockchain become immutable and tamper-resistant. Once recorded, the data cannot be altered or deleted, ensuring the integrity of the documents.*

2) *Enhanced Security and Privacy: Implementation of robust encryption and access control mechanisms provides enhanced security and privacy for sensitive vehicle documents, reducing the risk of unauthorized access or data breaches.*

3) *Streamlined Verification Processes: Verification of vehicle documents becomes more efficient and streamlined. Authorities, insurers, and other stakeholders can easily access and verify the authenticity of documents directly from the blockchain.*

4) *Reduced Fraud and Identity Theft: The use of blockchain technology reduces the risk of document forgery and identity theft. The transparent and decentralized nature of the blockchain enhances trust in the authenticity of stored documents.*

5) *Improved Regulatory Compliance: Adherence to regional and industry-specific regulations is enhanced, reducing the likelihood of legal issues. The transparent and auditable nature of blockchain transactions facilitates compliance reporting.*

6) *Efficient Data Retrieval: The implementation of data indexing and retrieval mechanisms on the blockchain ensures quick and efficient access to stored vehicle documents. This can expedite processes such as vehicle registration and verification.*

7) *User Empowerment and Ownership: Vehicle owners gain greater control and ownership of their documents. They can easily access, share, and manage their information while having confidence in the security and privacy of the stored data.*

8) *Interoperability with Existing Systems: Successful integration with existing databases and systems used by government agencies, insurance companies, and other stakeholders promotes interoperability, facilitating a seamless flow of information.*

9) *Environmental Sustainability (Depending on Blockchain Platform): If using environmentally friendly consensus mechanisms, the project can contribute to environmental sustainability by minimizing energy consumption, especially if using proof-of-stake or other eco-friendly alternatives.*

10) *Trust and Transparency: The transparent and decentralized nature of the blockchain instills trust among stakeholders. They can verify and trust the information recorded on the blockchain, promoting transparency in dealings related to vehicle documents.*

11) *Cost Savings: While there are costs associated with blockchain transactions, the project may lead to cost savings in areas such as fraud prevention, document verification, and data reconciliation.*

12) *Innovation and Technological Leadership: Implementing a blockchain storage solution for vehicle documents demonstrates innovation and technological leadership in the transportation and document management sectors, positioning the project as a forward-thinking initiative.*

13) *Improved User Experience: A user-friendly interface and efficient document retrieval processes contribute to an improved user experience for vehicle owners and other stakeholders interacting with the blockchain system.*

14) *Reduced Administrative Burden: Automation of document storage and verification processes on the blockchain reduces the administrative burden on government agencies, insurance companies, and other entities involved in managing vehicle-related information.*

VIII. Working of myDeed

As ‘myDeed’ is primarily a service-based entity, a website has been developed where the users can utilize the service. The objectives of ‘myDeed’ are to accept data from the users and store it securely in a blockchain where in which the users and the respective authorities can upload and view the documents and make necessary changes when necessary. The detailed working of ‘myDeed’ platform is mentioned in the following:

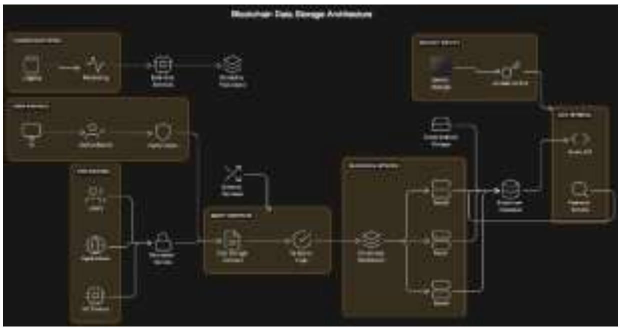


Figure 1: This figure depicts the architecture diagram of the working of myDeed’s Blockchain Data Storage.

a) Registration of Users:

Once the website of ‘myDeed’ is accessed, the users are prompted to the signup page where the user is requested to register their account by providing basic information such as; full name, email address, phone number and so on. The registered user data is store in a SQL server from where the verification and validation of the user will be done. Upon registering, the users are now redirected to a login page where the username and password given during the registration is prompted. Once the data is verified and logged, the user is now logged into ‘myDeed’ and is redirected to the homepage. All mentioned steps are shown in Fig. 3 in a flowchart manner for a better understanding of the workflow.

b) Navigation through the website:

The website of ‘myDeed’ contains several pages that has a different purpose. The pages are as follows:

1) *Homepage: The homepage contains all the basic information regarding what ‘myDeed’ represents and what services it provides. It also shows all the other primary parts of the websites that the users can visit for accessing other relevant information. It also gives the users information reagding the present services available on ‘myDeed’ and also an insight to what they can expect in the future.*

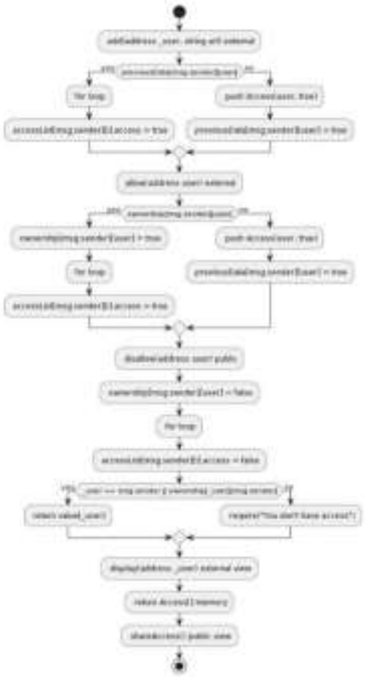

add(address _user, string url) external
yes
no
for loop
accessList[msg.sender][i].access = true
previousData[msg.sender][user] = true
allow(address user) external
for loop
accessList[msg.sender][i].access = true
disallow(address user) public
for loop
accessList[msg.sender][i].access = false
return value[_user]
require("You don't have access")
display(address _user) external view
shareAccess() public view

Figure 2: This figure depicts the flowchart of the pseudocode of the program module for uploading a file to the blockchain based database storage system.

2) *About Us: This page of the website tells the users about 'myDeed' as a whole and showcases the services provided. It also gives the users an insight to the philosophy of the developers of 'myDeed' so the users can understand the purpose of the website and the service developed. The realtime users of the website is also displayed so the new users can understand the significance of 'myDeed' and its services. The developers of 'myDeed' are also showcased in the website.*

3) *Profile: The profile page is similar to a dashboard but straight to the point of the relevant information that the user is seeking for. All data uploaded on-chain is displayed here along with the user information that can be used for their references. An option for a peer-to-peer connection for transfer of data as well as information is also enabled. This page is where the primaries of 'myDeed' is provided to the user.*

4) *Contact Us: The contact us page provides information to contact the developers for support and other queries related to the services provided by 'myDeed' and also for technical support in case they face any difficulties in using or accessing the services. The users can make use of the query box or directly contact the admins with the provided email address.*

SOFTWARE REQUIREMENTS		
for Development Environment	npm	Package manager to install JavaScript dependencies.
for Frontend Development	HTML5, CSS3, JavaScript ES6+, Bootstrap	For creating web pages and scripting.
	PHP	To handle database connections, login/signup page inputs.
	Web3.js Library(CDN)	To interact with Ethereum nodes from the web browser.
	Solidity	For writing smart contracts (version ^0.8.0).
	IDE/Text Editor	Visual Studio Code
for Smart Contract Deployment and Testing	Hardhat	For smart contract compilation, deployment, and testing.
	Sepolia Testnet	An ethereum testnet for smart contracts to interact with a testnet instance of the ethereum blockchain.

for Ethereum Wallet	Metamask	Browser extension or mobile app for Ethereum wallet management and transaction signing.
	Testnet Tokens	Acquire test Ether from faucets for Sepolia test net with Alchemy RPC URL and API key.
for IPFS	Pinata API details	To pin files to IPFS through Pinata's remote pinning service and for file storage and to interact with the IPFS network.
for Web Server	XAMPP (APACHE)	Web server software like Apache through XAMPP control panel for deploying the web application.
for Database Management	XAMPP (MYSQL)	To perform CRUD operations on databases and tables.
for Version Control	Github, Git	remote repository hosting.
Browser	Google Chrome, Firefox, or any browser	To be compatible with MetaMask and modern web standards.

Table 1 The Software requirements for myDeed .

c) Working of the backend instances:

Here we come to an understanding that once a user uploads their relevant documents, it must be uploaded on the blockchain.

1) *Connecting to metamask: The user has to connect their account with metamask wallet for a successful communication with the deployed smart-contract.*

2) *Post upload: Once the user clicks the upload button, the file is uploaded onto the Pinata IPFS Cloud and returns the URL of the IPFS upload or the CID (Content Identifier).*

3) *Displaying the uploaded files: This step can only be achieved after a successful login from the user's end where the data to be displayed is in the form of a table with the table headers – "file name", "users with access" and "IFPS URLs/CID".*

4) *Sharing Access: This step can also achieved only after a successful login from the user's end where a user is able to share access to their uploaded files to another wallet address(users/entities).*

5) *Backend Deployment of Smart Contracts: Using Hardhat deployment framework, we compile and also run the smart contracts and generate a contract address to be used for successful contract communication i.e., web3 communication such as upload, display and shared-access.*

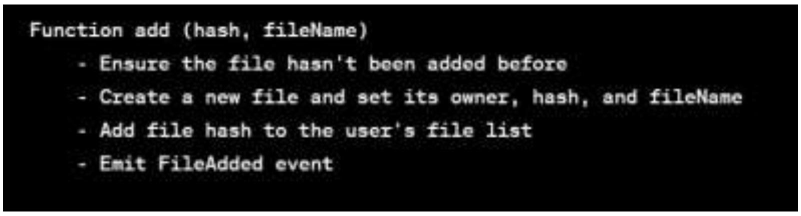
6) *Communication: A javascript file is used to contact or communicate with the smart contract using "ethers" CDN URL. It is also used for user interface design for upload, display and shared-access design.*

HARDWARE REQUIREMENTS	
Processor	Intel Core i5 or equivalent.
RAM	Minimum 8GB (16GB or higher recommended for development purposes).
Storage	SSD with at least 256GB of free space (for faster read/write operations).
Internet Connection	Stable high-speed internet for deploying contracts, connecting to IPFS, and accessing the Blockchain..
Operating System	Windows, macOS, or Linux (Latest)

Table II: The hardware requirements For myDeed

d) Understand the Code:

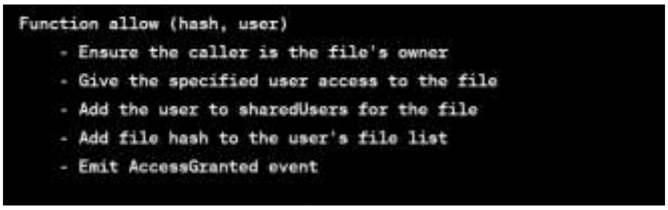
Here we have a few pseudo codes of the modules for a better understanding of the working of the backend;



```
Function add (hash, fileName)
    - Ensure the file hasn't been added before
    - Create a new file and set its owner, hash, and fileName
    - Add file hash to the user's file list
    - Emit FileAdded event
```

Fig. 4. Pseudocode of “File Upload” module of myDeed

1) *File Upload Module: The user is allowed to upload a file. It ensures that the file hasn’t been added before. It created a new file and sets its owner, hash, and file name. It then adds the file hash to the user’s file list*

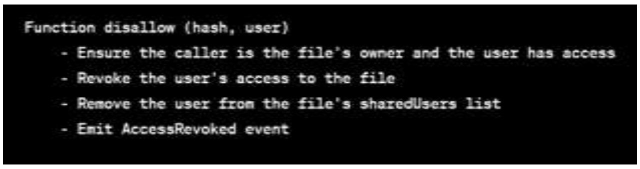


```
Function allow (hash, user)
    - Ensure the caller is the file's owner
    - Give the specified user access to the file
    - Add the user to sharedUsers for the file
    - Add file hash to the user's file list
    - Emit AccessGranted event
```

Fig. 5. Pseudocode of “Share Access” module of myDeed

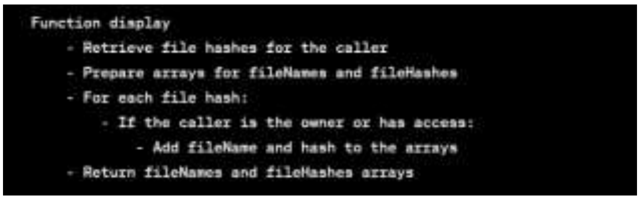
2) *Share Access: It is ensured that the share access is called by the file owner and the file belongs to the owner. It also makes sure that the owner has access to the files. It then gives the specified user’s access to the file and add user to the list of shared users. Then the hash of the file is added to user’s file list.*

3) *Revoke Access: It ensures that the function caller is the owner of the file and the shared user has access. It then revokes the user access to the file and then removes the user from the file’s shared user’s list.*



```
Function disallow (hash, user)
    - Ensure the caller is the file's owner and the user has access
    - Revoke the user's access to the file
    - Remove the user from the file's sharedUsers list
    - Emit AccessRevoked event
```

Fig. 6. Pseudocode of “Revoke” module of myDeed



```
Function display
    - Retrieve file hashes for the caller
    - Prepare arrays for fileNames and fileHashes
    - For each file hash:
        - If the caller is the owner or has access:
            - Add fileName and hash to the arrays
    - Return fileNames and fileHashes arrays
```

Fig. 7. Pseudocode of “Display” module of myDeed

4) *Display Module: It retrieves all the file hashes of the user. It then prepares arrays for the file names and file hashes. And then for each file hash, if the caller is the owner or has access to the file, it adds file name and file hash to the array.*

IX. Literature Review

A. *Trinh Viet Doan, Yiannis Psaras, Jörg Ott, Vaibhav Bajpai, ” Towards Decentralised Cloud Storage with IPFS: Opportunities, Challenges, and Future Considerations”, DOI: arXiv:2202.06315v2 [cs.NI]*

The paper introduces the InterPlanetary File System (IPFS) as a decentralized storage architecture utilizing peer-to-peer networking and content addressing. It details the design and core features of IPFS, including its unique content naming and addressing using multi-hash. The article discusses the growth and adoption of IPFS, highlighting its increasing network activity and support from projects like Cloudflare and Mozilla Firefox. The advantages of IPFS, such as file integrity checks and censorship resistance, are outlined, along with challenges related to access control and participation incentives. Projects like Filecoin are mentioned as attempts to address these challenges. The paper concludes that while IPFS offers a decentralized approach to cloud storage with unique properties, further research is needed to explore its performance, privacy, and incentive mechanisms.

B. Viktor Charpentie, Tom Johansson, "Blockchain database; technical background and a reconnaissance on an implementation within the banking industry", DOI: NA

The paper investigates the emergence of blockchain technology and its potential impact on traditional transactional banking. It explores technical implementations of blockchain suitable for banking, including permissioned trust ledgers and public no-trust ledgers, and discusses the potential effects on the banking ecosystem, such as lower transaction costs, reduced settlement risks, and increased transparency for auditors and regulators. The challenges and benefits of implementing blockchain, including standardization, integration with existing infrastructure, and scalability, are examined. Privacy in ledger access is emphasized, and approaches to achieve privacy in blockchain are discussed. The potential disruption of the current transactional system and the need for consistent terminology and taxonomy in defining blockchain are also considered. The paper concludes that trusted distributed ledgers are best suited for transactional banking due to their integration with current infrastructure and privacy features. However, it acknowledges the potential of public no-trust blockchains and the demand for transparency and non-authoritarian systems, suggesting that global standardization and collaboration among participating organizations are needed for blockchain to realize its full potential. Overall, the paper suggests that while blockchain has the potential to increase the efficiency and transparency of financial markets, its widespread implementation may be delayed by the complexity and interdependence of the current banking system.

C. Leila Benarous, Benamar Kadri, Ahmed Bouridane, Elhadj Benkhelifa, "Blockchain-based forgery resilient vehicle registration system", DOI: 10.1002/ett.4237

The research paper focuses on the challenges of detecting stolen and smuggled vehicles within the context of varying jurisdictions and criticizes the inefficiencies of the current paper-based registration system. The proposed solution, Asset Guard, allows for the reporting of stolen vehicles and offers tips, but the paper argues for a more robust alternative, leading to the proposal of a blockchain-based system. This proposed system, built on a blockchain of blockchains architecture, aims to enhance security, transparency, and efficiency in vehicle registration.

The blockchain-based system involves three permissioned blockchains for customs, state, and manufacturers, with users obtaining certified keys to automate and publicly facilitate vehicle ownership transfers. The paper outlines the organization and sections of the proposed solution, including its distinction from bitcoin, its various actors, creation of genesis blocks, and different purchase scenarios. The proposed solution offers heightened security and transparency by making ledgers public, allowing any node to verify transactions. Security is evaluated using attack trees, with the proposed system shown to significantly reduce the probability of successfully registering forged vehicles compared to the current system.

The move towards paperless e-government is emphasized, with vehicle registration relying on a pair of public and private keys to ensure transaction authenticity. The paper highlights the importance of secure key safeguarding and employs an attack tree analysis to evaluate security and resilience against forgery and fake transaction injection, calculating the probability of occurrence. In conclusion, the paper presents the blockchain-based system as a secure and transparent alternative to traditional vehicle registration processes.

D. Huawei Huang, Jianru Lin, Baichuan Zheng, Zibin Zheng, Jing Bian, "When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues", DOI: 10.1109/ACCESS.2020.2979881

The research paper provides an in-depth analysis of the intersection of blockchain and distributed file systems (DFSs), focusing on challenges, layered structure, and open issues. It highlights the importance of Merkle Trees and Merkle DAGs in ensuring data integrity and explores the BitTorrent distributed file system as a crucial component for the development of blockchain-based DFSs. The layered structure of blockchain-based DFSs, including key layers such as Identity, Routing, Network, Data, Incentive, Data-Swap, and Consensus, is thoroughly discussed with a focus on specific systems like IPFS and Swarm.

The paper addresses scalability challenges due to increasing transactions and limitations in block size and consensus latency, as well as privacy challenges in blockchain-based DFSs, discussing privacy-preserving solutions and scalability performance issues. It emphasizes the need for comprehensive performance measurement and new system measurement standards for IPFS and Swarm, and highlights privacy and security issues, application issues, and the relevance of blockchain-based DFSs in addressing big data challenges.

In conclusion, the paper summarizes its key findings and emphasizes the potential of blockchain-based DFSs for next-generation websites and data-sharing platforms. It encourages further research and development in this promising domain, providing a comprehensive taxonomy of cutting-edge studies on scalability and privacy, and anticipating future advancements and contributions from the research community.

E. Hye-Young Paik, Xiwei Xu, Hmn Dilum Bandara, Sung Une Lee, Sin Kuang Lo. "Analysis of Data Management in Blockchain based Systems: From Architecture to Governance", DOI: 10.1109/ACCESS.2019.DOI

The research paper explores blockchain technology as a data store within software systems, highlighting the challenges and best practices associated with managing data on blockchains. It emphasizes the importance of evaluating architectural choices and data governance frameworks related to on-chain and off-chain data storage. The paper proposes a systematic approach for understanding blockchain as a data store and advocates for best practices in data architectures and administration. It also delves into the analytics of blockchain data and governance issues concerning data privacy and quality.

The significance of understanding how data is stored and managed on blockchains for developers and database administrators is emphasized, with recommendations for integrating blockchain technology into larger software systems. The paper suggests that a combination of on-chain and off-chain data storage may be necessary to address scalability, privacy, and cost concerns. Additionally, it explores the potential of blockchain as a system log for recording changes to application data and as a collaborative platform for distributed machine learning and model training.

Acknowledging the diversity of blockchain data and its logical models, the paper discusses the need for systematic approaches to analyze blockchain data and emphasizes the importance of data privacy and quality governance in blockchain-based systems. It proposes solutions such as fine-grained access control and blockchain oracle configuration to address privacy concerns and emphasizes the necessity of a comprehensive governance framework for blockchain-based data sharing ecosystems.

Overall, the paper provides valuable insights into the capabilities and challenges of blockchain technology as a data store, contributes to the field by proposing best practices in data architectures, data administration, blockchain data analytics, and governance of data privacy and quality, and identifies areas for further research.

F. Njoroge, Nikita Thuo, "A Blockchain-based prototype for car registration", DOI: http://hdl.handle.net/11071/12030

The research paper explores the implementation of a blockchain-based motor vehicle registration system, addressing the challenges faced by existing systems. It begins with an introduction, problem statement, and literature review covering blockchain technology and existing vehicle registration systems in India, Nigeria, and Kenya. The paper presents a blockchain use case for car registration and a public blockchain-based motor vehicle history reporting system. It also discusses blockchain-based solutions in the motor vehicle industry and various blockchain platforms. The research methodology, system design, and implementation and testing are detailed. The paper covers functional and non-functional requirements, system architecture, membership service provider, transactions, ledger, and deployment. It also provides wireframe diagrams for mobile and web applications. The system implementation and testing cover functionality, hardware and software environments, mobile application, and testing methods. The key findings and recommendations chapter discusses the research objectives and offers recommendations for further improvement and future research. In conclusion, the paper offers insights into the challenges of existing motor vehicle registration systems and presents a novel approach using blockchain technology. It provides a detailed system design and implementation process, key findings, and recommendations for future.

X. Conclusion

The article discusses the potential of implementing a blockchain storage project for vehicle documents in the transportation sector. The use of blockchain technology is expected to offer benefits such as enhanced security, privacy, and streamlined verification processes. The inherent immutability and tamper resistance of blockchain technology ensure the integrity of vehicle documents, reducing the risk of fraud and identity theft. The transparent and decentralized nature of blockchain instills trust among stakeholders and facilitates a more secure and efficient system for document storage and verification. Interoperability with existing systems allows for smooth information flow across different entities involved in vehicle-related data management, contributing to improved regulatory compliance and reduced administrative burden. Vehicle owners will have greater control over their documents, promoting transparency and ownership. Additionally, the project aims to address challenges such as scalability and privacy concerns while demonstrating innovation and technological leadership. By considering environmental sustainability through eco-friendly consensus mechanisms, the project aligns with responsible technology implementation. Overall, the blockchain storage project for vehicle documents represents a transformative step towards a more secure, efficient, and trustworthy ecosystem. It not only addresses current challenges in document management but also sets the stage for continued advancements in blockchain technology and transportation.

Acknowledgments

We immensely express our gratitude to our respected professors Mrs. Sterlin Minish T N and Ms. Mounkia S for their invaluable patience and feedback. We also could not have successfully undertaken this journey without the resources and knowledge provided by the faculty and experts from Presidency University. We are also grateful to the services provided by OpenAI for collecting resources when it seemed limited, SciSummary for digestion of scientific articles, reports and journals and summarizing them for our better understanding and services provided by Quillbot Inc for paraphrasing text and information in more professional and academic sense for better understanding and readability. Lastly, we would like to thank our friends and family as their belief has kept our spirits and motivation up high during this process.

References

Trinh Viet Doan, Yiannis Psaras, Jörg Ott, Vaibhav Bajpai, " Towards Decentralised Cloud Storage with IPFS: Opportunities, Challenges, and Future Considerations", DOI: arXiv:2202.06315v2 [cs.NI]

Viktor Charpentie, Tom Johansson, "Blockchain database; technical background and a reconnaissance on an implementation within the banking industry", DOI: NA

C. Leila Benarous, Benamar Kadri, Ahmed Bouridane, Elhadj Benkhelifa, "Blockchain-based forgery resilient vehicle registration system", DOI: 10.1002/ett.4237

Huawei Huang, Jianru Lin, Baichuan Zheng, Zibin Zheng, Jing Bian, “When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues”, DOI: 10.1109/ACCESS.2020.2979881

Hye-Young Paik, Xiwei Xu, Hmn Dilum Bandara, Sung Une Lee, Sin Kuang Lo. “Analysis of Data Management in Blockchain based Systems: From Architecture to Governance”, DOI: 10.1109/ACCESS.2019.DOI

Njoroge, Nikita Thuo, “A Blockchain-based prototype for car registration”, DOI: http://hdl.handle.net/11071/12030

Vivekkumar Sanepara, Divyesh Savani, Shyam Khokhariya, Jainam Shah, “Blockchain Application in Motor Vehicle Registration”, DOI: 10.6084/m9.figshare.12927566

Peng Kang, Wenzhong Yang and Jiong Zheng, “Blockchain Private File Storage-Sharing Method Based on IPFS”, DOI: https://doi.org/10.3390/s22145100

1.G. Wood "ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER" Ethereum project yellow paper, vol 151, Apr.2014

“A platform used for designing flowcharts and diagrams.” Available : plantuml.com

“A tool for managing multiple active Node.js versions on a single system.” Available : github.com/nvm-sh/nvm

“Registration and Licensing Services in India: Offers services related to vehicle registration and license applications in India.” Available : parivahan.gov.in

“Government Department for Vehicle Administration and Regulation: Responsible for administrating and regulating vehicles in specific regions.” Available : rtovehicleinformation.com

“Data collection with code correction and assistance”, ChatGPT Available : (openai.com)