QUANTUM MEDICAL TRANSPORT, INC.
TECHNICAL REPORT

1/24/2018

Ricky Bernard, CEO

Technical Report

Quantum Medical Transport, Inc. a leading medical emergency and non-emergency medical transportation public company based in Texas sets out to develop a subscription based blockchain technology service platform called **QuantH**.

QuantH leading the path toward Blockchain-based medical records secure storage and sharing implementation of a patient controlled, blockchain-based system for clinical record maintenance and sharing. To understand how blockchain technology can improve the security and efficiency of electronic health data storage and sharing, it is first necessary to provide an overview of blockchain technology and its benefits.

Blockchain technology rests on three foundational principles. First, data is stored in a public, indestructible transaction ledger that anyone can read. Because the transactions can never be deleted or changed, there is always a complete and irrefutable record of all transactions. Second, blockchains are implemented in a decentralized network of computing nodes, which makes them robust against failures and attacks. Decentralization also means that no entity owns or controls the blockchain. Third, the metadata describing each transaction is available to everyone on the system, but that does not mean the data stored within the blockchain is readable. Blockchain relies on pseudoanonymity (replacing names with identifiers) and public key infrastructure (PKI), which allows the blockchain's contents to be encrypted in a way that is prohibitively expensive to crack. When applying blockchain technology to health data, each of these foundational principles apply.

Distributed Healthcare Transaction Ledger

Healthcare providers, payers and patients would contribute encrypted data, which would reference a patient ID, to a public blockchain. This could include clinical data that is stored in EHR systems today; claims history and gaps in care from payers; and family history and device readings from patients. This information

would be encrypted and stored in the blockchain and could only be decrypted by parties that have the patient's private key.

Because the ledger is indestructible, no one can erase or alter the record. Updates include metadata records of the date, time, location and entity making the update. In this way, a blockchain-based medical record will be self-auditing.

Public Key Cryptography is an encryption system that uses pairs of keys: a "public key" available to everyone and a "private key" that is known only to its holder. Either key may be used to encrypt a message, but the other key must decrypt the message. Practically speaking, there are two use cases involving public and private keys. First, a sender can encode a message with a public key and be sure that only the holder of the private key can decrypt it. Second, a message or document can be encrypted with a private key. If the message makes sense when it is decrypted using the corresponding public key, it's guaranteed that the holder of the private key is the party that encrypted the message. This is sometimes called "signing" a message12 because it is analogous to someone putting his unique signature on a document.

Blockchain also supports a concept called M-of-N signatures or "multisig," meaning that there are a total of N cryptographic keys, and at least M of them have to be present in order to decrypt the data. In this way, the patient can provide keys to authorized caregivers, doctors and others to grant access without the patient's specific key. This is useful when the patient is incapacitated and cannot provide consent to access the data.

Public Key Cryptography is an important concept for blockchain. All transactions are signed with private keys as a way of establishing the participants' identities. In the context of storing healthcare data in a blockchain, cryptography would have the additional role of encrypting the contents of the message, so that only intended users can read its contents.

Currently in the ecosystem of health records, each hospital or health system serves as its own central authority to provide record keeping and transmission services.

The traditional, centralized transaction infrastructure is a natural solution to the problem. While it has many advantages, there are also drawbacks. A centralized

infrastructure is vulnerable to hackers using ransom ware, failure, corruption and attack. This architecture causes the information silos that are prevalent in healthcare today to be significantly vunerable.

Blockchain replaces the centralized infrastructure with a distributed one. The blockchain software is running on thousands of nodes distributed across an entire network globally. To process a transaction, it is distributed to all the network nodes, and the transaction is cleared when the nodes have reached a consensus to accept the new transaction into the common ledger.

The process is technologically sophisticated, but it replaces entire record keeping and transaction processing institutions. This lowers transaction overhead in terms of price and execution time. It also means there is no single point of failure, providing a more robust, safer infrastructure.

Implementation of the QuantH Blockchain Solution

To implement a blockchain-based healthcare record system, EHRs and other record keeping systems would encrypt and send a transaction containing patient care documents – encounter notes, prescriptions, family histories, etc. – into the public healthcare blockchain. The transaction would include a digital signature from the contributor to trace provenance and the patient's blockchain ID as the recipient of the transaction.

After the documents are stored in the blockchain, patients would use a web-based or mobile application to view their blockchain contents and to grant or revoke access to specific parties via their private key.

The distributed blockchain system has a number of advantages over current methods of record keeping:

1. Patients become the platform, owning and controlling access to their healthcare data. This removes all obstacles to patients acquiring copies of their healthcare records or transferring them to another healthcare provider.

2. Because data is stored on a decentralized network, there is no single institution that can be robbed or hacked to obtain a large number of patient records.

3. Data is encrypted in the blockchain and can only be decrypted with the patient's private key. Even if the network is infiltrated by a malicious party, there is no practical way to read patient data.

4. The infrastructure itself provides auditing and non-repudiation capabilities. The methods used to add the data to the blockchain also include tamperproof timestamps, account IDs, and methods of determining if the contents have been altered.

A blockchain-based method of storing healthcare data includes all the expected criteria of a medical record keeping system, and it goes beyond what a traditional, centralized system can do because it improves patients' access to their records and strengthens security against data breaches.

The proposed solution begins with today's health IT systems, primarily EHRs, but also potentially includes laboratory information systems, radiology systems, payer databases, medical devices and consumer devices. These systems will continue to operate as they do today, storing data in their proprietary databases. In addition to storing its own copy of the data, each system will also transmit a copy to the blockchain-based PHR.

All EHR systems that are Meaningful Use compliant must provide the ability for patients to view, download and transmit their health information in human readable as well as machine readable format15. The document format is C-CDA, a machine-readable XML format. By applying a style sheet to the C-CDA document, it becomes an HTML file that can be read by a human using a web browser.

Many health systems satisfy the view/download/transmit criterion by making C-CDA documents available to the patient on a patient portal. From there, the patient can download or forward the document to the destination of their choice. Some EHR systems also offer other methods of transmission that do not require a patient portal.

There are three options for connecting an EHR's view/download/transmit function to a blockchain-based PHR:

Option 1: EHR vendors implement a blockchain client within their EHR software that communicates health information directly and automatically to the blockchain-

based PHR. (See Figure 4 below.) This would be the preferred option, but it requires effort and cooperation on the part of EHR vendors and is unlikely to occur without regulation or incentive.

Option 2: EHR vendors use existing protocols, such as REST, SOAP or Direct Messaging to send health information to a blockchain-based PHR, which is equipped to receive data according to these standards. This would mean that the blockchain-based PHR would need to be able to handle these communication protocols and configured to receive documents from various sources. Such functionality is somewhat heavyweight for a blockchain-based system, which is conceived as a simple electronic transaction ledger.

Option 3: Patients continue to receive their health information through existing patient portals and then forward or upload the documents to the blockchain-based PHR. The lowest common denominator method will work in all cases, but it relies on the extra, manual step of the patient acting as an intermediary. In a worst-case scenario, this will result in incomplete records if the patient does not complete the manual step.

Option 3 is the simplest scenario and the easiest to implement. The feasibility of the other two options depends on the willingness of EHR vendors.

For systems other than EHRs, the situation is somewhat less clear. Conceptually, there are ways to split the stream of data coming out of these systems and send a copy to the blockchain-based PHR; however, the economics and regulatory issues involved may complicate and delay the implementation of these efforts.

Patient Granting Access

- Patient A grants access to EHR to Practitioner A
- Practitioner A’s ID is added to Patient A’s authorized asset on the ledger
- Patient A’s ID is added to Practitioner A’s authorized asset on the ledger
- The Symmetric key for the EHR is decrypted with Patient A’s private key
- Symmetric key is then encrypted with Practitioner A’s public key

Patient Revoking Access

- Patient A revokes access from Practitioner A
- Practitioner A's ID is removed from Patient A's authorized asset
- Patient A's ID is removed from Practitioner A's authorized asset
- Patient A's private key is used to decrypt Symmetric key for EHR which is used to decrypt the EHR
- The EHR is encrypted with a new Symmetric key
- The new Symmetric key is encrypted with Patient A's public key and the public keys of all the remaining ID's that have permission

Practitioner Referring Patient

- Practitioner A updates the permissions to allow Practitioner B to access the Patient's EHR.
- Chaincode will check that the Practitioner A has permission on the EHR.
- Practitioner A uses its private key to decrypt the EHR's symmetric key
- Practitioner B's public key is used to encrypt the Symmetric key
- Practitioner B's ID is added to Patient A's authorized asset
- Patient A's ID is added to Practitioner B's authorized asset

In essence, the blockchain is a shared database. Unlike a traditional database, however, there is no central ownership. Instead, data is managed through the consensus of participants in a network, who work together (with the help of

cryptography) to decide what gets added, while each participant maintains an identical, full copy of all transactions. The network can be public (like bitcoin, open to anyone) or private (restricted to certain members). When new information needs to be added, every computer on the network is notified and updates its copy accordingly. The result is an expansive and distributed source of truth — built not from trust, but through cryptographically enforced consensus. Yet blockchain's most important attribute is its immutability: once something has been added, it is permanent — stored across thousands of computers, cryptographically locked in history.

The technical details of how this is done are somewhat complex, but involve public/private key encryption (for anonymity), proof-of-work (for agreement on what gets added to the ledger), longest-chain rule (for resolving conflict), and peer-to-peer networks (for communication).

How Will QuantH Blockchain Technology Be Applied to Health Care?

Our primary platform use will be health care is data exchange. Take medication prescribing as an example. A patient's medications are frequently prescribed and filled by different entities — hospitals, provider offices, pharmacies, etc. Each one maintains its own "source of truth" of medications for a patient, frequently with outdated or simply wrong information. As a result, providers in different networks, or on different EHRs, may not see one another's prescriptions. Additionally, electronic prescriptions must be directed to specific pharmacies, and paper prescriptions can be duplicated or lost.

To counter these difficulties, a medication prescription blockchain could be a shared source of truth. Every prescription event would be known and shared by those authorized to see it. This would allow, for example, prescriptions to be

written electronically without specifying a pharmacy, or prescriptions to be partially filled (and “fully” filled at a later date, by a different pharmacy). Since the QuantH blockchain would be the source of truth, each pharmacy would see all events surrounding that prescription — and could act accordingly. Most importantly, all health care providers could have an immediate view into a patient’s current medications, ensuring accuracy and fidelity.

Here are some of the other ways that QuantH blockchain platform may benefit health care:

- *Clinical data sharing*. Advance directives, genetic studies, allergies, problem lists, imaging studies, and pathology reports are just some of the data elements that could be distributed. Alternately, instead of storing actual patient data, blockchain could be used to store access controls — like who a patient has authorized to see their health data — even if the clinical data itself is stored by the EHR.
- *Public health*. A shared, immutable stream of de-identified patient information could more readily identify pandemics, independent of governmental bodies currently aggregating this data — for example, an influenza reporting system.
- *Research and clinical trials*. Distributing patient consent or trial results could foster data sharing, audit trials, and clinical safety analyses.
- *Administrative and financial information*. Insurance eligibility and claims processing workflows could benefit from blockchain and have decreased transactional costs.
- *Patient and provider identity*. National (or international) patient or provider identities could be secured in the blockchain, providing the basis for health data portability and security.

- *Patient-generated data*. Personal health devices, “wearables,” “Internet of Things” (IOT) devices, and patient-reported outcomes are just some examples of patient-generated data that could leverage the blockchain for security and sharing.

  The greatest potential of QuantH blockchain technology is the empowering of patients to own and gather their own data. Our health information technology framework — directly disrupts the siloed, centralized data stores that dominate health care data today.

  Quantum Medical Transport, Inc. is in the process of retaining technical advisors to fully develop and implement its technology initiatives outline above. We will be launching our ICO via Ambisafe platform.

Quantum Medical Transport, Inc.

Ricky Bernard, CEO

832-436-1831 x100

info@quantummedicaltransport.com

www.quantummedicaltransport.com