Blockchain: Securing a New Health Interoperability Experience

Brodersen, C; Kalis, B; Leong, C; Mitchell, E; Pupo, E; Truscott, A
Accenture LLP

August 2016

Abstract

Globally, and across multiple industries, an innovative model is emerging that enables faster, more efficient and highly secure business-to-business and business-to-consumer transactions. Many involved in healthcare hope the same distributed database technologies enabling this new model can drive similar results within the industry and, as with many other major innovations, recognize that confusion and hype can mask the potential of real world applications. Known as *blockchain* technologies, these solutions can support many existing healthcare business processes at a fundamental level. They promise to improve data integrity dramatically while enabling at-scale interoperability for information exchange, patient tracking, identity assurance and validation – among healthcare professionals, and between patients, their proxies and their healthcare providers.

Introduction

This paper explores how integrating current health IT investments with a permissioned blockchain distributed ledger technology (DLT) environment might drive better patient outcomes and align with the ONC's roadmap for change. The blockchain methodology addresses many of the issues with current health IT paradigms that involve security (specifically data integrity)[1] and privacy, immutably assuring expressed identities, creating highly robust audit trails and improving healthcare-related security for both providers and patients. The private sector is experimenting aggressively across a number of industries, including healthcare, to apply blockchain technology, owing to the benefits of distributed ledger technologies underpinned by it. The ONC should proactively explore this technology and prepare for how it will play a role in a vast array of potential healthcare use cases. In order for the ONC to perform its role effectively, there is a significant need to understand blockchain from the perspectives of the technology itself, the necessary computing power, the human skill sets required to operate in such an environment, and how to best leverage blockchain innovations. This paper focuses on three of the most important applications relevant to the mission of the ONC:

1. **Creating secured and trusted care records:** Securing healthcare records created by healthcare professionals and patients into an electronic chain of events, while preserving the inherent

[1] "Security" is a complex field, and includes Data Integrity, Data Privacy, Data Confidentiality and Data Quality issues, in addition to traditional "Security" matters. All of these can be considered Information Governance topics as outlined in the following white paper: https://newsroom.accenture.com/industries/health-public-service/accenture-finds-information-governance-framework-needed-to-guide-e-health-investments-and-strategy.htm

provenance and integrity of those records

2. **Linking identities:** Supporting strong identity proofing by preserving an immutable record of the declared identities of both patients and healthcare professionals
3. **Recording patient consent:** Empowering patients through the recording of consent decisions and patient directives within the secured healthcare record

To be effective, a blockchain must be additive to the healthcare ecosystem—users should not view it as a "rip and replace" technology that invalidates or minimizes existing technology investments.

Furthermore, despite the hype surrounding blockchain technology, it is not a cure-all for what ails the healthcare ecosystem but rather a tool in the healthcare toolbox—one that may face some of the same challenges current service models do.

However, it also has a unique ability to bring cohesion to an otherwise disparate and overly complicated system of delivering data across the healthcare spectrum.

Blockchains can drive ONC's Shared Nationwide Health Interoperability Roadmap

Blockchain technology applications in the above three areas can advance the ONC's Shared Nationwide Interoperability Roadmap[2], enabling the "quadruple aim" (better outcomes, improved clinician experience, improved patient experience and lower costs). What's more, they can address some of the root causes of the projected 20% of total healthcare expenditures attributed to waste identified by prior research.[3]

The technology aligns well to each of ONC's roadmap[4] goals. The blockchain methodologies described below have enormous implications for privacy, security, and risk management efforts in today's risky environment, where cyber-attacks are increasingly pervasive[5], and widely documented[6].

Blockchain: A Quick Definition

A distributed tamperproof database that secures all records that are added to it, wherever they exist. Each record contains a timestamp and secure links to the previous record.

Creating secured and trusted care records

Trust is the foundation for the provision of healthcare services to patients. The required trust might flow from a patient to a healthcare professional regarding whether they will receive the right care. Alternatively, it could flow the other way, from a healthcare provider to a patient, and involve the belief that the patient is honestly sharing his or her experiences and conditions.

A patient's healthcare information must represent trusted, authoritative evidence of care provided and decisions made, and display the identities of the participants in the care cycle. The use of cryptographic techniques such as public and private key pairs and the distributed nature of the

---

2 https://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf

3 Berwick, D and Hackbarth, A; *Eliminating Waste in US Health Care*il, JAMA. 2012;307(14):1513-1516. doi:10.1001/jama.2012.362.

4 https://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf

5 https://www.accenture.com/t20150723T115443__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_19/Accenture-Provider-Cyber-Security-The-$300-Billion-Attack.pdf

6 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

blockchain will vastly improve the non-repudiation and auditability of each healthcare transaction. Patients would be empowered to manage their own private keys as they wish. Since systems do not store actual Personal Health Information (PHI) on the blockchain, and use cryptographic keys to authenticate a user, it reduces the risk related to sensitive data leaks compared to today. Furthermore, the governance rules of a blockchain solution would pre-define access and control permissions to assure the appropriate levels of privacy versus transparency and ensure that only entitled parties can see necessary data. To protect the privacy of each user, healthcare organizations can also use a number of solutions such as tokenization, pseudonymization or masking technologies.

Once a party has joined the chain, additional parties can help to increase the quality and reliability of its identity. For example, to enable faster access to care providers, a patient can provide additional certified trust authorities (such as the Federal PKI Bridge Certification Authority, provider-specific Certification Authorities, or an authority from another industry such as financial services) to support an identity claim. Patients could boost the level of trust associated with their identities by requesting acknowledgement from trustworthy entities such as banks, employers or existing primary healthcare providers on the chain. The system could also rate sources of trust, and the strength of the verification would depend on the reliability of those sources.

Linking identities

The benefits of using a blockchain identity include the distributed ledger feature, which enables complete record integrity and transparency, and the system's nonrepudiation capability, which can become an enormous benefit in dispute resolution and fraud reduction cases. For example, because the blockchain infers that the owner of the key is the actual person that the records concern, when that person dies, any trusted party on the chain with knowledge of the fact could add this information to the system, thereby boosting its accuracy.

While a number of different tools can periodically authenticate the user, health professionals must also ensure that identity claims are true and reflect the user's status at a given point in time. This is especially crucial for healthcare providers, as issues

Why use Blockchains?

A blockchain allows a system of independent actors to share a record of digital assets, transactions and information without the need for a central, trusted third party. It enables users to replace certain inefficient intermediary functions in different economic, social and technological systems with decentralized digital networks.

Originally conceived as a way to disintermediate the financial establishment, the blockchain's strengths have attracted the attention of a variety of industries. Healthcare players can and should apply many of the lessons learned during the aggressive early experimentation and implementation within financial services. Increasing numbers of large organizations beyond financial services are investing heavily in exploring the technology's value as a digital business platform.

In short, blockchain will not replace but rather re-architect many incumbent business models, removing friction and

surrounding fraud, waste, and abuse have become of paramount importance to both providers and payers[7]. Furthermore, patients with access to an immutable record of care might question the credibility and value of the care provided to them if inaccuracies exist.

The integrated nature of the blockchain also means that the technology inherently links the disparate identities authenticated at the point of care for both patients and health-care professionals.

Recording patient consent

Several blockchain uses tie directly to the achievement of the short- and long-term goals of the ONC roadmap. For example, a key factor in the sharing of patient information involves gaining the consent of the person receiving treatment. Fundamental to the underlying professional ethics of healthcare, empowering the individual in this way is also a foundational consideration in internationally accepted approaches such as Privacy by Design[8].

By capturing patient consent statements in an immutable blockchain, healthcare professionals and others involved in the care cycle are able to trust those statements and act upon them accordingly. In addition, patients are able to add consent statements at any point in their care journey – confident that the blockchain will hold them securely. Healthcare professionals can act upon those directives, and the systems that they use can interpret them as access control decisions – with the assurance that the system is adhering to patient wishes.

The foundation of blockchain-enabled health information exchange

To reinforce the benefits outlined in this paper, and to utilize blockchain technologies to support ONC's roadmap directly, organizations should consider making investments in a number of aspects of the blockchain, its technology and its administration. All of which build on existing IT investments made by healthcare organizations. They include:

Core technical standards and functions - Envision a scenario where providers and provider organizations (as well as patients themselves) can store data for patients (including private identity information) in traditional databases and associate that information to the blockchain using cryptographic hash functions. This concept enables users to control their own data while at the same time allowing the network to validate identities. It also lets users access various data sources, tying together currently disparate systems that require often-intense validation and reconciliation processes.

Certification to support the adoption and optimization of health IT products and services - Because this concept envisions the storage of actual patient and provider data "off-chain" with access via a secure hash function stored on the blockchain, the approach should satisfy the desire for increased flexibility in the ONC regulatory structure. Essentially, data transport and content functions remain separate and can be attested individually, while at the same time the approach will broaden health IT to settings such as long-term and post-acute care environments.

A supportive business, clinical, cultural and regulatory environment - The blockchain phenomenon aligns with a broader change in the culture of interoperability, since it defines a patient and provider trust model where patients have a greater willingness to

7 http://www.healthaffairs.org/healthpolicybriefs/brief.php?brief_id=72

8 https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

participate in an interoperable, learning health system. They also have more control over how their data is used.

The rules of engagement and governance of the exchange of health information - Blockchain technology will change the model for engaging with and governing a Health Information Exchange. There is greater potential for shared patient/provider/payer collaboration using the blockchain compared to current methods, because patients have more control over their healthcare information. The enabling factor for this change involves the blockchain's distributed ledgers, which offer superior patient access compared to other forms of patient engagement, such as Personal Health Records (PHRs). The blockchain can also promote coordinated data exchanges among providers and payers because it reduces the current trust barriers that

Blockchain: How does it work?

Blockchains are cryptographic protocols that allow a network of computers (nodes) collectively to maintain a shared ledger of information without the need for complete trust between the nodes. Each blockchain database is essentially a time-sequenced chain of events that have been authenticated using a consensus mechanism specified by the protocol. The mechanism guarantees that, as long as the majority of the network validates the blocks posted to the ledger (i.e., chain) as per the stated governance rules, information stored on the blockchain can be trusted as reliable. This ensures that the transaction data is replicated consistently across the network. The effect of the distributed consensus mechanisms often means that all of the nodes of the network hold all the information stored on the blockchain.

From a regulatory and audit perspective, entries can be added to—but not deleted from—the distributed ledger. A network of communicating nodes running dedicated software that replicates the ledger among the participants on a peer-to-peer basis performs the maintenance and validation of the distributed ledger. All information shared on the blockchain has an auditable trail, which means it has a traceable digital "fingerprint." The information on the ledger is pervasive and persistent and creates a reliable "transaction cloud" so that data cannot be lost and can only be technically corrupted by any of the participants at prohibitive cost. Consequently, the technology essentially eliminates single point of failure risks and data fragmentation disparities among counterparties.

From a security perspective, cryptography protects the data via a number of different mechanisms. Users can address privacy and transparency needs using different consensus mechanisms specified by the protocol and public and private key pairs. A blockchain environment protects information at the data element level rather than in aggregate, and appropriate parties can only access data using appropriate permissions as defined by the protocol. Blockchain technology can also obfuscate data (i.e., the nodes, while having the data and knowing it is valid and validated by the rest of the network, will not be able to read it unless given access).

providers may have with payer requests for clinical data[9].

Understanding the technical interoperability challenges a blockchain can address

Whether patients or healthcare providers, system users should have ready access to, and control of, their validated identification information. Used in conjunction with other tools such as biometrics and tokenization, blockchain technology can support the management of digital identity issues[10] in healthcare. It can help to deliver non-repudiation and transparency, enabling the unique authentication of an identity in an irrefutable, immutable and secure manner, while ensuring the anonymity of each identity and transaction.

Ensuring each transaction is anonymous and not linked (unless the user requests it) - As envisioned, the blockchain would not store any PHI. However, healthcare professionals still need to address the transparent nature of a blockchain to ensure that each transaction a user conducts is not linked or traceable back to the user (unless otherwise requested). For example, a patient with a very sensitive condition visits a specialist provider but does not want the primary care provider to know this. The relationship between patient and primary care provider must remain separate and unlinked even though all three are on the same chain. Therefore, there has to be a way that the ownership of the key is anonymous and each transaction is untraceable except by the two transacting parties or the owner of the key.

Traditional data protection methods such as tokenization or masking can enable the anonymization of transactions within a blockchain environment. As these traditional methods are proven, they can be applied in other ways to provide different levels of data access and, where required, time-limited access.

Overcoming healthcare's lack of a single trusted source of identity data - While discussions regarding global digital identities and universal blockchain identities flourish across industries, healthcare presents a different challenge: no single, trusted source of available identity data exists today that the entire healthcare ecosystem can use.

Despite this, a number of other entities could provide, support and attest to identity claims as a starting point for creating digital identities. In a blockchain DLT environment, for example, banks and payment networks have already positioned themselves well for this activity and should support identity verification. Similarly, other organizations such as employers, telecom service firms and utility providers can also support identity verify-cation, especially for the underserved or "unbanked"[11] populations. These organizations are implicitly established trusted parties for patients and individual care providers alike, since most people have some combination of bank accounts, jobs, mobile, internet and telephone service, and insurance policies.

Moreover, the actual individual usually utilizes services from these entities, enabling them to provide more tangible authentication mechanisms, such as a PIN transaction on a payment card. Every time a physical authentication takes place with the digital ID, it adds to the chain as a form of continuous identity authentication.

---

9 https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf

10 http://www.modernhealthcare.com/article/20160123/MAGAZINE/301239980

11 http://demandinstitute.org/the-end-of-cold-hard-cash/

Entities can become sources of trust to verify identity claims to a blockchain, which would help to reduce the reliance on a government-issued ID for healthcare authentication and increase the quality and level of assurance associated with proof of identity in the industry.

Blockchains face implementation barriers

Compared to the financial markets (which themselves have yet to achieve blockchain maturity), the healthcare industry's participation with the technology remains in its infancy. Most of the current activity focuses primarily on research and development functions[i] of healthcare organizations that are exploring potential applications. The following represent the key barriers the technology must overcome to gain a legitimate place in the healthcare industry.

Regulatory and legal - Because blockchain technologies offer a new socio-political paradigm for doing business, few legal and regulatory frameworks are in place to govern their use. From a healthcare perspective, strong regulatory frameworks can ensure the integration of blockchain technology to avoid challenges in terms of regulatory reporting, HIPAA compliance, etc. Regulators will also need an in-depth understanding of how to operate in a blockchain environment, including the necessary skill sets, technology, and human capital requirements.

Scalability - As users add data, the blockchain grows—in this case, by storing all of the hashes associated with the appended data. This increases storage and computational power demands, which means the network might have fewer nodes with enough computing power to process and validate information on the blockchain. If health professionals fail to meet storage and computational power demands, the potential for increased centralization and slower data validation and confirmation grows.

Verification speed - To ensure that data on the blockchain is a trusted source, the network must verify it. To that end, various methods of validation exist, such as multi-signature, PBFT (Practical Byzantine Fault Tolerance), the Raft Consensus Algorithm[12], among other approaches, which must undergo testing for specific use case functionality and optimization. While the transactional throughput speeds necessary in healthcare applications do not approach the transactions per second seen in financial services, the need for near-real-time retrieval of healthcare information is paramount. Researchers need to determine the optimal verification process to avoid creating latency over time as the data on the blockchain grows.

Security breaches of blockchain infrastructure - The underlying blockchain protocol is stable and secure, largely owing to the fact that any malicious actor(s) attempting to reorganize (i.e., "attack and rewrite," commonly referred to as a 51% attack) the chain would have to control a majority of the computing power associated with the blockchain which carries significant, if not impossible costs. However, the supporting infrastructure of blockchain technologies such as exchanges and wallets have suffered from various security breaches, with hundreds of millions of dollars of cryptocurrency being stolen or "lost"[13]. Thus, while blockchain technology itself remains highly secure, healthcare entities need to choose the support infrastructure they use with great care.

[12] https://raft.github.io/

[13] http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP

As technology progresses, higher security standards will undoubtedly emerge, especially as they relate to the protection of private user keys and identity theft (i.e., securely replacing lost keys versus fraudulent attempts at obtaining keys). The industry also needs to comply with existing regulations around information security and key management.[14]

Immutability of the blockchain - While many tout the immutability of the blockchain as a significant plus in terms of data tracking and audits, it could pose major challenges. Blockchain-based code is only as good as the programmers who created it and humans are prone to error. Governance models and solutions must exist for situations where users need to remove data from the blockchain, for either privacy or legal reasons. To date, there are numerous examples where content that should be removed from the Bitcoin protocol is enshrined "forever" on the blockchain. A number of companies, including Accenture, are working with solution providers and other partners to solve this problem.

Blockchain technology has the potential to transform the healthcare ecosystem

As the hype surrounding the blockchain begins to fade, users will view it as another tool in the broader set of technologies that the healthcare system uses to enable an interoperable, learning health system. Initially, a number of potential use cases will emerge for leveraging blockchain DLTs in the healthcare ecosystem:

1 – Patient profiling for population health - The blockchain can leapfrog current population health approaches by providing trust where none now exists.

2 – Improved audit logging - Because the blockchain can act as a mechanism for collectively recording and notarizing any type of data, it can capture an audit trail of communications among providers, patients and payers regardless of each individual organization's audit logging function, largely eliminating many data dispute resolution challenges that exist today.

3 – Patient data as a service - One of the blockchain's healthcare interoperability strengths is its ability to replace the concept of a PHR in a way that makes patient data accessible "as a service."

4 – Improving health IT application deployment - A blockchain network may include identity schemes, data storage, and smart contract applications that execute against shared data infrastructure.

5 – New access points to healthcare data - The use of a blockchain with patient devices, such as wearables and remote monitoring devices, provides a further view into the patient ledger, with patient devices able to communicate with blockchain-based ledgers to update or validate smart contracts. This use case has been demonstrated in research settings using blockchain technologies available in the market.[15]

6 – Connecting traditional databases in a blockchain environment - One challenge involves guaranteeing that gaining access to traditional databases will not enable unauthorized users to read patient data. Controlling data access via the blockchain will require the development of new techniques to tie the data on the blockchain with the data on a traditional database. For example, traditional databases should store information so that the blockchain offers users the only way to "decrypt" content –

[14] A wide variety of these exist, including the Federal PKI Common Policy; FISMA; FICAM; Federal PKI Common Policy; HHS PKI Policy; The HHS Domain Device CA root certificate; and others.

[15] Accenture Technology Labs demonstration; U.S. Patent Application "Distributed Healthcare Records Management" (filing date Apr. 13, 2016)

such an approach affirms that patients can control their own data.

ONC's role: support, track and highlight demonstration opportunities

To stay ahead of this disruption, the ONC should support, track and highlight demonstration projects for the application of blockchain platforms in the above three areas. The goal is to encourage private sector innovation and to inform future policy using the insights captured from the demonstrations.

Suggested ONC actions over the next 12 to 36 months include:

- **ONC environmental scans and industry outreach** - investigate the current state of blockchain capabilities and uses, including in the financial sector; conduct outreach to organizations using blockchain and other relevant technologies, and synthesize findings into an environmental scan
- **ONC white paper** - synthesize findings from the ONC Blockchain Challenge, industry outreach, and additional research into a white paper that outlines the potential applications and benefits of blockchain technology in healthcare, discusses relevant health IT standards, and identifies challenges that may prevent industry adoption of the blockchain approach
- **ONC blockchain workshop** - evolve ONC blockchain workshops to a private/public conference modeled on Healthdatapaloza[16]
- **ONC's Federal Advisory Committees** - convene a public hearing to gather input on the benefits and challenges of the blockchain approach, discuss industry implications of blockchain use, address standards gaps, and provide guidance on policy considerations
- **ONC demonstrations** – fund demonstration projects in collaboration with industry on the application of blockchain technology.

The industry has a rich selection of possible demonstration projects from which to choose. For example, individual use cases from various service providers already support many of the recommendations laid out in this paper.

By using a broader identity management framework and leveraging smart contracts applied via a distributed ledger, operators can create a public encrypted ledger that gathers all of the medical records of users within a blockchain network. Any medical document would be accessible only by the parties that require access to information related to the medical act including patients, healthcare providers, and payers.

Accenture Technology Labs have demonstrated this approach in a research environment using blockchain technologies.[17]

Conclusion

Blockchain has the potential to significantly advance healthcare information sharing and support the delivery of improved patient outcomes. The creation of secured, trusted, portable healthcare records that have a high degree of integrity and fidelity, and can be trusted across the healthcare continuum, is foundational to this progress.

This paper has explored how integrating current health IT investments with a permissioned blockchain distributed ledger

[16] NOTE: This paper is part of an ONC Blockchain work-shop scheduled in September 2016

[17] Ibid.

technology (DLT) environment aligns with the ONC's roadmap for change.

In addition, the blockchain provides a route to address some of the interoperability issues that have long vexed the healthcare industry, notably the need to connect disparate patient identities and to store clinically meaningful consent information.

The Office of the National Coordinator is in a powerful position to advance and manage these developments as outlined in this white paper, benefitting the entire healthcare community here in the United States of America, and leading the world in interoperability supported healthcare advances. Based on our experience, the application of blockchain technology can move the needle on interoperability adoption in the United States *if* it targets and aligns to existing healthcare stakeholder interests.

Each of the three use cases identified in this paper are situations where we believe blockchain technology could significantly help in solving intractable issues that have had a prolonged negative impact on the healthcare industry.

From our perspective, blockchain offers a way for providers to improve their ability to understand their patients, thus creating a broader level of trust in the sharing of medical information, and a consistent view of identity.

Blockchain is an additive technology, building on top of existing investments, that we believe the industry needs in order to address the immediate and longer-term needs that ONC has identified in its Interoperability Roadmap. The technology development and research we have conducted to date demonstrates that, while the blockchain has many obstacles to overcome, it will have a positive impact in solving healthcare industry challenges.

We enthusiastically support blockchain technology as part of the vision where:

- **Patients** realize value from their healthcare data and share it securely as part of an ever-learning healthcare system; and
- **Providers** leverage patient data to improve health and wellness for their patients with improved clinical and financial outcomes

Accenture continues to explore and invest in technologies to benefit patients, providers and all healthcare actors. Consequently, Blockchain technology is a focal point for our practice, and we continue to invest in and lead industry thinking.

Acknowledgements

The authors thank the contributions from our colleagues Giuseppe Giordano, Christine Leong, Emily Mitchell, James Morgan, Kaveh Safavi, David Treat, Emmanuel Viale and Ronan Wisdom each of whom provided additional insights regarding blockchain technology, privacy enhancing technologies and applications within and outside of the healthcare industry.

[i] The Estonian eHealth Authority is the commonly cited example of a real world application of blockchain technology in healthcare. The Estonian eHealth Authority is collaborating with Guardtime, a cyber-security provider that uses blockchain systems to ensure the integrity of data, to secure the over one million healthcare records of its citizens. Source: http://www.coindesk.com/blockchain-startup-aims-to-secure-1-million-estonian-health-records/.

Additional real world examples of the application of blockchain in healthcare are taking place in research and development functions. Some examples include:

- **Philips Healthcare Launches Blockchain Lab to Explore Applications in Health** http://www.coindesk.com/philips-health-care-launches-blockchain-lab/
- **MIT Media Lab MedRec Project** https://medium.com/mit-media-lab-digital-currency-initiative/medrec-electronic-medical-records-on-the-blockchain-c2d7e1bc7d09#.8skj2962p
- **Accenture Technology Labs Blockchain for Healthcare Demonstrations** which explore new opportunities around Blockchain and Healthcare to enable Health and Medical Data to be shared anonymously across multiple actors