# Secure Health Record Management System using Blockchain & IPFS

| | | |
|---|---|---|
| Mukesh.M | - | 732120104030 |
| Sathish.M | - | 732120104310 |
| Sureshkumar.S | - | 732120104311 |
| Vivin Shankar.P.J | - | 732120104315 |

Guide:

Mrs.D.Mohanapriya

# ABSTRACT

- Most of the hospitals store their patient's data locally and some even do not have any backup storage. This poses a real threat of data loss or data corruption.

- The traditional database practices is that they often misplace or mix the patient's data, which, needless to say, have severe complications.

- Many researchers are working on IPFS and Blockchain technology to improve the storage of medical records.so, implementation of the IPFS and Blockchain based healthcare secure storage solutions.

- This model proposes two-factor authentication and multi-factor authentication for preventing fake node attacks.

# INTRODUCTION

- In today's world, healthcare data access is restricted to only few stake-holders like hospitals, healthcare providers, insurance companies and research organizations.

- The data should be available to patients and ,they can access to health data and their control rights provided from admins.

- Blockchain has the potential to facilitate healthcare organizations in addressing these issues by maintaining a decentralized ledger of patients' health data in a distributed manner.

- This improves trust in the system and data integrity. This access management using blockchain can ensure that data is accessed only by authorized individuals and no one else can view it stealthily.

# EXISTING APPROACH

❑ **Cloud-Based Health Record Management Systems:**

- These systems store patient data on remote servers maintained by third-party vendors.
- Cloud-based Health Records offer Scalability, accessibility from any location with an internet connection, and automatic updates without requiring on-site hardware maintenance.

❑ **Client-Server Health Record Management Systems :**

- In this approach, the Health Records software is installed on a local server within the healthcare facility, and users access it through client applications installed on their devices.
- Client-Server Health Records provide more control over data security and customization but may require significant initial investment in hardware and maintenance.

# DISADVANTAGES IN EXISTING APPROACH

- Medical data intervention is always possible because the existing system is a centralized distributed system.

- In the existing system there are drawbacks such as no data privacy, less reliability and lack of network security in sharing the health record among the cloud servers.

- Also failure in single point can happen in existing system which results in unavailability of data.

- It also lacks in data retrieval process since the existing system faces storage issues.

# PROPOSED APPROACH

❑ Patient's data must be stored in IPFS which ensures the benefit of being dispersed and immutability of records and hash of the record only must be stored in Blockchain.

❑ Symmetric key encryption (AES-192) is used for encrypting data before storing into IPFS. Asymmetric encryption (RSA-4096) is used for generating digital envelopes to pass on symmetric key to authorized entities.

❑ The proposed framework for off-chain storage of health data using IPFS saves blockchain structure from scalability issues.

❑ Hashing of the encrypted data is done using SHA-256 algorithm. Proposal for blockchain integration with IPFS helps preserve privacy in the healthcare system, making it highly secure, scalable and robust.

# ADVANTAGES IN PROPOSED APPROACH

- **Confidentiality and Access control:** Technical measures must be adopted to keep health records inaccessible and/or unintelligible for parties that have no permission to gain any knowledge about them.
- **Decentralized Storage:** Decentralized storage ensures that patient data is stored across a network of nodes rather than in a central repository, reducing the risk of privacy breaches.
- **Faster Data Access and Recovery:** Because of using IPFS as the storage system, the CID (content identity) is used to access and recover data stored across the peer to peer network. It is way more better than the centralized storage system.
- **Anonymity:** Research organizations may handle health records, under patient consent, during the realization of studies (e.g., public health research), provided that the records are anonymized beforehand.
- **Emergency access:** In order to maintain a patient’s health condition stable, the regulations provide that health records from the patient may be accessed by healthcare collaborators without patient consent within emergency scenarios.

# APPLICATIONS

❑ **Healthcare Industry:**

**Hospitals and Clinics:** Facilitates secure storage and sharing of patient health records, streamlining healthcare processes and enhancing interoperability. -

**Pharmaceutical Companies:** Enables secure and transparent management of clinical trial data and drug development records.

❑ **Insurance Providers:**

**Health Insurance Companies:** Enhances the efficiency of claims processing by providing secure access to relevant health records.

❑ **Research and Development:**

**Medical Research Institutions:** Facilitates secure sharing and access to research data, ensuring the integrity and authenticity of findings.

**Pharmaceutical Research:** Enables secure storage and sharing of research data related to drug discovery and development.

# APPLICATIONS (Contd...)

- **Identity Verification Services:**

  **Identity Management Platforms:** Leverages blockchain for secure and verifiable storage of personal health information, contributing to secure identity verification processes.

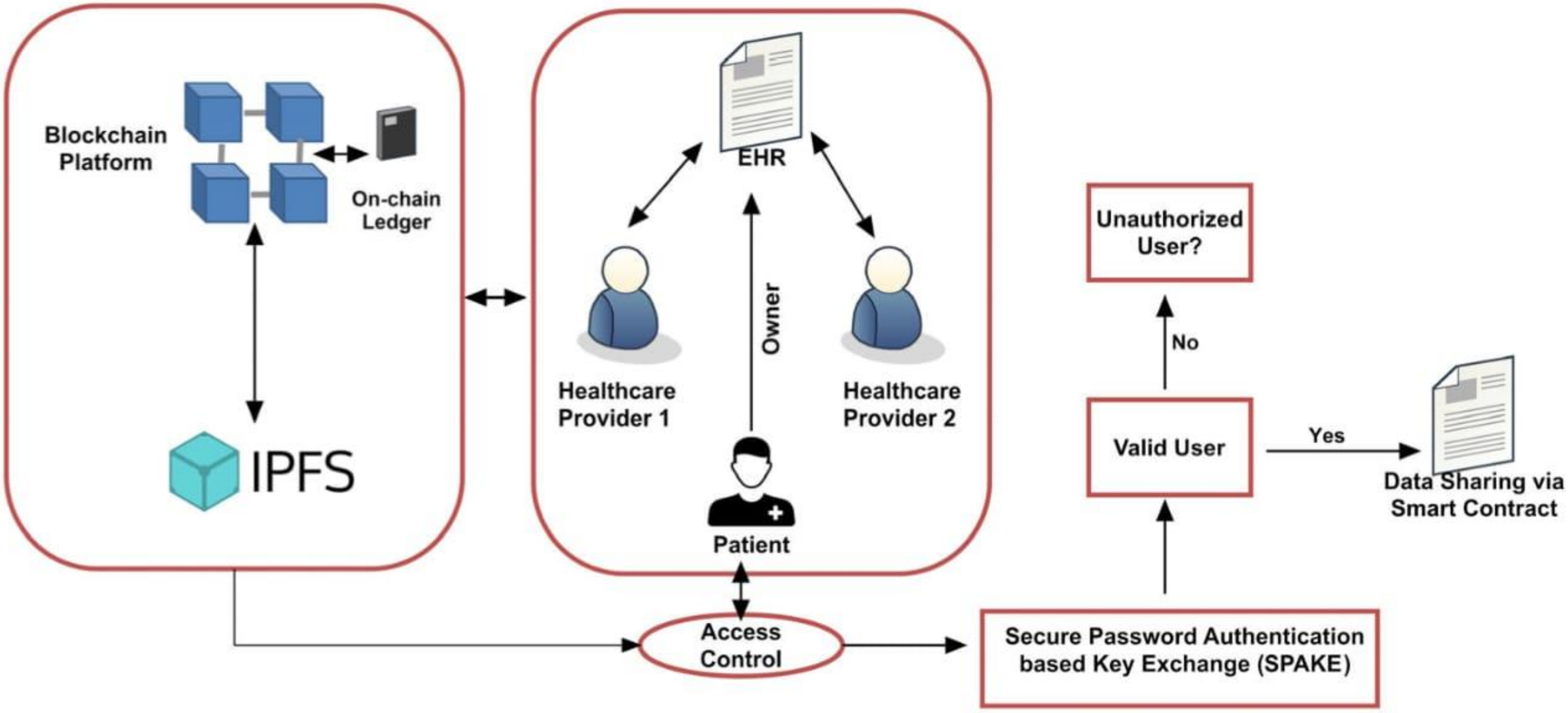
- **Education and Training:**

  **Medical Training Institutions:** Utilizes secure health records for training purposes, allowing students to access real-world medical cases securely.

- **Personal Health and Fitness:**

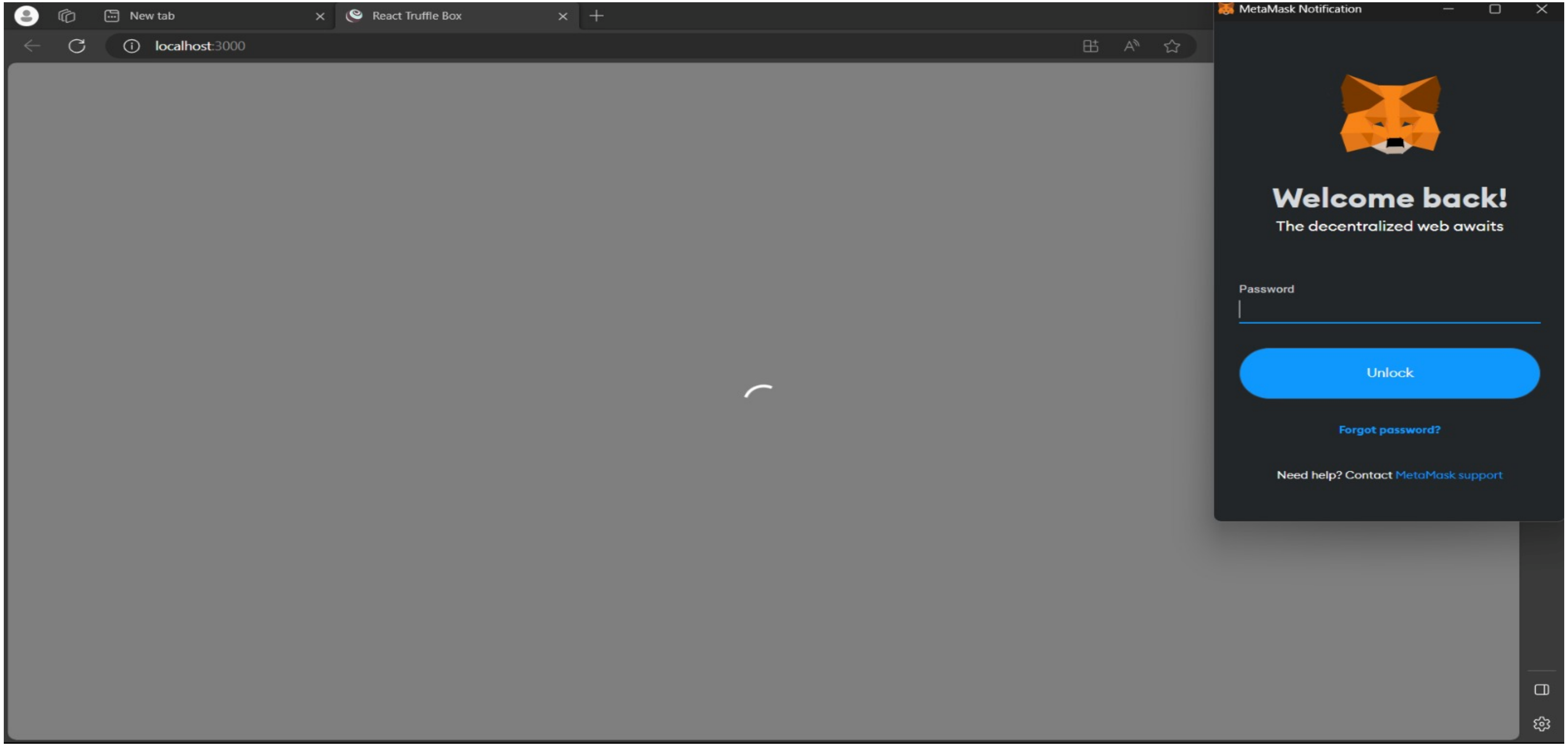
  **Fitness Apps and Devices:** Integrates with secure health record systems to provide users with a comprehensive view of their health and fitness data.

# BLOCK DIAGRAM



# MODULE 1

1. Wallet Recognition
2. User Authentication
3. Admin Authentication
4. Admin Portal
5. Doctor Registration
6. Confirmation of Doctor Registration
7. Doctor Authentication



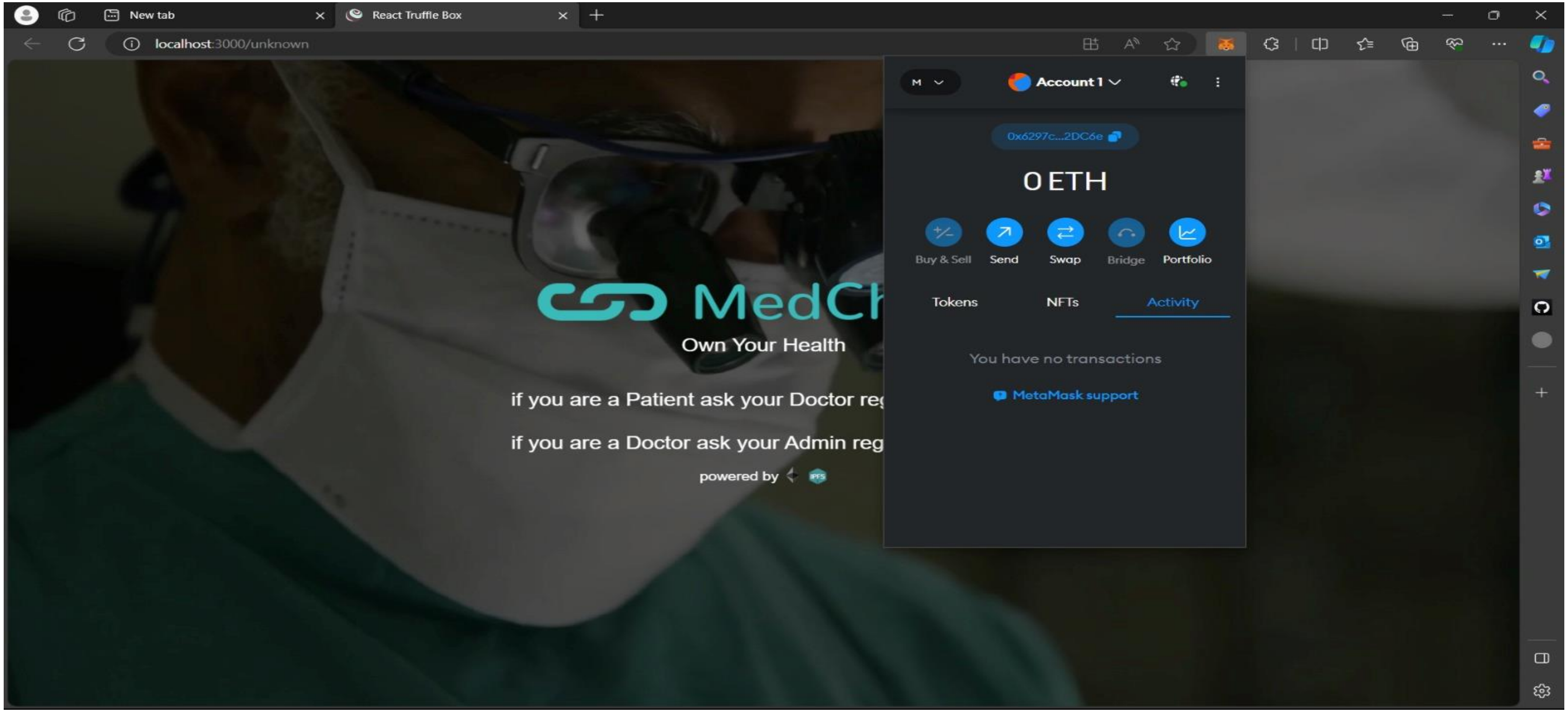
Welcome back!

The decentralized web awaits

Password

Need help? Contact MetaMask support

1.Wallet Recognition



Own Your Health

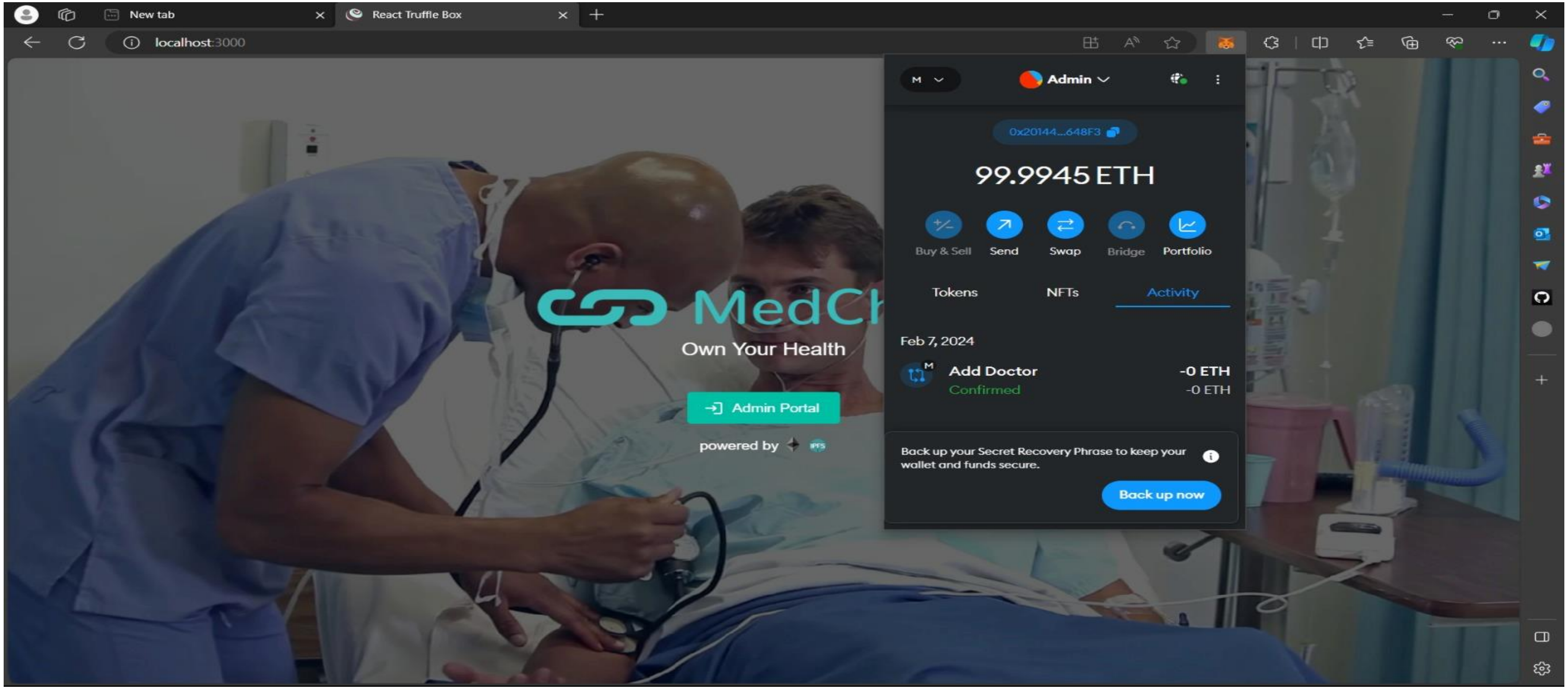
if you are a Patient ask your Doctor reg

if you are a Doctor ask your Admin reg

powered by

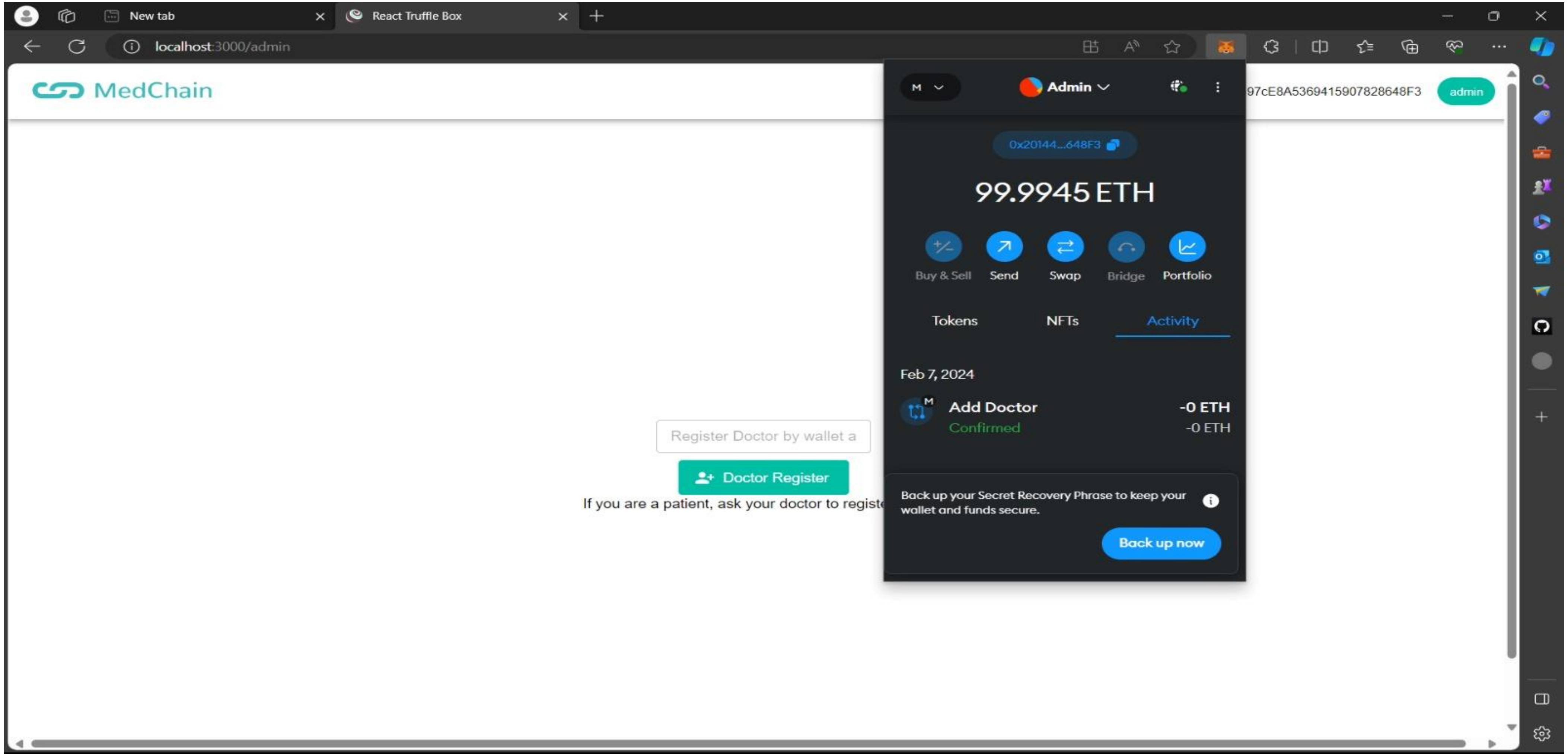
You have no transactions

2.User Authentication



Back up your Secret Recovery Phrase to keep your wallet and funds secure.

3.Admin Authentication



Register Doctor by wallet a

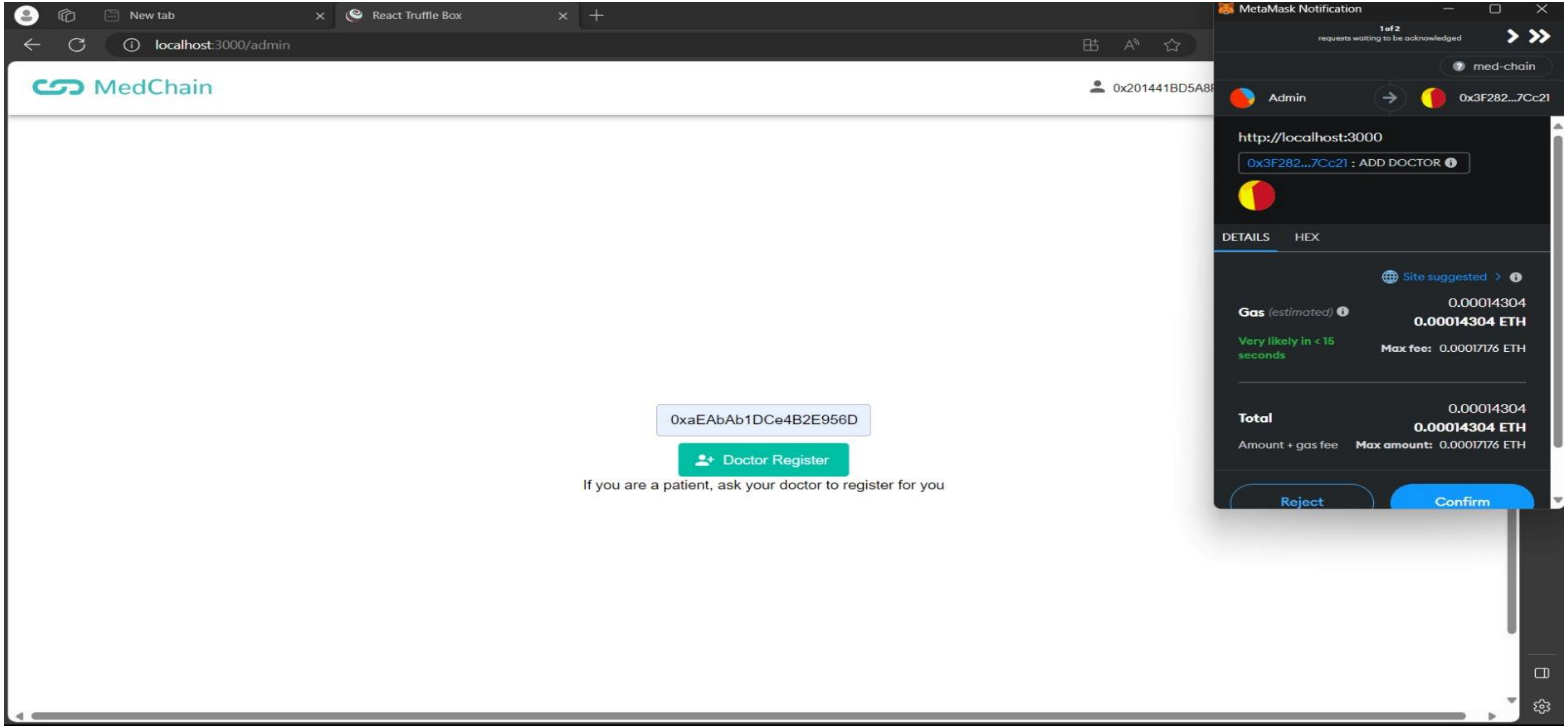
If you are a patient, ask your doctor to registe

Feb 7, 2024

Add Doctor -0 ETH
Confirmed -0 ETH

Back up your Secret Recovery Phrase to keep your wallet and funds secure.

4.Admin Portal



localhost:3000/admin

0x201441BD5A8F

1 of 2
requests waiting to be acknowledged

med-chain

Admin → 0x3F282...7Cc21

http://localhost:3000

0x3F282...7Cc21 : ADD DOCTOR

Site suggested

Gas (estimated) 0.00014304
0.00014304 ETH

Very likely in < 15 seconds Max fee: 0.00017176 ETH

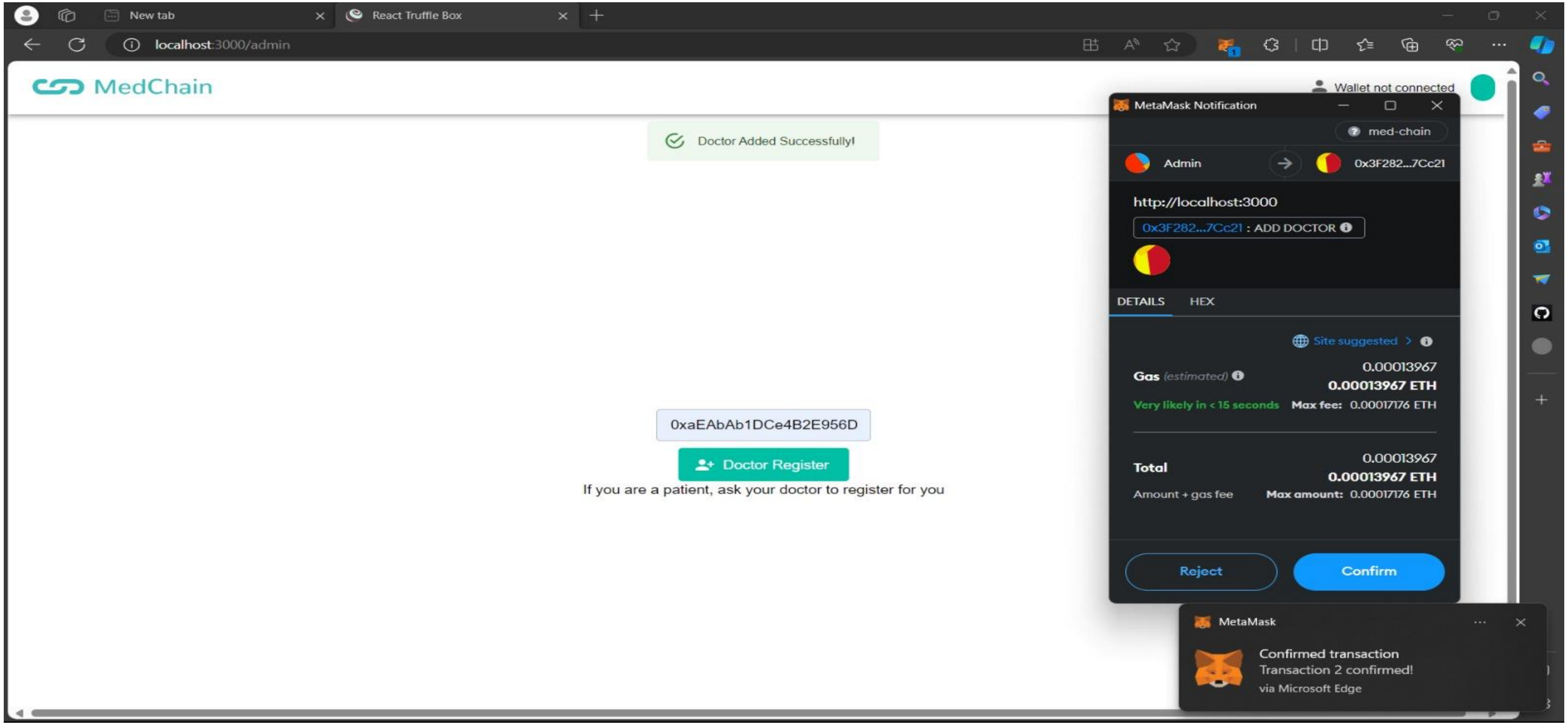
Total 0.00014304
0.00014304 ETH

Amount + gas fee Max amount: 0.00017176 ETH

0xaEAbAb1DCe4B2E956D

If you are a patient, ask your doctor to register for you

5.Doctor Registration



Doctor Added Successfully!

0xaEAbAb1DCe4B2E956D

If you are a patient, ask your doctor to register for you

http://localhost:3000

0x3F282...7Cc21 : ADD DOCTOR

Gas (estimated) 0.00013967 0.00013967 ETH

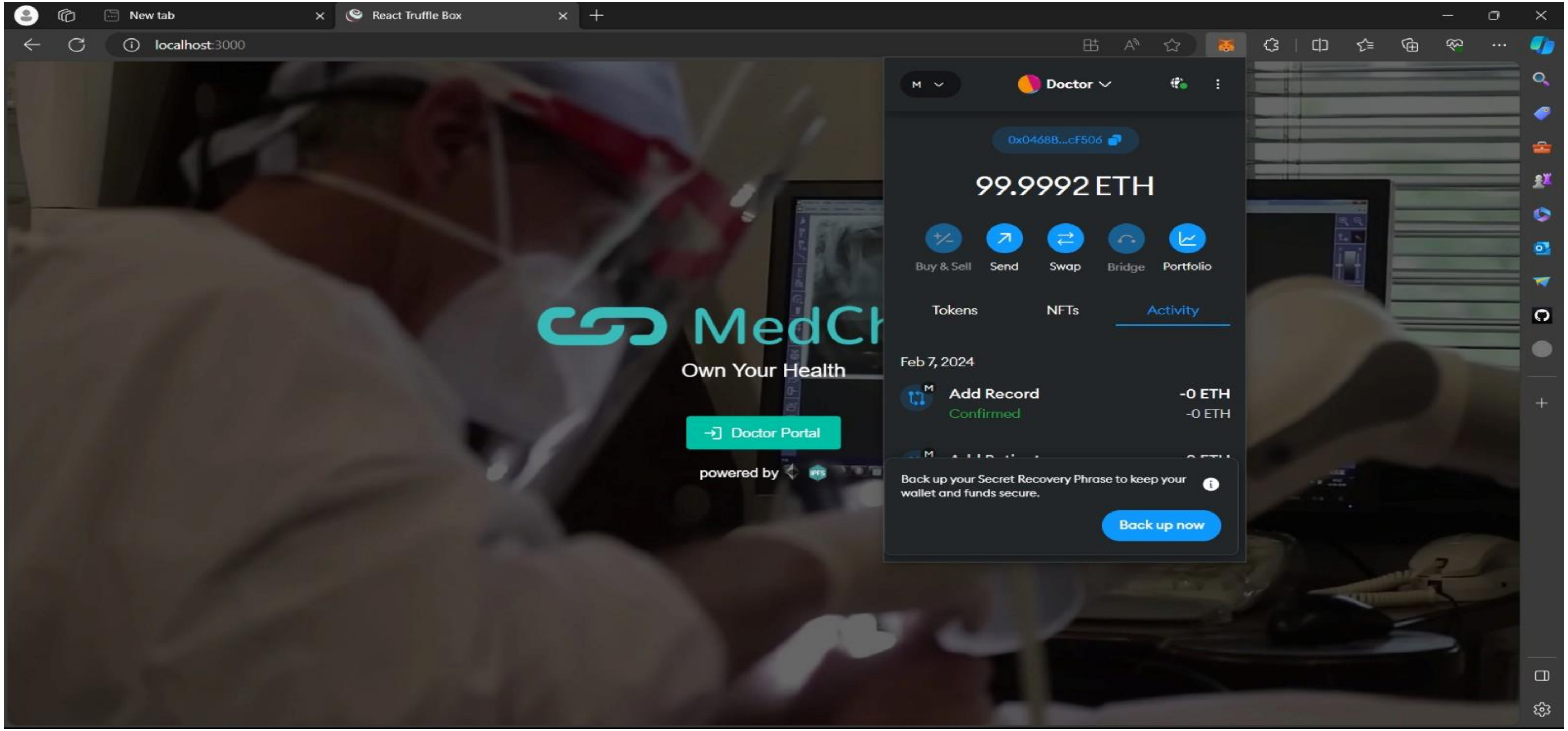
Very likely in < 15 seconds Max fee: 0.00017176 ETH

Total 0.00013967 0.00013967 ETH

Amount + gas fee Max amount: 0.00017176 ETH

Confirmed transaction
Transaction 2 confirmed!
via Microsoft Edge

6.Confirmation of Doctor Registration



Feb 7, 2024

Add Record -0 ETH
Confirmed -0 ETH

Back up your Secret Recovery Phrase to keep your wallet and funds secure.

7.Doctor Authentication

# LITERATURE SURVEY

❑ V. Vijayakumar, M. K. Priyan, G. Ushadevi, R. Varatharajan, G. Manogaran, and P. V. Tarare, ‘‘E-health cloud security using timing enabled proxy re-encryption,’’ Mobile Netw. Appl., vol. 24, no. 3, pp. 1034– 1045, Nov. 2022.

❑ I. Abunadi and R. Kumar, ‘‘BSF-EHR: Blockchain security framework for electronic health records of patients,’’ Sensors, vol. 21, no. 8, p. 2865, Apr. 2021.

❑ M. Zghaibeh, U. Farooq, N. U. Hasan, and I. Baig, ‘‘SHealth: A blockchain-based health system with smart contracts capabilities,’’IEEE Access, vol. 8, pp. 70030–70043, 2020.

❑ H. Qiu, M. Qiu, M. Liu, and G. Memmi, ‘‘Secure health data sharing for medical cyber-physical systems for the healthcare 4.0,’’IEEE J. Biomed. Health Informat., vol. 24, no. 9, pp. 2499–2505, Sep. 2020.

# E-Health Cloud Security using Timing enabled Proxy Re-encryption

- ❑ E-health cloud security using timing-enabled proxy re-encryption (TPRE) refers to the application of cryptographic techniques to enhance the confidentiality and integrity of healthcare data stored in the cloud.

- ❑ In this context, "e-health" refers to the use of electronic information and communication technologies in healthcare, and "cloud security" pertains to safeguarding sensitive medical information stored and processed in cloud-based environments.

# Blockchain Security Framework for Electronic Health Records of Patients

- ❑ The integration of blockchain technology into the healthcare sector has garnered significant attention due to its potential to address critical issues related to the security, privacy, and interoperability of electronic health records (EHRs).

- ❑ Blockchain, a decentralized and tamper-resistant distributed ledger, provides a promising framework for enhancing the security and integrity of patient data in electronic health records.

- ❑ This introduction outlines the key motivations, challenges, and objectives of implementing a blockchain security framework for patient EHRs.

# A blockchain-Based Health System with Smart Contracts Capabilities

- ❑ The intersection of blockchain technology and healthcare has given rise to innovative solutions aimed at addressing longstanding challenges in the industry.

- ❑ One such groundbreaking concept is the development of a blockchain-based health system with smart contract capabilities.

- ❑ This introduction provides an overview of the motivations, potential benefits, and key features of such a system, highlighting how it could revolutionize the management and delivery of healthcare services.

# Secure Health Data Sharing for Medical Cyberphysical Systems for the Healthcare

- The emergence of Healthcare 4.0, marked by the integration of cyber-physical systems (CPS) and advanced technologies, presents unprecedented opportunities for enhancing patient care, improving operational efficiency, and advancing medical research.

- However, the realization of these benefits hinges on the secure sharing of health data within the intricate framework of medical cyber-physical systems.

- This introduction explores the imperative for secure health data sharing in the context of Healthcare 4.0, emphasizing the challenges and potential solutions that underpin this transformative paradigm.

# THANK YOU