Blockchain-based Monetization of Patient's Private Data using NFTs

Milind Mahajan
*Department of Information Technology*Pune Vidyarthi Griha's College of Engineering and Technology & G.K. Pate(Wani), Institute of Management Pune, India

Atharv Bobade
*Department of Information Technology*Pune Vidyarthi Griha's College of Engineering and Technology & G.K. Pate(Wani), Institute of Management Pune, India

Mohammedzayed Nejkar
*Department of Information Technology*Pune Vidyarthi Griha's College of Engineering and Technology & G.K. Pate(Wani), Institute of Management Pune, India

Shashank Wangkar
*Department of Information Technology*Pune Vidyarthi Griha's College of Engineering and Technology & G.K. Pate(Wani), Institute of Management Pune, India

Abstract—**Data, famously known as the digital gold of the modern world, plays a vital role in emerging sectors of the economy and in finding breakthrough solutions. But who owns it? Not the one who should. Healthcare data is sensitive in nature, and therefore important for the user to have authority over it. The paper proposes a blockchain based system and Non-Fungible Tokens (NFTs) for healthcare systems. The research particularly deals with ownership, sharing, monetization, and privacy of data, particularly patient's data. The approach here is to use NFTs to enable time bound access of patients data to third parties. The third parties are the organizations, pharma companies, scientists, or independent researchers who are willing to acquire this data for analysis and research work. The aim is to establish a system that gives control to the actual owner over his data.**

Keywords— Blockchain Technology, Ethereum, Non-Fungible Tokens (NFT), InterPlanetary File System (IPFS), Healthcare, Monetization, Private data, Data Privacy, Decentralization.

Introduction

Data in the internet world is termed as digital data. Digital data can be broadly categorized as public and private. The data that is available to the general public for view, use and modification is categorized as public data. On the other hand, data that needs to be confidential, the control of which must be restrained to the only owner and not to the general public, is termed as private data. Healthcare data in particular that includes patients' personal information, medical reports, analysis, diagnosis details has to be confidential in nature.

The traditional systems working today are client-server based which gives the control of data to the central authority. That is the data, its possession and the capacity to alter lies with the organizations [1]. In a traditional system data is stored in a centralized manner, controlled by central authority. This leads to the issue about privacy of the data, the monetization benefits and others that will be raised further.

The proposed solution aims to transform the digital data assets in the form of token that can be traded in such a manner, that the authentic owner of the data is benefited. The paper proposes the idea of decentralization, where no single entity owns the rights to govern the data or has authority to perform any operations on data. The prototype designed in the paper proposed the system where the privacy of data is maintained, monetization authority lies with the owner, achieving 'explicit' consent[2].

The Healthcare industry has a reputation for being slow to embrace change, as evidenced by the persistence of paper records in many hospitals. Interoperability is a significant concern in this industry, referring to the manner in which Health Records are exchanged, retrieved, and examined [3].

The use of Blockchain, NFTs makes it appropriate for its use in the healthcare industry to solve the concerns mentioned ahead.

The paper aims to deal with three major concerns of digital data as follows:

a. The Storage and Ownership of Data
b. Time Bound Sharing of Data
c. Monetization of Data

The remainder of the paper deals with the Literature Survey we used during our research, methodology, the concepts used in the paper, the system flow and the proposed system architecture. The end of this paper deals with Conclusion and Future Scope.

I. Literature Survey

Few methods have been put forward regarding the digital data. Some of them are mentioned ahead. A paper named "*Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability*" proposes [4] 'the idea of interoperability of healthcare data with emphasis on patient-driven and patient-mediated data exchanges'.

"*Blockchain technology applications in healthcare: An overview. International Journal of Intelligent Networks*" [5] focuses on how the healthcare system is moving towards patient centric approach for better interoperability and information exchange in healthcare system.

A review paper titled "*Blockchain Technology in Healthcare: A systematic review*" concludes that the upcoming 'research can support the pervasive implementation of Blockchain Technology to address the critical dilemmas related to health diagnostics, enhancing the patient healthcare process in remote monitoring or emergencies, data integrity, and avoiding fraud'[6].

A review paper named "*Blockchain Application in Healthcare System*", highlights the importance of access control and data integrity of clinical data. Access control is primarily a concept in cyber security which dictates who is allowed to access what and how much. Data integrity deals with maintenance of data accuracy and consistency. It argues for keeping the patient information confidential [7]. Hence playing an important role in building trust between owners and companies.

Many new methods are being developed based on the decentralized and immutability of the Blockchain based system. Many more are being contemplated. But these take into consideration individual aspects of the issue. We propose to integrate the three aspects of Ownership, Sharing and Monetization of Data, and build a holistic system that would take care of concerns of privacy, security, integrity and trust.

II. Concepts Explored and Used

A. Blockchain Technology

Blockchain technology is made of different existing technologies like cryptography, distributed systems, game theory, consensus mechanisms, peer-to-peer networking, data structures, smart contracts etc. The mixture of these technologies makes it possible to manage digital data in a way that has the ability to build a transparent ecosystem. Blockchain technology eliminates the need of third parties such as central banks or organizations that govern the data of organization's users [8].

The properties of Blockchain such as decentralized network, transparency, and immutability plays a significant role. It works as a distributed ledger and works by keeping a record of the previous transactions [9].

Blockchain being a 'zero trust network', means there is no human interaction involved in the decision making process, or any mechanism that occurs during the running network. The code is law is the philosophy of blockchain technology. It is a peer-to-peer based network which is run by all the nodes that are participating, because of this not only we have a zero trust network but also all the structural information is stored within the blockchain network [10].

B. Non Fungible Tokens

NFT stands for Non-Fungible Tokens. depict a digital certificate of authentication being created on the blockchain technology which is similar to other virtual crypto assets and currencies [11]. As suggested these are tokens that represent some real assets in tokenized form. Here we use the term 'non-fungible' denoting the one that cannot be replicated. This non-replication property makes the NFT's unique. 'They represent ownership of a unique item which is then attached to a token through the blockchain' [11]. They are cryptographic and backed by smart contracts. This technology makes it easy to validate the owner and easy transfer of the tokens.

C. Ethereum

Ethereum is a Cryptocurrency but not limited to it, as a concept of blockchain technology it is increasingly being used for developing applications and organizations, holding assets, transacting and communicating without being controlled by a central authority. Using it makes it possible for us to not hand over all our personal details to use Ethereum - we keep control of our own data and what is being shared [12].

D. Interplanetray File System

IPFS i.e. Interplanetary File System is a 'peer-to-peer distributed file system'[13]. IPFS is not built on Blockchain but rather is designed to work together with existing Blockchain protocols. Unlike IPFS, Blockchain is not suitable for storing vast quantities of data.IPFS is used to store data that is publicly accessible and Blockchain is used to verify the addresses [14].

E. dApp

Decentralized applications—also known as dApps or dapps—are digital applications that run on a blockchain network of computers instead of relying on a single computer [15]. They are decentralized in the sense they cannot be controlled or interfered by any single user. dApps have the potential to store and monitor medical records, as well as promote communication and teamwork among healthcare practitioners.

F. Ceramic Protocol

Ceramic Protocol is a decentralized protocol that facilitates the creation, sharing, and retrieval of open data on the Web3.0 or decentralized web. The protocol is constructed on top of IPFS, a distributed file system that enables storing and sharing of files, and Ethereum, a blockchain platform that enables the development of decentralized applications and smart contracts. It offers a decentralized and tamper-resistant approach for storing and accessing data on the web, which empowers developers to create applications that require robust and trustworthy data storage.

G. Metamask

MetaMask is a software tool available as a browser extension and mobile application that permits users to access and engage with the Ethereum blockchain and its accompanying decentralized applications (dapps). MetaMask serves as an intermediary between the user's web browser or mobile device and the Ethereum blockchain, providing a secure connection that enables them to securely participate in the blockchain and dapps without running a complete Ethereum node. This simplifies the process of accessing and utilizing dapps, as it does not necessitate advanced technical skills or intricate setup processes.

III. Methodology

The paper proposes solving traditional data privacy issues with a decentralized platform. In a centralized traditional system we found no existing solution that together tries to solve data ownership, sharing and monetization problems. The main sector or industry where all these aspects are highly concerned when it comes to data privacy of users is the healthcare industry.

Patients are becoming more aware of their entitlement to own their data, and they are exercising caution accordingly. The ideal scenario is for patients to have the ability to receive and authenticate their medical records and details, such as x-ray scans and genomic sequences, without any other entity claiming ownership or gaining access without the patient's consent. As medical reports or patient data embodies all the aspects of data ownership, sharing and data monetization, we are using patient data as a user data for prototype in this research paper.

IV. System Flow

All the entities (end users) interacting with the system (as shown in Figure. 01) can be classified into 3 categories: Patient, Hospital and Consumer. The patient is the primary user of the system whose data will be used to generate reports. The Hospital is the entity responsible for producing the medical report. Consumer is the third party interested in buying the license of the reports for the research and analysis purposes. End users will interact with the system through frontend of the application by registering as one of the user. The system will grant the role to the user at the time of registration.

Medical tests will be performed on the patient as prescribed by the hospitals which are registered and verified by the system. Once the Patient transfers the price for the test to the system, the hospital will generate the medical reports, encrypt them to prevent any information leak, and upload it to the IPFS (Decentralized Storage). IPFS sends original reports to the re-encryptors (oracle service) with re-encryption keys. Re-encryptors will re-encrypt the reports sent by the IPFS and upload the re-encrypted reports back to the IPFS. IPFS will send a copy of re-encrypted medical reports to the patient. Patient then confirms receiving the copy of re-encrypted reports and pays an oracle fee to the system and the system will distribute the fee to the oracles as a reward for verifying and re-encrypting the original

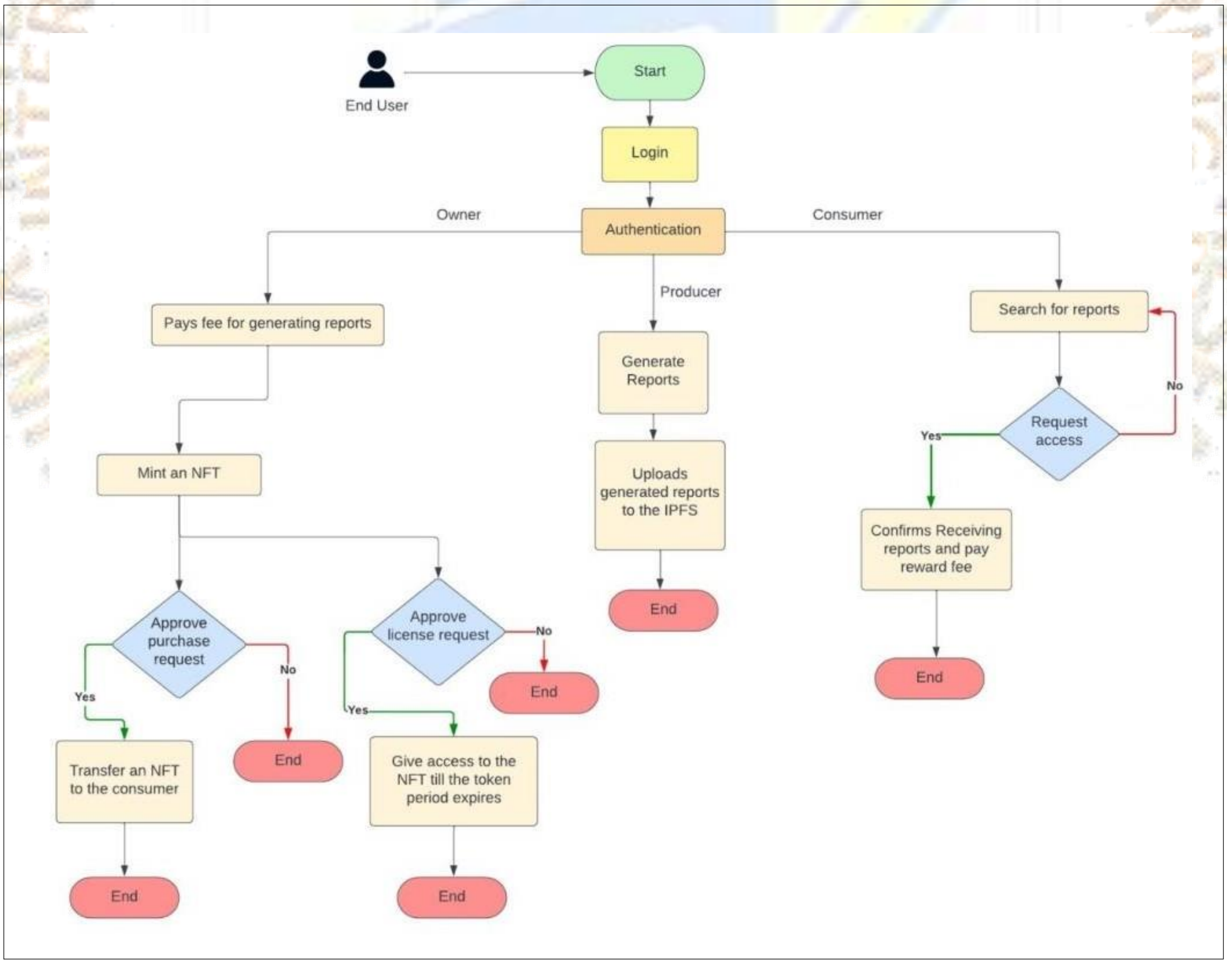

End User
Start
Login
Owner
Authentication
Consumer
Producer
Pays fee for generating reports
Generate Reports
Search for reports
Request access
Yes
No
Mint an NFT
Uploads generated reports to the IPFS
Confirms Receiving reports and pay reward fee
End
Approve purchase request
Yes
No
Approve license request
No
Yes
End
End
Transfer an NFT to the consumer
End
Give access to the NFT till the token period expires
End
End

Figure 01 - The System Flow

medical reports.

The working of backend logic starts with ContenSC (smart contract code) once the patient has the re-encrypted medical reports. Patient will then mints (the process of converting piece of data to the NFT's) the medical reports to the NFT's using ContentSC logic. After minting NFT's patient has the option to put it on sale in the NFT marketplace or to keep it to himself. This functionality or feature of NFT's gives the sense of ownership to the patients.

Minted NFT's will be available to buy or access for a limited time on the NFT marketplace for consumers. Consumers can query as per their requirements on the marketplace and can request to buy ownership of NFT for lifetime or can request license for a limited time period. If the patient or the owner of the NFT, approves the request of the consumer to sell NFT, the consumer will pay the amount set by an owner and ownership of the NFT will be transferred to the consumer. Once the owner confirms the payment, then consumer will be having the control over the content of NFT which he can use for his own purposes or can resell for profit. If owner of NFT approves the request for license for accessing NFT for limited period of time, the consumer can access the NFT content for that particular time period till the token gets expired. Once the license token gets expired the access of the NFT will be revoked from the consumer as the ownership of NFT still lies with the primary owner of the NFT. The time bound sharing of NFTs is only applicable where the data is dynamically produced and streamed to the third party.

V. System Architecture

Below mentioned is the following Architecture of the system for time bound sharing and monetization of Private data using Blockchain and NFT's. The system comprises the following components as shown in figure 02: User Interface, Smart Contract, Off-chain Oracles and Decentralised Storage.

A. User Interface

The end user will interact with the system through the user interface (Front-End). This interaction will take place through the dApp and the decentralized storage. The end user can be categorized into 3 major roles: Producer, Owner and Consumer.

- *Producer* - Generates medical reports
- *Owner* - Mints medical reports to NFT's
- *Consumer*- Tradeoffs (buy/sell) NFT's

B. Smart Contract

Smart Contract acts as a backend logic for blockchain applications. It can be understood as a code running on a blockchain network. Smart contracts are immutable in nature , hence cannot be changed once deployed on the network. Without the need of an intermediary, they help in automatic execution of agreements.

The prototype proposed in the paper involves dividing the blockchain tasks into two distinct smart contracts. The initial contract, named ContentSC, enhances the ERC721 NFT protocol by introducing exclusive attributes for every NFT, access controls based on user accounts, and management of Ether transfers. The second contract, OracleSC, manages off-chain oracles, offering both on-chain and off-chain services, while also keeping track of the participation and reputations of the oracle nodes.

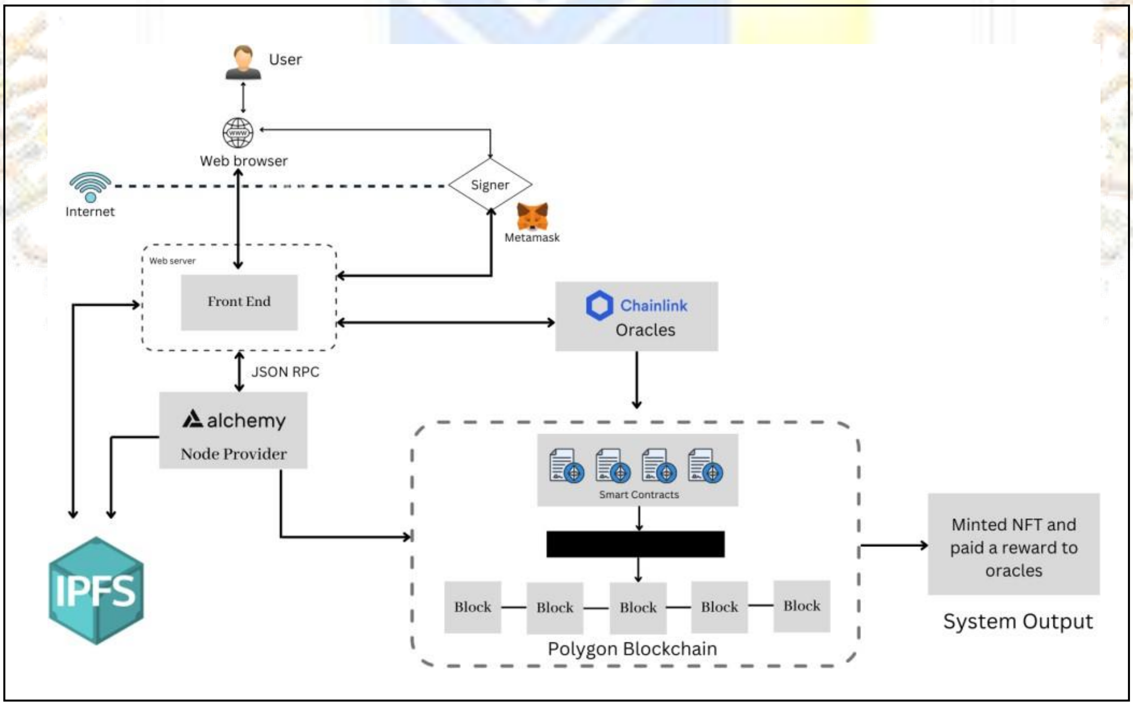


Figure 02 - The System Architecture

C. Off-chain Oracles

Off-chain oracles help blockchain applications in expanding their capabilities by exchanging the real world data with the on-chain data. Oracles helps in performing a lot of heavy operation outside the network which helps in saving gas cost.

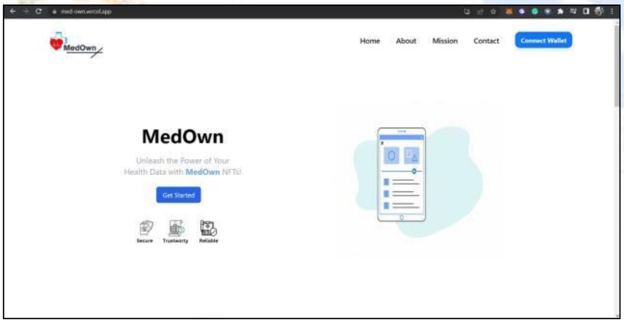
To ensure oracles correctly perform their tasks, we incorporate trust models as a logical interface in OracleSC. The trust models do not oversee the interactions between end-users and oracle nodes instead, alternative methods are employed to encourage correct actions, such as requesting collateral payments. Furthermore, OracleSC forbids oracles from engaging in multiple requests. By locking oracles, they are prevented from being involved in a large number of requests that they may not be willing or able to fulfill.

D. Decentralised Storage

Although critical to the system, the decentralized storage component operates as an unmanaged entity. In a decentralized storage solution, the two essential functions are the ability to add and publish content assets. Adding a content asset generates a content-addressable URL, which makes it impossible to update the asset on the same URL, while publishing an asset results in a fixed URL that points to the latest version of the asset. These core capabilities are provided by the IPFS network. However, IPFS does not offer any monetary incentives, which means it lacks the assurance to store content for extended periods. To address this concern, Filecoin incorporates monetary incentives based on proof-of-storage into IPFS.

VI. Graphical User Interface

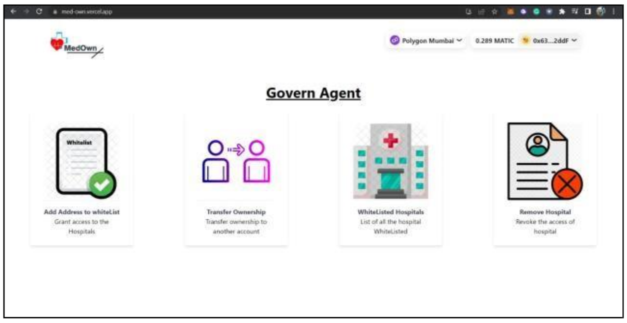
A graphical user interface (GUI) is a type of user interface that allows users to interact with electronic devices, such as computers or mobile devices, through graphical elements such as icons, windows, and buttons, rather than using text-based commands.



MedOwn

Unleash the Power of Your Health Data with MedOwn NFTs!

Figure 03 - Main Page



Govern Agent

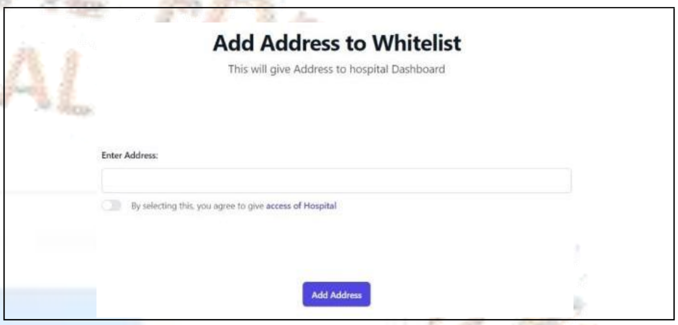
Add Address to whiteList
Grant access to the Hospitals

Transfer Ownership
Transfer ownership to another account

WhiteListed Hospitals
List of all the hospital WhiteListed

Remove Hospital
Revoke the access of hospital

Figure 04 - Government Agent Dashboard



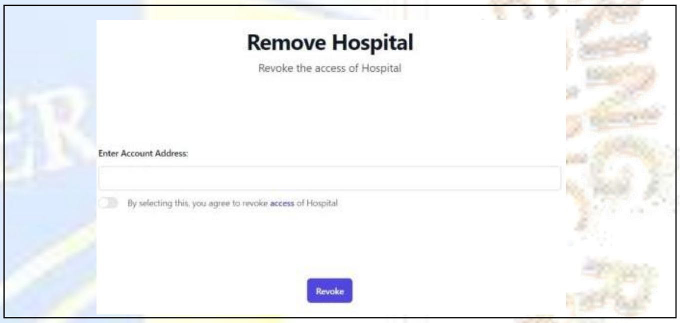
Add Address to Whitelist

This will give Address to hospital Dashboard

Enter Address:

By selecting this, you agree to give access of Hospital

Figure 5 - Interface for Government Agent to whitelist Hospitals



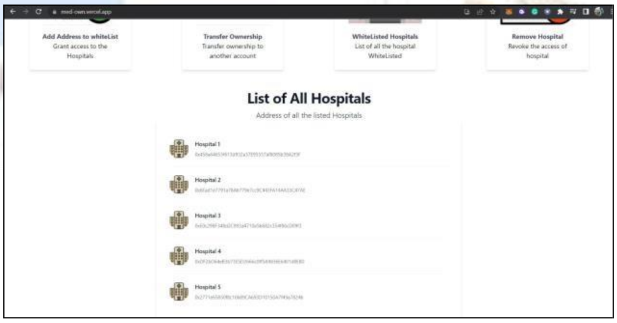
Remove Hospital

Revoke the access of Hospital

Enter Account Address:

By selecting this, you agree to revoke access of Hospital

Figure 6 - Interface for Government Agent to remove Hospital



Add Address to whiteList
Grant access to the Hospitals

Transfer Ownership
Transfer ownership to another account

WhiteListed Hospitals
List of all the hospital WhiteListed

Remove Hospital
Revoke the access of hospital

List of All Hospitals

Address of all the listed Hospitals

Hospital 1
[illegible]

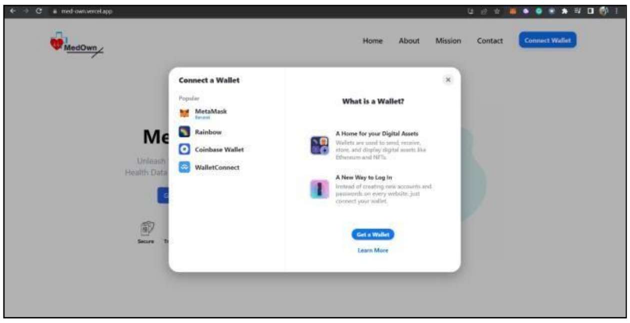
Hospital 2
[illegible]

Hospital 3
[illegible]

Hospital 4
[illegible]

Hospital 5
[illegible]

Figure 7 - Shows the List of All Government approved Hospitals



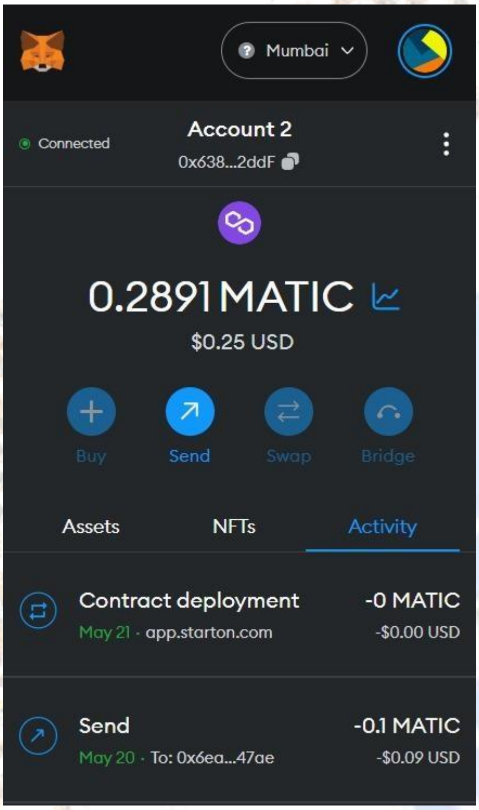
A Home for your Digital Assets

Wallets are used to send, receive, store, and display digital assets like Ethereum and NFTs.

A New Way to Log In

Instead of creating new accounts and passwords on every website, just connect your wallet.

Figure 08 - Use of wallet



Connected

Account 2

0x638...2ddF

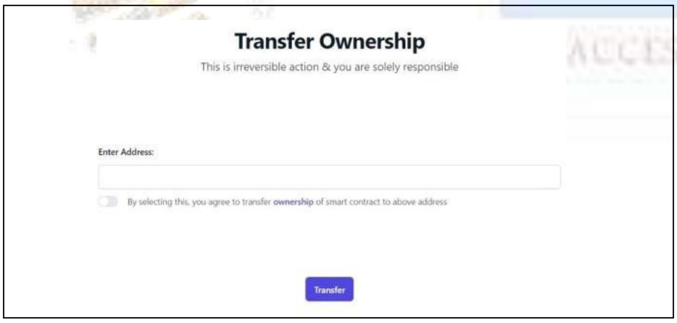
0.2891 MATIC

$0.25 USD

Contract deployment — May 21 · app.starton.com — -0 MATIC — -$0.00 USD

Send — May 20 · To: 0x6ea...47ae — -0.1 MATIC — -$0.09 USD

Figure 09 - Metamask



Transfer Ownership

This is irreversible action & you are solely responsible

Enter Address:

By selecting this, you agree to transfer **ownership** of smart contract to above address

Figure 10 - Interface for Transfer of Ownership

VII. Conclusion

Time-bound sharing and monetization of private data using blockchain and NFTs offer a novel solution to the problem of data privacy and ownership. By leveraging blockchain's decentralized and immutable nature, users can have greater control over their data and choose how and when to share it. NFTs provide a way to monetize private data by allowing users to tokenize and sell access to their data. Moreover, time-bound sharing of data ensures that data is only shared for a specific period, after which access is revoked. This adds an extra layer of security and ensures that private datais not available indefinitely. However, there are still challenges to overcome, such as the development of a robustinfrastructure and standards for NFTs, and addressing the ethical and legal concerns surrounding the ownership and monetization of private data. Despite these challenges, time-bound sharing and monetization of private data using blockchain and NFTs hold great potential for transforming the data economy, putting users in control of their data and enabling them to benefit from its value.

VIII. Future Scope

The proposed system is of significant use in the sector of health care. It can be used as an integrated mechanism to store health records and regulate the health data.

The Government of India has drafted a National Health Policy in 2017, with the goal to streamline the electronic health records of individuals with ease of access, by standardizing and controlling the overall data retrieving process and protecting users' rights[9]. This could be envisaged as a blockchain-based healthcare system.

References

[1] M. Madine, K. Salah, R. Jayaraman, A. Battah, H. Hasan and I. Yaqoob, "*Blockchain and NFTs for Time-Bound Access and Monetization of Private Data*," in *IEEE Access*, vol. 10, pp. 94186-94202, 2022, doi: 10.1109/ACCESS.2022.3204274.

[2] Health Research Board, 2021, "*Explicit Consent*", url: https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-health-research/consent/explicit-consent/#:~:text=Explicit%20consent%20in%20GDPR&text=The%20Article%2029%20Working%20Party,an%20express%20statement%20of%20consent.

[3] American Medical Association, "*What is Information Blocking*",url: https://www.ama-assn.org/system/files/2021-01/information-blocking-part-1.pdf.

[4] William J. Gordon, Christian Catalini, "*Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability*", 2018. Doi: https://doi.org/10.1016/j.csbj.2018.06.003.

[5] Abid Haleem, Mohd Javaid, Ravi Pratap Singh, Rajiv Suman, Shanay Rab, ScienceDirect, "*Blockchain technology applications in healthcare: An overview. International Journal of Intelligent Networks*", doi: https://doi.org/10.1016/j.ijin.2021.09.005

[6] Huma Saeed, Hassaan Malik, "Blockchain Technology in Healthcare: A systematic review", 21 April 2022, doi: https://doi.org/10.1371/journal.pone.0266462.

[7] Pranto Kumar Ghosh, Arindom Chakraborty, Mehedi Hasan, et al, "*Blockchain Application in Healthcare Systems: A review*", 2023, doi: https://doi.org/10.3390/systems11010038.

[8] OECD, "Opportunities and Challenges of Blockchain Technologies in Health Care", December 2020.

[9] Dr. R. Sriram,Parth Gupta, "*Blockchain in Indian healthcare system*", 22 January 2020.

[10] R. Aroul Canessane, N.Srinivasan, Abinash Beuria, et al, "*Decentralised Applications Using Ethereum Blockchain*", doi: https://doi.org/10.1109/ICONSTEM.2019.8918887.

[11] Yashika Nagpal, "*Non-Fungible Tokens (NFT's): The Future of Digital Collectibles*", doi: https://doij.org/10.10000/IJLMH.111984.

[12] Ethereum, url: https://ethereum.org/en/.

[13] Morteza Alizadeh, Karl Andersson and Olov Schelen. "*Efficient Decentralised Data Storage Based on Public Blockchain and IPFS.*", doi: https://doi.org/10.1109/CSDE50874.2020.9411599.

[14] Kaspar Triebstok, 03 May 2018, "How IPFS is Challenging the Web as We Know It."

[15] Jake Frankenfield, Jefreda R. Brown, Michael Logan, January 09, 2023, "*Decentralised Applications (dApps): Definition, Uses, Pros and Cons*"