

tech racers

Racing your ideas to reality

ROR, Node, Angular, Ember, Meteor, iOS & Android.

CASE STUDY

PATIENTORY– A Healthcare Peer-to-Peer EMR Storage Network

CONTENT

- ABSTRACT
- ABOUT PATIENTORY
- THE BUSINESS REQUIREMENTS
- SYSTEM OVERVIEW
- BLOCKCHAIN SOLUTION
- INTEROPERABILITY IN BLOCKCHAIN
- KEY FEATURES OF PATIENTORY
- PROJECT CHALLENGES
 - USER ONBOARDING AND EHR ACCOUNT PAIRING
 - MITIGATING THE ISSUE OF SINGLE POINT OF FAILURE
- TOKEN EXCHANGE SYSTEM
- PROPOSED
- TECH STACK
- TECHRACERS INPUTS
- END RESULT
- ABOUT TECHRACERS

TECHRACERS – CASE STUDY: PATIENTORY

A HEALTHCARE PEER-TO-PEER EMR STORAGE NETWORK

I. ABSTRACT

Patientory is blockchain powered health information exchange (HIE) platform that uncovers the true value of interoperability and cybersecurity. This system intends to eliminate the friction and costs of current third-party intermediaries when considering population health management.

The storage network promises improved data integrity, reduced transaction costs, decentralization and disintermediation of transparency and trust.

A patient-centered protocol supported by blockchain technology, patientory direct the healthcare stakeholders to manage electronic medical data and interact with clinical care teams.

II. ABOUT PATIENTORY

Patientory is a patient-centered enterprise solution designed to eliminate several areas of concern in the existing centralized healthcare ecosystem and allows Health IT infrastructures to cope with the ever-changing trends in Healthcare management.

Patientory is supported by blockchain technology to ensure end-to-end encryption whilst adhering to regulatory guidelines and compliance requirements. Built on cutting-edge technology and years of practical application, the major focus of Patientory is privacy and anonymity and how it is being applied to data sharing. This ensures that only the authorized parties have the access to the data as the patient is not just the sole ethical responsibility but also a legal mandate.

III. THE BUSINESS REQUIREMENTS

- The client wanted solutions that can ensure cyber security and facilitate the secure transfer of patient information from one provider to another. With the integration of blockchain technology, Patientory intends to ensure secure health information transmission via smart contracts.
- To create a flexible care model tailored to include patients' multi-faceted health and wellness needs
- The client's vision is to empower patients, clinicians, and healthcare organizations to safely access, store and transfer information, thus improving care coordination while ensuring data security.
- Their offerings are focused on transforming the sickness management mindset to a wellness lifestyle mindset.
- The intention is to bring together a network of health information providers to ensure improvement in the quality of wellness outcomes, whilst reducing the reducing associated care cost.
- Also, to incentivize different participants in the network to pro-actively create better care regimes in a transparent blockchain powered network.
- To create a token-based payment system to support the entire infrastructure for the foreseeable future

TECHRACERS – CASE STUDY: PATIENTORY

A HEALTHCARE PEER-TO-PEER EMR STORAGE NETWORK

IV. SYSTEM OVERVIEW

The Existing Health Information Exchange model of the commercial space does not have the provision for the patients to make a profit from sharing the information, it is usually not seen as an entity but rather a simple data sharing activity.

In most of the frameworks, the typical Health Information Exchange activity falls into both HIO and HIE definitions. Here, the data link sold to the purchases (internal or outside organizations) is not patient-centric because the model does not benefit the patients.

Moreover, most information providers often are reluctant to share the data as they fear that the information being shared might give others a competitive edge.

V. BLOCKCHAIN SOLUTION

These current issues are solved using the Patientory Blockchain Network. Legacy EMR is centralized structures subject to hacking, strict security regulations, and onerous overhead costs. By implementing the Patientory Blockchain infrastructure, providers will see minimized breaches due to the inherent access control properties of the system; a channel for facilitated care coordination with results in overall improvement in health outcomes.

Cross-institutional sharing of this critical patient information allows the care providers to avoid usual medication errors which result in decreased duplicate testing. Blockchain technology is effective to track and timestamp all the activities related to the Health Information Data and provides an immutable audit trail whilst ensuring the updated version of the record is put to use.

Also, the blockchain makes it possible for the providers to establish a positive belief that the procedures and technical infrastructure they are providing are backed with security and minimal interruptions.

VI. INTEROPERABILITY IN BLOCKCHAIN

EHR systems in a blockchain network are based on an isolated credential validation architecture where the health information is kept in separate organized systems. The information access right from the principal provider to other organizations is only possible via limited capability, it can only be Read, Submitted, to Forwarded or Notified.

In order to establish an interoperable health IT environment, maintaining the standards are particularly critical in these areas of EHR technology:

- How the applications are networking with the users
- How different systems are communicating with each other
- How the information is being processed and managed
- How IoT devices integrate with systems and the healthcare applications

TECHRACERS – CASE STUDY: PATIENTORY

A HEALTHCARE PEER-TO-PEER EMR STORAGE NETWORK

Furthermore, in a blockchain network, the Patient/Consumer interaction is very limited as the entire system is transparent. Once a blockchain and its smart contracts are configured, the parameters become absolute. The patient becomes the primary intermediary in sending and receiving health information. Since blockchain records are immutable and stored across all participating users, recovery contingencies are unnecessary. Moreover, blockchain's transparent information structure is capable to prohibit many data exchange integration points and tedious reporting activities.

VII. KEY FEATURES OF PATIENTORY

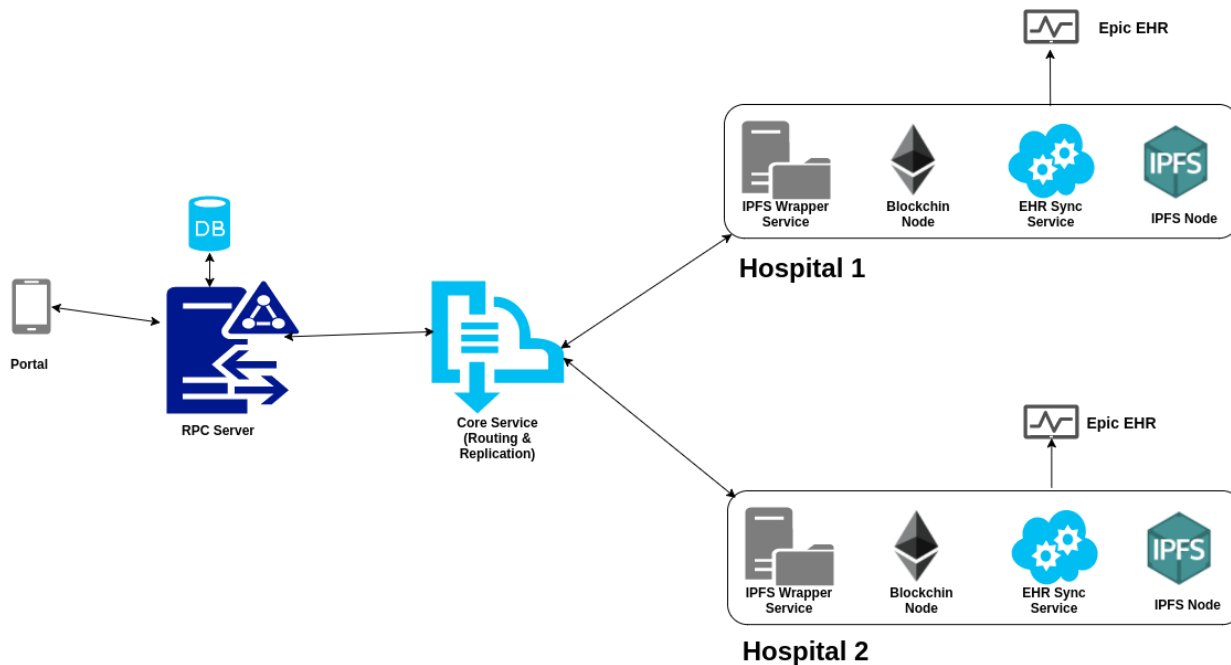
- Allows patients to instantly access their health information.
- Allows hospitals to store patient information on the secure blockchain and run their node
- AI-powered technology stores data onto the blockchain network
- Patients are able to interact with the blockchain via a mobile app which enables access and provides features such as messaging
- Coordinated patient care via a blockchain HIE essentially alleviates unnecessary services and duplicate tests
- The patients or users can buy tokens from main public Ethereum Blockchain as per their storage needs
- Can be interconnected with any EHR system and enable doctors, care providers and everyone in the ecosystem to communicate on a single easy to use platform
- Encrypted middleware to meet the high-volume demands of modern day Health IT
- APIs with Electronic Health Records for fast medical information transfer
- HIPAA-compliant protected health information storage that adheres to region-specific regulatory guidelines
- Use Big Data to gain valuable insights for clinical care teams with actionable analytics

VIII. PROJECT CHALLENGES

- It was required to fetch the database from the existing EHRs which belong to the providers, in order to do so we worked on the third-party front to carry out the EHR synchronization.
- Since blockchain supports data privacy to strengthen the privacy of EHRs, we used HIPAA compliance so as to prevent the data leak.
- There were no public nodes so we had to run a private blockchain. We used Quorum blockchain node (private) only to connect with hospital systems.
- This also runs on every hospital infrastructure and each instance of it connects with the existing EHR System of hospital Like Epic through a wrapper service(Sansoro) to fetch all the data files. Here, each instance only connects with one EHR System. It fetches data files of all registered patients in the background, encrypts all data files and further takes steps to get the file stored on IPFS and then writes the IPFS hashes of files in the blockchain.

TECHRACERS – CASE STUDY: PATIENTORY

A HEALTHCARE PEER-TO-PEER EMR STORAGE NETWORK



User onboarding and EHR Account pairing

- The user provides his mobile number on the Patientory app and the app sends the mobile number to RPC Server.
- RPC Server requests Core Service to find out if a patient record exists on any of the Hospital EHR Service.
- Core Service connects with one of the Patientory Hospital Infrastructure to find such user inside. The Patientory infrastructure EHR-Sync service connects with Hospital EHR System and tries to find a user. If found it returns the patientID to Core Service and Core Service returns the patientID to RPC Server.
- RPC Server generates a registration_reference_id and sends it to the mobile device. Along with it, an SMS OTP is also sent to the provided mobile number.
- Now Patientory app will send registration_reference_id and OTP to the RPC server.
- RPC server now verifies the OTP and registration_reference_id, if it gets verified RPC will send signup_reference_id to the Patientory app.
- Now to register the user on the Patientory, the mobile app will generate a 12-word mnemonic and let user note it down somewhere safe.
- With the mnemonics, the device will generate following things
 - ECDSA public/ private key pair along with wallet address
 - RSA public/private key pair

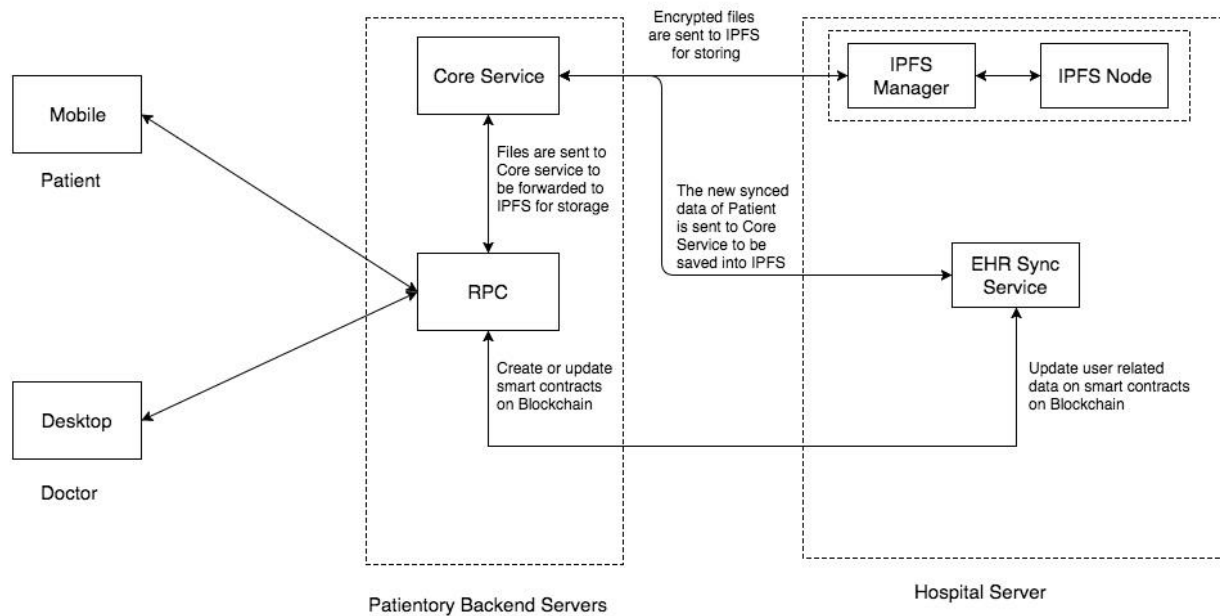
TECHRACERS – CASE STUDY: PATIENTORY

A HEALTHCARE PEER-TO-PEER EMR STORAGE NETWORK

- RSA private key will be encrypted with 12-word mnemonics using AES encryption. Let's call it encryptedRSAPrivateKey.
- ECDSA private key will be encrypted with 12-word mnemonics using AES encryption. Let's call it encryptedECDSAPrivateKey.
- Now the wallet address will be treated as data and the signature for this data will be generated using ECDSA Private key. Let's call this signature ecdsa_verification_signature.
- Similarly, treating wallet address as data, another signature will be generated using RSA private key let's call it rsa_verification_signature.
- Now the device will send the following things to RPC Server.
 - signup_reference_id
 - Wallet Address
 - ECDSA Public Key
 - RSA Public Key
 - encryptedECDSAPrivateKey
 - encryptedRsaPrivateKey
 - ecdsa_verification_signature
 - Rsa_verification_signature
- RPC Server will validate everything sent by the device by matching signatures and SMS OTP with registration_reference_number.
- If all validations go well, RPC Server will now again fetch the patientID by performing the same steps mentioned in point 2 and 3.
- Now RPC Server will generate a transaction (Using RPC-Server-Private-Key) for blockchain that will create a new instance of User Smart Contract that will have all the details including patientID encrypted_private_keys etc. and will set the owner of this contract to the address provided by the mobile device.
- RPC Server will create a user record on Postgres database.
- access_token and refresh_tokens will be generated and will be sent to the user device.
- In the background, RPC Server will faucet the user wallet with few ethers to allow the user to perform actions on his Smart Contracts.
- Now user needs to grant permission to one of the Hospitals (Currently there is only one) to write user data on his FileVault Smart Contract. To do so the device will call an API with the wallet address of hospital and the RPC Server will generate a raw transaction on the behalf of a user and will be sent back to the user device.
- On the device, this raw transaction will be signed with user's ECDSA private key and will be sent to RPC Server.
- RPC Server will forward this signed transaction to blockchain and on being mined the hospital will get the write permission to user *FileVault Smart Contract*.

TECHRACERS – CASE STUDY: PATIENTORY

A HEALTHCARE PEER-TO-PEER EMR STORAGE NETWORK



Mitigating the issue of single point of failure

We ran multiple instances of RPC Server Service, Core Service, and the Postgres was also run in a distributed manner with master-slave configurations.

Things Hosted on the Patientory Infrastructure

- **RPC Server**
Serves the main APIs for registration, listing files, downloading files, authentication etc.
- **Core Service**
This service will handle the Replication of files on multiple hospitals, Routing of requests from RPC server to proper Hospital Infrastructure.
- **Postgres Database RPC Server**
Serves as a persistent layer for access tokens and intermediate data for user onboarding and pairing.
- **Postgres Database RPC Server**
Serves as a persistent layer for hospitals infrastructure list and RPC server client id and secrets for communication between RPC and Hospitals Infrastructure.

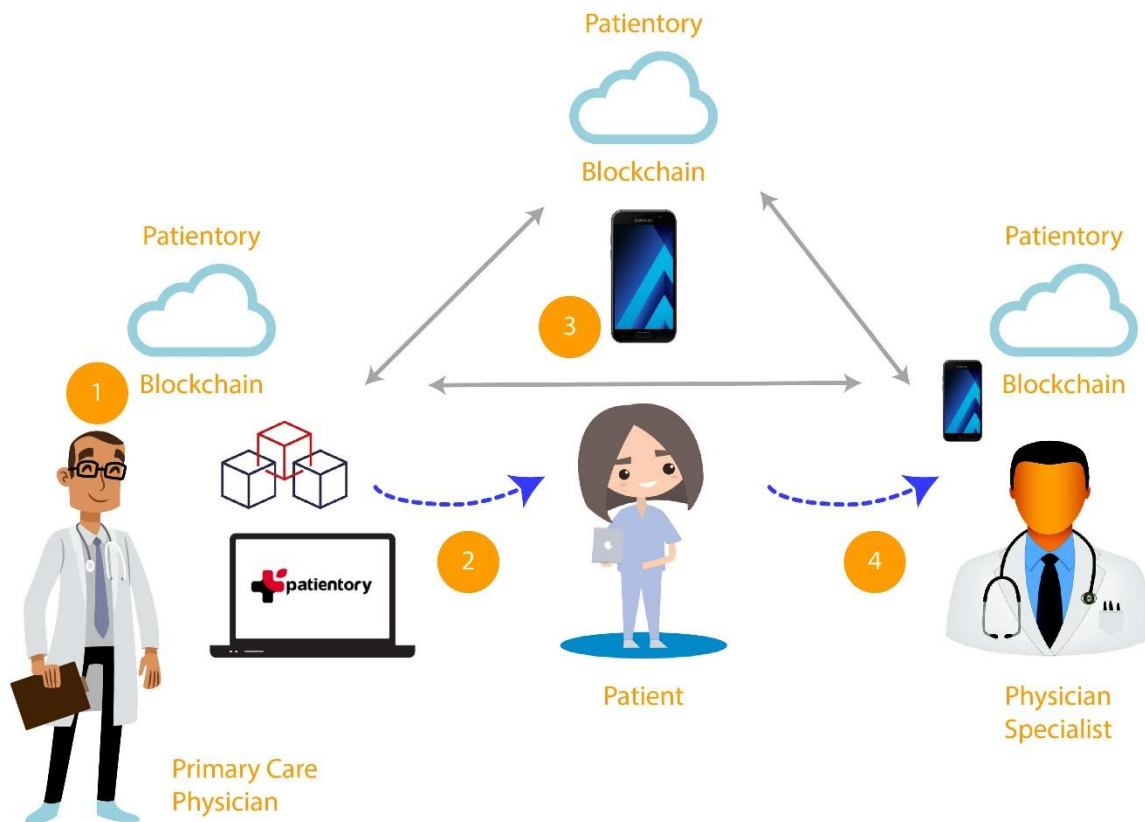
TECHRACERS – CASE STUDY: PATIENTORY

A HEALTHCARE PEER-TO-PEER EMR STORAGE NETWORK

IX. TOKEN EXCHANGE SYSTEM

PROPOSED

- The Patientory model renders the ability for information seeker to transfer tokens as incentives to healthcare information providers when both the parties agree upon certain criteria to activate the smart contract.
- This exchange will likewise provide the much-needed “carrot” to the providers (patients) and engage them in a symbiotic collaboration
- Henceforth, Patientory issued tokens (PTOY), is the native token of the platform. In exchange for these PTOY tokens, users will be able to use the network to rent health information storage space and to execute health specific smart contract payments and transactions.



TECHRACERS – CASE STUDY: PATIENTORY

A HEALTHCARE PEER-TO-PEER EMR STORAGE NETWORK

X. TECH STACK

- Modified Ethereum
- Custom IPFS
- NodeJS
- Postgres
- React
- Swift
- Java

XI. TECHRACERS INPUTS

- Helping build the entire blockchain enabled backend solution
- Following a microservice architecture with services built in NodeJS
- Using a private fork of Ethereum with a consensus mechanism that allows up to 400 transactions per second
- Building a wrapper over IPFS for a custom replication algorithm that factors in parameters like geographical location, the reputation of the node, latency etc.
- Building a smart contract layer in solidity for access and permission control
- Building mobile end SDKs for iOS and Android that does:
 - Generation of private keys via mnemonics
 - Symmetric and asymmetric encryption/decryption of large files on the device
- Dockerization of all services for a one-click deployment

XII. END RESULT

The future of health information sharing is a vibrant ecosystem of different tokens, for which healthcare will need a closed loop payment system in place. The result is a blockchain powered efficient care cycle management which will develop trust among different parties involved in HER. Also, it will direct the mHealth industry towards ethical business practices thereby eliminating healthcare payment fraud and information breach.

The current HIE architectures come short of enabling several abilities, thus, our services helped Patientory to create a business model that facilitates granting or receiving tokens. Also, the client was able to fix the inefficiencies in the existing HIE ecosystem.

TECHRACERS – CASE STUDY: PATIENTORY

A HEALTHCARE PEER-TO-PEER EMR STORAGE NETWORK

XIII. ABOUT TECHRACERS

Techracers is a dedicated blockchain and crypto-advisory services company that provides customized services to developing blockchain technology companies worldwide. Our tailored services help organizations to accelerate the integration and implementation of blockchain technology into their growth plans. We are the warhorses of the niche technologies like *RoR*, *Node*, *Angular* and other battlefields of Information Technology. Our team of polished experts is capable of providing cutting-edge blockchain solutions based on business requirements and individual insights.

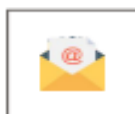
TO TAKE A STEP AHEAD



+1 801 405 6334



sales.techracers1



sales@techracers.com