viral communications

MedRec: Medical Data Management on the Blockchain

MedRec applies blockchain smart contracts to create a decentralized content-management system for your healthcare data, across providers

by Ariel Ekblaw and Asaf Azaria

Apr 11, 2016 *1* *11* *7*

Abstract: Electronic Medical Records (EMRs) crave innovation. Years of regulation have stifled tech development in medical data management, while an array of incompatible back-end sy limit patients' ability to engage with their medical history. We demonstrate MedRec as a solution tuned to the needs of patients, the treatment community, and medical researchers. MedR contracts to create a decentralized content-management system for your healthcare data, across providers. The MedRec authentication log governs medical record access, while providing sharing. A modular design integrates with providers' existing, local data storage solutions, enabling interoperability and making our system convenient and adaptable. As a key feature of c research community with an integral role in the protocol. Medical researchers provide the "mining" necessary to secure and sustain the authentication log on a private, Ethereum network, medical metadata in the form of "transaction fees."

Our Motivation & Approach

From fragmented access to comprehensive access

Patients interact with a staggering number of health care providers through the course of their lives-- from pediatrician, to university physician, dentist, employer health plan provider, spe they leave data scattered across a particular jurisdiction's system [1]. This leads to a fragmented data trail and decaying ease of access, as providers often retain primary data stewardship (explicit legal provisions in over 21 states) [2].

Our MedRec prototype enables patients with one-stop-shop access to their medical history across multiple providers: smart contracts on an Ethereum blockchain [3] aggregate data point that are stored elsewhere) into "patient-provider relationships." These contract data structures are stored on the blockchain and associate references to disparate medical data with owners and record retrieval location. This provides an immutable data-lifecycle log, enabling later auditing. We include a cryptographic hash of the record in the smart contract to establish a base thus provide a check against content tampering. The raw medical record content is never stored on the blockchain, but rather kept securely in providers' existing data storage infrastructure

MedRec facilitates reviewing, sharing and posting of new records via a flexible user interface, designed to reflect best-practices from the Blue Button health record competition. We abstrac to focus on usability for the medical record use case. The interface includes a notifications system to alert users when a new record has been posted on their behalf or shared with them.

From data rigidity to data sharing

Interoperability challenges between different provider systems pose significant barriers to effective data sharing. Patients face hurdles in authorizing data exchange (with other consulting members) due to the lack of a common interface or standard system that orchestrates record access across databases. MedRec provides streamlined data sharing functionality by updating relevant data pointers. With pointers to patient data aggregated in smart contracts on the blockchain, we can offer a single, common interface where patients chose when, and with whom,

From obscurity to clarity

While most valuable to the patient and provider, medical records also prove critical for research. A recent report from the Office of the National Coordinator for Health Information Techn and public health researchers "require the ability to analyze information from many sources in order to identify public health risks, develop new treatments and cures, and enable precision trickles through to researchers from clinical studies, surveys and teaching hospitals, we note a growing interest among patients, care providers and regulatory bodies to responsibly share n care for others.

With MedRec, we incentivize medical researchers and other healthcare stakeholders to participate in the blockchain network as "miners" (see Appendix: Bitcoin Basics for more on mining blockchain). These researchers can now obtain greater clarity in their investigations by earning census level, anonymized metadata in return for contributing the computational resources t enables the emergence of data economics between data consumer and data producer, as the system supplies big data to empower researchers while engaging patients and providers in the release.

Designing for patient agency

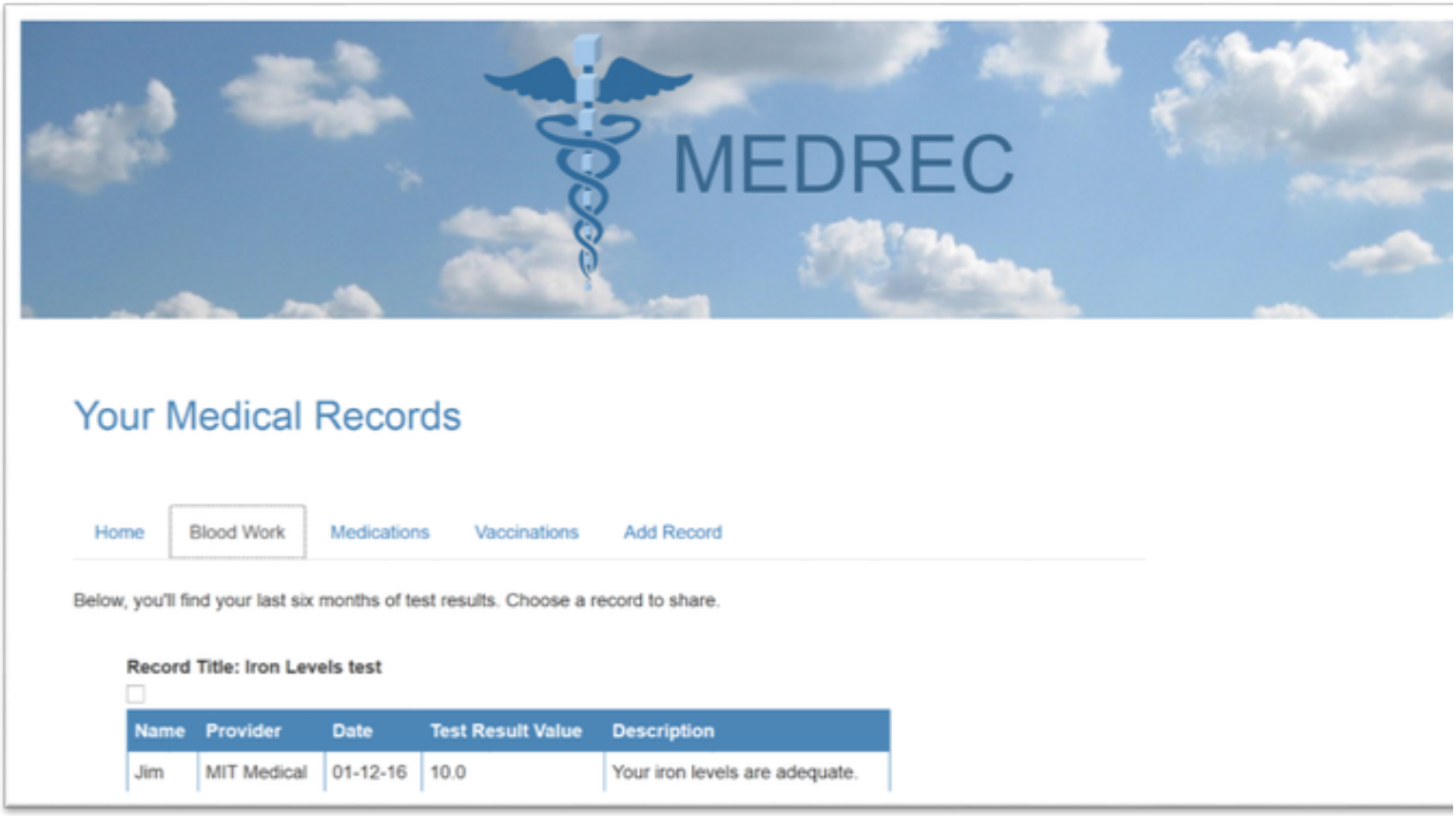
When designing new systems to overcome current EMR challenges, we must prioritize patient agency. Patients benefit from a holistic, transparent view of their medical history, and in the media, patients are increasingly willing, able and desirous of managing their data on the web and on the go [1]. MedRec restores patient agency by empowering users with a focal point for history, and an easy mechanism for sharing their data across medical jurisdictions. Patients can authorize a new doctor to review their record and obtain a second opinion, or grant viewer Grandparents can seamlessly share medical data with their families, to reduce the mystery of family health history. Furthermore, the authorization log persists in the distributed network, restore functionality. Patients can leave and rejoin the system multiple times, for arbitrary periods, and regain access to their history by downloading the latest blockchain from the networ

Summary of MedRec contributions:

- Comprehensive, immutable log of authentication permissions for ease of data access and auditing
- Data sharing authorization, with off-blockchain content syncing
- Interoperability with providers' existing data storage infrastructure
- Blockchain mining incentives for medical researchers via anonymized metadata rewards
- Custom API for handling smart contract content and posting to a private, Ethereum blockchain
- Intuitively designed user interface for patient and provider use

MedRec Highlights

User Interface

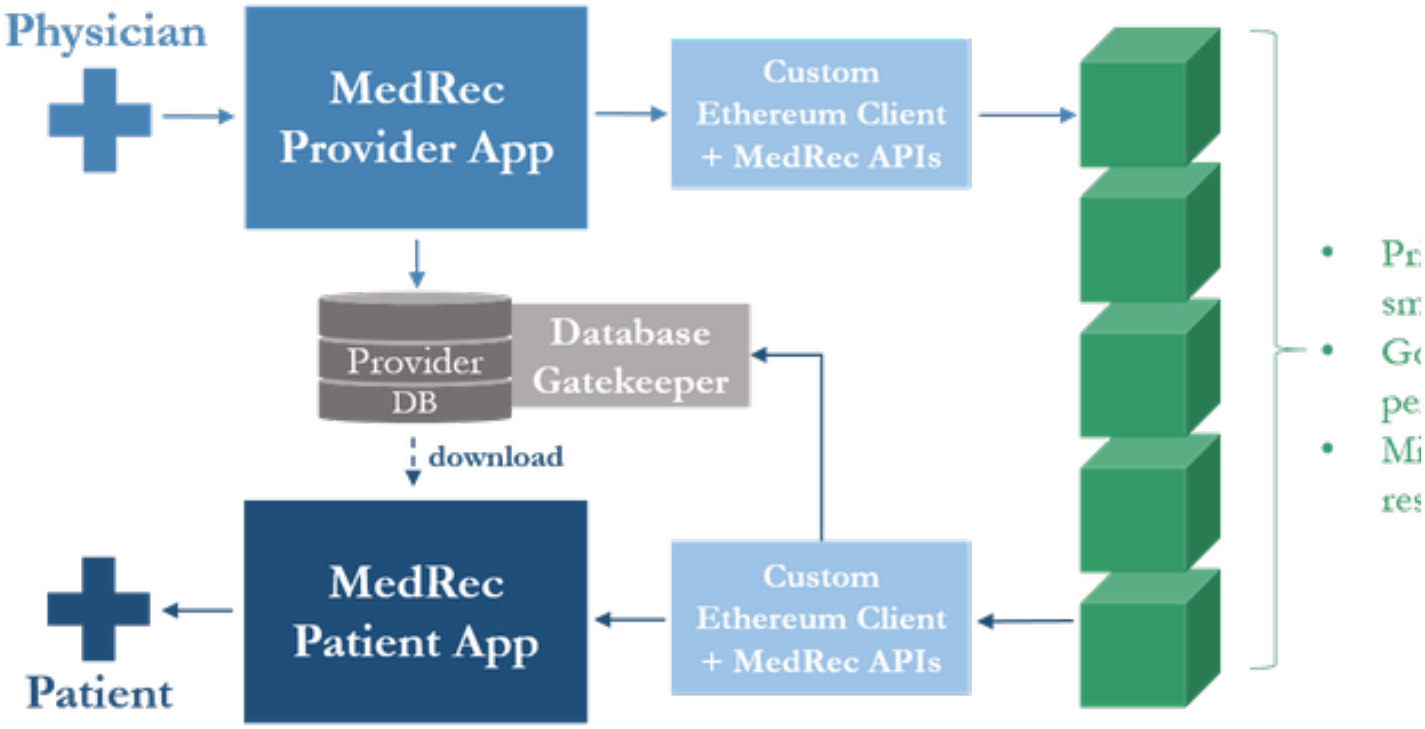


A screenshot from the MedRec prototype, showing the patient view. Patients can select multiple records to review and share, or add their own record to report symptoms an

Database Gatekeeper

Our Database Gatekeeper functions both as a local, distributed authentication server and a content-syncing service. Each local version of the Gatekeeper listens for incoming data query re retrieve data from their provider's database). The requests are cryptographically signed by the requester, allowing the Gatekeeper to confirm identities. Once the requester signature is veri blockchain Patient-Provider contract referenced in the request to determine if the identity in question has been authorized for data viewership. If the request is approved, the Gatekeeper r requester and allows a sync with the local database.

System Architecture



This use case example begins with a physician adding a new record through the MedRec Provider App. The record information is stored in the Provider's existing database system, and a h appropriate viewing permissions) is posted to the blockchain through our Ethereum client and library of backend APIs. The patient can retrieve and download this data from the provider's gatekeeper checks the blockchain to confirm their access and ownership rights.

Discussion & Future Work

MedRec gives patients a comprehensive log of their health care records that focuses on: easy, intuitive access; data sharing; and credible, verified content. This model restores patient agen fully informed of their medical history and any modifications to it. Through permission management on an Ethereum blockchain, we enable patient-initiated data exchange between medic need for confidentiality at a granular scale, MedRec allows for authorizations at the level of single records and even specific metadata fields. Blockchain smart contracts furnish a compellin expiration on viewership rights, revocation updates, custom identity registration procedures and more. The MedRec blockchain ledger keeps an immutable, auditable history of medical in providers.

Interoperability

By integrating with providers' existing data storage infrastructure (via our Database Gatekeeper layer), we facilitate continued use of their existing systems. The Database Gatekeeper curre can be easily configured to run on other query string database models, while keeping the same fundamental blockchain interactions. We believe this will ease adoption, lower integration c HIPAA regulations. Building on the principle of interoperability, we have designed the system with flexibility to support open standards for health data exchange-- be that FHIR and other proposals like the Continuity of Care Document [5]. In addition, MedRec is source agnostic and thus able to receive data from different endpoints (physician offices, hospital servers, patier address identity management, our Registrar Contract establishes a DNS-like mapping between a commonly used form of ID (name, patient PUID, etc) and on-blockchain addresses. Polici Contract can regulate registering new identities or changing the mapping of existing ones, and would be managed by providers (to interface with their existing identity verification procedu

Decentralization

Our blockchain implementation gives us several key properties of decentralization. The MedRec protocol enjoys a strong fail-over model, relying on the many participating entities in the s failure: medical records are stored locally in separate provider and patient databases; copies of authorization data are stored on each node in the network. Furthermore, because the medica system does not create a new, central target for content attack.

Data Economics

The MedRec mining model, where researchers earn metadata as a mining incentive, enables the emergence of data economics by writing in the research community from the very beginni the network while network beneficiaries (i.e. providers and patients) release access to aggregate, anonymized medical data as transaction "fees" that become mining rewards. Researchers c that providers release by selectively choosing which transactions to mine and validate. Providers are then incentivized to match what researchers are willing to accept, within the boundarie Patients and providers can limit how much of their data is included in the available mining bounties.

With this incentive model, researchers can now access a regular, dependable source of census level medical data. This opens an opportunity to observe wide-reaching patterns in medical t privacy of individuals and lowering the overhead associated with traditional research trials. One could envision that various agencies, such as the US CDC, might participate and use the re epidemics and diffusion characteristics of various medical conditions. Data-as-a-mining-incentive answers a pressing need in the medical research community while sustaining and securi authentication log via blockchain Proof of Work.

The "cost" to mine on MedRec will be held constant across participants, thus equalizing access to data and bringing in stakeholders outside of just academia and Big Pharma. We can envis

community on MedRec also including public health organizations, the CDC, regulated healthcare NGOs, insurance companies and other stakeholders in the healthcare industry. Because t private, networks of providers can decide on the proper process and qualifications for onboarding new research entities into the system. This prevents rogue, unregulated entities from joi

Next Steps

For the near future, we are planning user studies to assess the feasibility of the system and to gauge patient and provider interest. This will include partnering with local health care institu system efficiency. While outside the scope of the initial prototype, but unarguably crucial for future development, a rigorous k-anonymity analysis [4] of how best to construct privacy-pres

The MedRec team remains committed to the principles of open source software, and we intend to make our framework available as a platform for further development. Use of MedRec wil the data. We believe this policy is key, especially for a medical record system that emphasizes patient agency.

Noted Caveats

- Most importantly, this is a prototype still under development. Though we intend to open source our code, we would not recommend out-of-the-box-use of the current system, as it is yet
- We recognize that not all provider records can or should be made available to patients (i.e. psychotherapy notes, or physician intellectual property) [6], and thus MedRec does not presu management system for all of a Physician's output.
- Notably, MedRec does not claim to address the security of individual provider databases where the record content is stored. This must still be managed by the local IT admin. Nor does M Rights Management problem. Our system assumes provider nodes that are bound by external regulation governing data copying in the medical use case, i.e. HIPAA.
- The blockchain is pseudonymous, not anonymous. The organization of pointer data via public key address allows for data forensics by inferring patterns of interaction from frequency a and PII may remain private, one could infer that some ID has repeatedly interacted with a certain provider. Improving obfuscation while preserving auditability on the blockchain is an

This piece summarizes work presented in "MedRec: Using Blockchain for Medical Data Access and Permission Management" (2016), submitted to IEEE for publication. The authors woul Currency Initiative for the class and advising team out of which this project was born.

Appendix: Bitcoin Basics

First, we distinguish between "Bitcoin," the full protocol, and "bitcoin," the currency. The Bitcoin cryptography protocol describes a novel, distributed system of exchanging, securing and financial value. The bitcoin currency is the medium of transaction and the reward for participating in network stewardship (i.e. validating others' transactions). Participation in the networ provenance of bitcoin tracked from public key address to public key address. The "owner" of a bitcoin sum is the keeper of a public key address at which the bitcoin amount can be redeem of the protocol and currency, read Michael Nielson's blogpost.

The Bitcoin protocol is often referred to more generally as "the blockchain," referring to the append-only ledger that chains blocks of transaction records together into an immutable log (w members). Decentralization proves key to the "trustless" nature of the protocol, as all participating full nodes keep copies of the authoritative log, rather than trusting a central orchestrato used to secure the transaction record from tampering enables this trustless model, where individual nodes must compete to solve computationally-intensive "puzzles" (hashing problems) appended to the chain [7]. These worker nodes are known as "miners," and the work required of miners to append blocks ensures that it is difficult to rewrite history on the blockchain. Thi not collude and attempt to direct collective mining power at modifying a block, also known as a "51% attack [8]. The protocol issues mining rewards in sums of bitcoin. These are earned f the crucial role that miners play both in securing content and validating new transactions. This Proof of Work process essentially exchanges energy for security, as the mining process cons power.

Blockchain technology is a means to update and maintain the integrity of a fully distributed dataset. It is an alternative to a central repository that may be a target of attack or may not be u derives from its use to validate cash transactions in Bitcoin, and to date, supports a $6.5 Billion market capitalization [9] with a transaction volume of about $125 Million per day [10]. The running for seven years.

In the Bitcoin blockchain, all transactions are public and the transaction chain is maintained by an (ideally) unconnected set of miners. This group reaches consensus on the complete reco issuance of the first coin, thus insuring that no party can unfairly manufacture money.

Blockchain technology can be disassociated with the bitcoin currency and used in a variety of other settings (both public and private) where one desires a validated, unalterable, time-stam leverage these blockchain properties in MedRec to streamline access management for EMRs.

Additional Resources

- Michael Nielson's Blogpost
- October 2015 Economist Article
- For an in-depth course on the details of the Bitcoin protocol, head over to the Princeton Coursera class

Citations:

1. Public Standards and Patients' Control: how to keep electronic medical records accessible but private. *BMJ*. 322, 7281, 283–287.
2. Who Owns Medial Records: 50 state comparison. *Milken Institute School of Public Health*.
3. A Next-Generation Smart Contract and Decentralized Application Platform. *White Paper*.
4. FHIR Overview.
5. The Continuity of Care Document: Changing the landscape of healthcare information exchange. *White Paper*.
6. Individuals' right under HIPAA to access their health information.
7. Bitcoin: A Peer-to-Peer Electronic Cash System. *White Paper*.
8. 51% Attack, Majority Hash Rate Attack. *bitcoin.org*.
9. Market Capitalization (USD).
10. Estimated USD Transaction Volume.
11. K-anonymity: A Model for Protecting Privacy. International Journal of Uncertainty. 10, 5, 557–570.