BLOCKCHAIN™ IN HEALTHCARE TODAY

Blockchain as a Foundation for Sharing Healthcare Data

Marek A Cyran[1]

Author: [1]Booz Allen Hamilton, Inc., 8283 Greensboro Dr., McLean, VA 22102, United States

Corresponding Author: Marek A Cyran at **Cyran_Marek2@bah.com**

Keywords: Blockchain, Data Exchange, Data Sharing, EHR, Electronic Health Record, Ethereum, Interplanetary File System, IPFS

Section: Use Cases/Pilots/Methodologies

Blockchain technology has the potential to transform healthcare delivery by facilitating data sharing between providers and electronic health record (EHR) systems. However, significant roadblocks stand in the way of widespread implementation of this technology across the healthcare industry. Our blockchain-based data-sharing solution addresses two of the most critical challenges associated with using blockchain for health data sharing: protecting sensitive health information and deploying and installing blockchain software across diverse hospital environments. Since transparency is a fundamental feature of blockchain, we enabled user- and group-based secret sharing by adding purpose-built software that leverages a collection of well-established cryptographic algorithms. To streamline deployment, we built a containerized solution that guarantees portability, simplifies installation, and reduces overhead maintenance costs associated with administration. To ensure ease of implementation in a hospital system, we designed our blockchain solution using a distributed microservices architecture that allows us to encapsulate core functions of our system into isolated services that can be scaled independently based on the requirements of a particular hospital system deployment. As part of this architecture, we built core components for securely handling cryptographic secrets, interacting with blockchain nodes, facilitating large file sharing, enabling secondary-index based lookups, and integrating external business logic that governs how users interact with Smart Contracts. The innovative design of our blockchain solution, which addresses critical data security, deployment, and installation challenges, provides the healthcare community with a unique approach that has the power to connect providers while protecting sensitive data.

Keywords: Blockchain, Data Exchange, Data Sharing, EHR, Electronic Health Record, Ethereum, Interplanetary File System, IPFS

Blockchain technology provides a decentralized, transparent, authenticated platform that applies a consensus driven approach to facilitate the interactions of multiple entities through the use of a shared ledger. Beyond the financial sector, where much of the initial development is taking place, blockchain has the potential to revolutionize the healthcare system. By providing doctors, patients, researchers, and other healthcare professionals with a mechanism for the controlled exchange of sensitive, permissioned data, blockchain technology can improve data sharing and transparency between clinical and research data systems. Any healthcare organization participating in a blockchain consortium would be able to share medical information, regardless of their native electronic health record system. Blockchain provides significant opportunities for healthcare organizations to deliver more efficacious treatments and diagnoses through increased provider data sharing, and potentially safer and more effective clinical trials through research method tracking. However, significant challenges remain towards wide-spread implementation of this technology across healthcare systems. This report will describe how we addressed two specific challenges associated with blockchain implementation in a hospital system, namely protecting sensitive data on the blockchain, and deploying and implementing solutions across hospital systems.

METHODS AND FINDINGS

In this section, we describe approaches for enabling permissioned data sharing, and deploying blockchain solutions to facilitate collaboration across hospital systems.

Data Sharing/Security Solution

Modern blockchains are fundamentally transparent platforms where interactions between users and Smart Contracts, modeled by cryptographically signed but unencrypted transactions, are visible to every participant on the blockchain network. This central feature of blockchain technology results in obvious challenges to implementing solutions that share sensitive data, where only a restricted number of recipients should be given access to a piece of data, or a cryptographic artifact that can unlock a piece of data stored off the blockchain. Because of this property, special purpose software designed to work alongside the blockchain must be implemented to facilitate additional layers of encryption that enforce the privacy of content embedded within transaction data. In order to enable data sharing across hospital systems, we developed a purpose-built solution based on hospital privacy and security requirements that leverages a collection of strong cryptographic algorithms to enable user and group based secret sharing.

Within our blockchain implementation, each piece of data has one user (owner) who can share a piece of data they own with other users or groups at varying levels of access (summary versus full data). To limit full access, and instead enable summary access, each piece of data consists of a descriptor, viewable to anyone on the blockchain network, a summary, and content, which are stratified at different access levels. Therefore, having summary access gives the receiver only access to the descriptor and the summary, whereas full access provides all three components. Data sharing between users is modeled by a system where users can share data with other users and groups, as well as receive data requests from other users at any access level. If a user responds to a request by granting data access, a cryptographic artifact is exposed to the receiver in a way that allows only that receiver to view data at the specified access level. Our system ensures that sensitive information is never exposed on the blockchain, including both private and document keys, which is necessary in order to maintain the privacy and security of user-controlled data. As an additional security measure, our system preserves the fundamental property of revocation where the data owner may revoke access to a piece of shared data with a guarantee that even a receiver's private key together with the raw blockchain transaction data would not be sufficient to obtain data access.

Having a robust encryption scheme as part of a blockchain-based data sharing system is particularly critical from a security perspective because most blockchain implementations replicate the entire transaction ledger onto each node, therefore multiplying the potential attack surface by the number of nodes in the network. Though our existing system implements access controls at the document level, at its core, we designed the underlying architecture to support attribute-based sharing. This approach would require that the structure of submitted documents is captured within the underlying smart contracts so that not all data fields are treated homogenously, and that sensitive fields are treated separately from the rest of the document. The components of our platform that deal with secret sharing are not coupled to the format or structure of the underlying sensitive data being shared.

Our solution utilizes the Ethereum[1] platform for smart contract functionality with Docker containers and distributed architecture using microservices. Security in our data sharing system is derived from the use of a collection of well-established cryptographic algorithms. We used Elliptic Curve Integrated Encryption System (ECIS), which is a hybrid of the Elliptic Curve Diffie-Hellman (ECDH)[2] algorithm, Concatenation Key Derivation Function (KDF)[3], and the Advanced Encryption Standard (AES-256 in Galois Counter Mode) Block Cipher[4] that facilitates key encryption using elliptic curve primitives. ECDH is a well-studied algorithm and has been endorsed by the National Institute of Standards and Technology (NIST)[3]. Of note, many of the algorithm choices we employ for this cryptosystem were informed by the standard set of algorithms utilized by Ethereum. The use of these cryptographic algorithms is foundational to all blockchain implementations, particularly the use of hashing and digital signature algorithms to maintain the immutability of blockchain data and the authenticity of submitted transactions, respectively.

To build a data sharing system requires additional design requirements including the use of asymmetric cryptographic algorithms and approaches to facilitate encryption and decryption operations on arbitrary data. Algorithms using asymmetric cryptography utilize public and private keys to decrypt data. The keys are essentially large numbers that have been paired together but are not identical. One key in the pair can be shared with everyone, termed the “public key”. The other key is the private key and is kept secret. Either of the keys can be used to encrypt a message and the opposite key is used for decryption.

Blockchain technology is not typically designed for large transaction data payloads, so when building a data sharing system, one approach is to store data in a separate software solution that can provide a global reference to uniquely identify a document. In our system, we chose to use the InterPlanetary File System (IFPS)[5] decentralized filesystem that we could deploy alongside our blockchain nodes to enable the storage of very large files in a way that ensures minimal duplication across the entire filesystem network. Since file storage is decentralized, and has a large potential attack surface, all data is fully encrypted before being written into it. Because data is stored within an external storage solution, the blockchain component of our system is responsible for executing Smart Contracts that, in part, refer to our data and provide information on how data is owned, retrieved, and decrypted. Constraints may be added to our system to ensure that data files are standardized to Healthcare relevant specifications (i.e., Fast Healthcare Interoperability Resources HL7). Figure 1 depicts the system architecture of our solution, and in particular, the containerized platform deployed across a number of hospital systems.

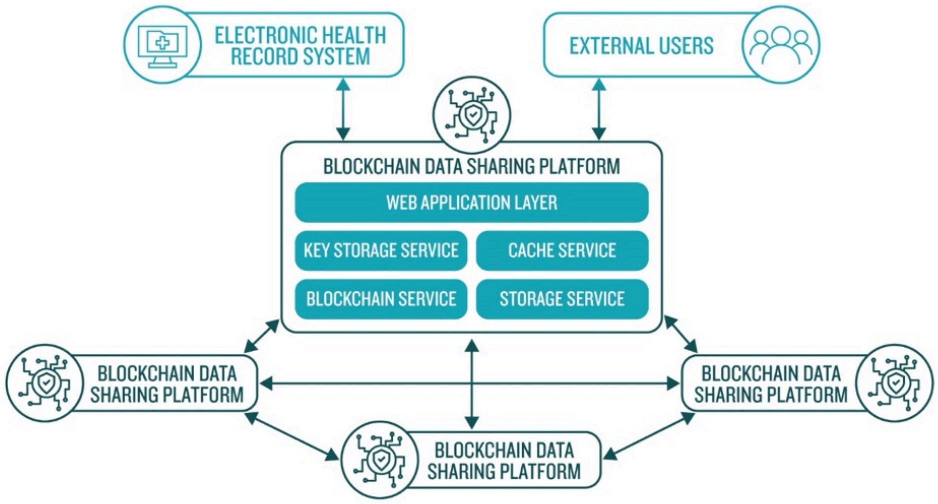
ELECTRONIC HEALTH RECORD SYSTEM
EXTERNAL USERS
BLOCKCHAIN DATA SHARING PLATFORM
WEB APPLICATION LAYER
KEY STORAGE SERVICE
CACHE SERVICE
BLOCKCHAIN SERVICE
STORAGE SERVICE
BLOCKCHAIN DATA SHARING PLATFORM
BLOCKCHAIN DATA SHARING PLATFORM
BLOCKCHAIN DATA SHARING PLATFORM

Figure 1. An illustration of the system architecture of our blockchain solution

Ease of Deployment and Implementation within a Hospital System

Streamlining the deployment of our blockchain solution is essential for acceptance and utilization within a hospital system. Often, variations in hospital information technology (IT) infrastructure can impede deployment and lead to increased reliance on IT administration. Our system uses the concept of containerization where the blockchain solution is wrapped within a special virtual machine image.

Containerization guarantees the portability of our software, simplifies deployment, and reduces the maintenance overhead across a variety of infrastructure environments. An application that can be easily deployed within any infrastructure environment reduces overhead costs since the only requirement for becoming a member of the network is the provisioning of one or more computing instances and any IT administration support required to make connections to the external blockchain network.

Ease of implementation within a hospital system requires both solution scalability and services within the blockchain architecture that perform functions necessary for data sharing including encryption, decryption, facilitation of transaction signatures, and storage of cryptographic artifacts that adhere to security best practices. Additionally, since blockchain technology is not built for data queries based on a set of user criteria, our solution includes a component that enables us to build secondary indices to enable this capability. Web application services act as the public endpoint into the system and contain all higher order business logic which leads to the creation of and interaction with smart contracts and data retrieval within the blockchain. We designed and developed a high-level abstraction layer for creating and interacting with smart contracts that acts as the primary interface to a blockchain node. Since blockchain is not geared towards storing large data payloads, we utilized a distributed file sharing solution that enables the decentralized sharing of documents between members of the blockchain network.

We leveraged and enforced open standards on data being submitted into the system to allow for flexibility on data specifications. This flexibility allows a user to employ their own organizational specifications for formatting and downstream analytics. Each of the above services encapsulate defined roles in the system, which makes them easier to develop in parallel. They may also be developed in different programming languages eliminating any tight coupling to a specific technology stack. These functionalities were enabled using a distributed microservice architecture where overall resource usage is spread across multiple computing instances and any component may be developed and scaled individually and independently depending on the requirements of the deployment site.

Finally, an integral part of implementation of our solution within and between hospital systems is its ability to enable semantic interoperability. As part of the larger solution, our system relies on submissions of health data that are triggered by software components embedded within electronic health record (EHR) systems that are part of our blockchain network. Submissions of this data come from a variety of different EHR systems, including Cerner and EPIC. In order for the submitted data to be computable by all consortium members, regardless of software deployed within their native environment, the data is encoded using open standards based on FHIR HL7.

CONCLUSIONS

Current centralized data sharing solutions struggle to meet the scale, accessibility and security requirements of healthcare organizations. Although blockchain technology provides a promising solution for addressing these issues and improving the interoperability of health data, permissioned blockchain capabilities must be combined with robust encryption components for integrity, security, and portability of user-owned data. In this paper, we shared our innovative solution for a blockchain system that supports the secure exchange of data with the addition of cryptographic algorithms that enforce the privacy of transactions. Our design, which combines enhanced security measures with containerization, provides a trusted and easy to deploy solution that will drive adoption of a blockchain-based health data sharing network.

Our solution is just one example of a health data sharing platform. Our system is unique because it is designed specifically for our use-case (data sharing across EHR systems), enables user and group-based data sharing, is fully containerized and deployable across multiple hospital IT infrastructures, and is designed as a platform solution utilizing a distributed microservice architecture that can be scaled depending on deployment requirements.

Although blockchain technology is still in its infancy, excitement about potential applications is growing. Solutions for permissioned sharing of health data, including data generated by wearables and other “Internet of Things” (IoT) devices, will become increasingly important to individuals who want greater access to their own data. Beyond the hospital, blockchain promises a solution that can empower patients, and support greater transparency between healthcare professionals. Developing and testing new designs on real-world use cases, such as data sharing between hospital systems, provides the first step in demonstrating the power of blockchain to break down data siloes in healthcare.

Acknowledgments
I would like to thank all those involved in the development and support of this manuscript including Steven Escaravage, Lauren Neal, Ernest Sohn, Holly Stephens, and Dr. Henry Francis.

Funding Statement
This paper is a work product of Mr. Cyran as part of his ongoing employment by Booz Allen Hamilton.

Competing Interests
We have no competing interests to declare in regard to the content of this manuscript including financial interests or other situations that might raise the question of bias in the work reported or the conclusions, implications, or opinions stated.

Copyright Ownership
Booz Allen Hamilton, Inc.

References

1. Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper. 2014 Apr;151.
2. Allen C. Evaluation of secp256k1 as Popular Alternate Curve. Lecture presented at; 2017; CFRG Interim Meeting, Paris.
3. Barker E, Chen L, Roginsky A, Smid M. Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography. NIST special publication. 2007:800-56A.
4. Daemen J, Rijmen V. AES proposal: Rijndael.
5. Allen C. Evaluation of secp256k1 as Popular Alternate Curve. Lecture presented at; 2017; CFRG Interim Meeting, Paris.