

## **Blockchain:**

### Opportunities for Health Care

by RJ Krawiec, Dan Housman, Mark White, Mariya Filipova,  
Florian Quarre, Dan Barr, Allen Nesbitt, Kate Fedosova,  
Jason Killmeyer, Adam Israel, Lindsay Tsai

This white paper was developed in response to the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology (ONC) ideation challenge—*The Use of Blockchain in Health IT and Health-Related Research*. It was selected as one of the winning papers from a field of over 70 submissions from a wide range of individuals, organizations, and companies addressing ways in which blockchain technology might be used in healthcare.

# 1 Blockchain—A new model for Health Information Exchanges

A blockchain powered health information exchange could unlock the true value of interoperability. Blockchain-based systems have the potential to reduce or eliminate the friction and costs of current intermediaries. Particularly compelling use cases for blockchain technology include the Precision Medicine Initiative, Patient Care and Outcomes Research (PCOR), and the Nationwide Interoperability Roadmap. For these and other high-potential areas, determining the viability of the business case for blockchain is paramount to realize the benefits of improved data integrity, decentralization and disintermediation of trust, and reduced transaction costs.







The exchange of Personal Health Records and Health Information Exchange (HIE) data via the Integrating the Health care Enterprise (IHE) protocol is an important part of addressing the challenges of system interoperability and accessibility of medical records. The strategy outlined to date

[Blockchain] does offer a promising new distributed framework to amplify and support integration of health care information across a range of uses and stakeholders.

provides the technical requirements and specific incentives for health systems to meet the Meaningful Use interoperability standards necessary to support the envisioned National Health Information Network, buttressed by a network of HIEs operating on a broad scale. That unrealized scale, driven in large part by insufficient incentives outside of compliance, threatens the viability of HIEs and merits exploration of new models. It may be possible that new

value based models embedded in MACRA will be sufficient to make the market model work, but HIEs have been seeking alternative business models. Meanwhile the health systems that see true benefits from establishing a clinically integrated network in order to engage in risk-based contracts focus on private exchanges and are looking for low cost solutions that enable secure integration and support the assembly of virtual health systems that move beyond organizational boundaries.

While blockchain technology is not a panacea for data standardization or system integration challenges, it does offer a promising new distributed framework to amplify and support integration of health care information across a range of uses and stakeholders. It addresses several existing pain points and enables a system that is more efficient, disintermediated, and secure.

HIE pain points	Blockchain opportunities
	
<b>Establishing a trust network</b> depends on the HIE as an intermediary to establish point-to-point sharing and “book-keeping” of what data was exchanged.	<b>Disintermediation of trust</b> likely would not require an HIE operator because all participants would have access to the distributed ledger to maintain a secure exchange without complex brokered trust.
	
<b>Cost per transaction</b> , given low transaction volumes, reduces the business case for central systems or new edge networks for participating groups.	<b>Reduced transaction costs</b> due to disintermediation, as well as near-real time processing, would make the system more efficient.
	
<b>Master Patient Index (MPI)</b> challenges arise from the need to synchronize multiple patient identifiers between systems while securing patient privacy.	<b>Distributed framework for patient digital identities</b> , which uses private and public identifiers secured through cryptography, creates a singular, more secure method of protecting patient identity.
	
<b>Varying data standards</b> reduce interoperability because records are not compatible between systems.	<b>Shared data</b> enables near real-time updates across the network to all parties.
	
<b>Limited access to population health data</b> , as HIE is one of the few sources of integrated records.	<b>Distributed, secure access</b> to patient longitudinal health data across the distributed ledger.
	
<b>Inconsistent rules and permissions</b> inhibit the right health organization from accessing the right patient data at the right time.	<b>Smart contracts</b> create a consistent, rule-based method for accessing patient data that can be permissioned to selected health organizations.

# 2 What is Blockchain?

At its core, blockchain is a distributed system for recording and storing transaction records. More specifically, blockchain is a shared, immutable record of peer-to-peer transactions built from linked transaction blocks and stored in a digital ledger. Blockchain relies on established cryptographic techniques to allow each participant in a network to interact (e.g. store, exchange, and view information), without preexisting trust between the parties. In a blockchain system, there is no central authority; instead, transaction records are stored and distributed across all network participants. Interactions with the blockchain become known to all participants and require verification by the network before information is added, enabling trustless collaboration between network

participants while recording an immutable audit trail of all interactions.

Deloitte's blockchain framework<sup>1</sup> serves as a simple guide for organizations interested in utilizing blockchain technology. It can help guide decision making by answering four key questions: When should organizations *initiate* blockchain pilots? How should they *design* the use cases? When should they *strengthen* the system through smart contracts? Should they *implement* permissioned, permissionless, or consortium blockchains? For organizations new to the technology, the guided, four-step process simplifies a complex, rapidly evolving field into a series of discrete decisions.

Before leaders **initiate** blockchain projects, they should consider whether the technology is suitable to the organization's needs. Not all problems require a blockchain solution. Blockchain truly shines when four conditions have been met: (1) multiple parties generate transactions that change information in a shared repository, (2) parties need to trust that the transactions are valid<sup>2</sup>, (3) intermediaries are inefficient or not trusted as arbiters of truth, and (4) enhanced security is needed to ensure integrity of the system.

For health care organizations that have decided to initiate blockchain projects, the next step is to **design the use cases**. There are two primary use cases to consider: (1) verify and authenticate information, or (2) transfer value.

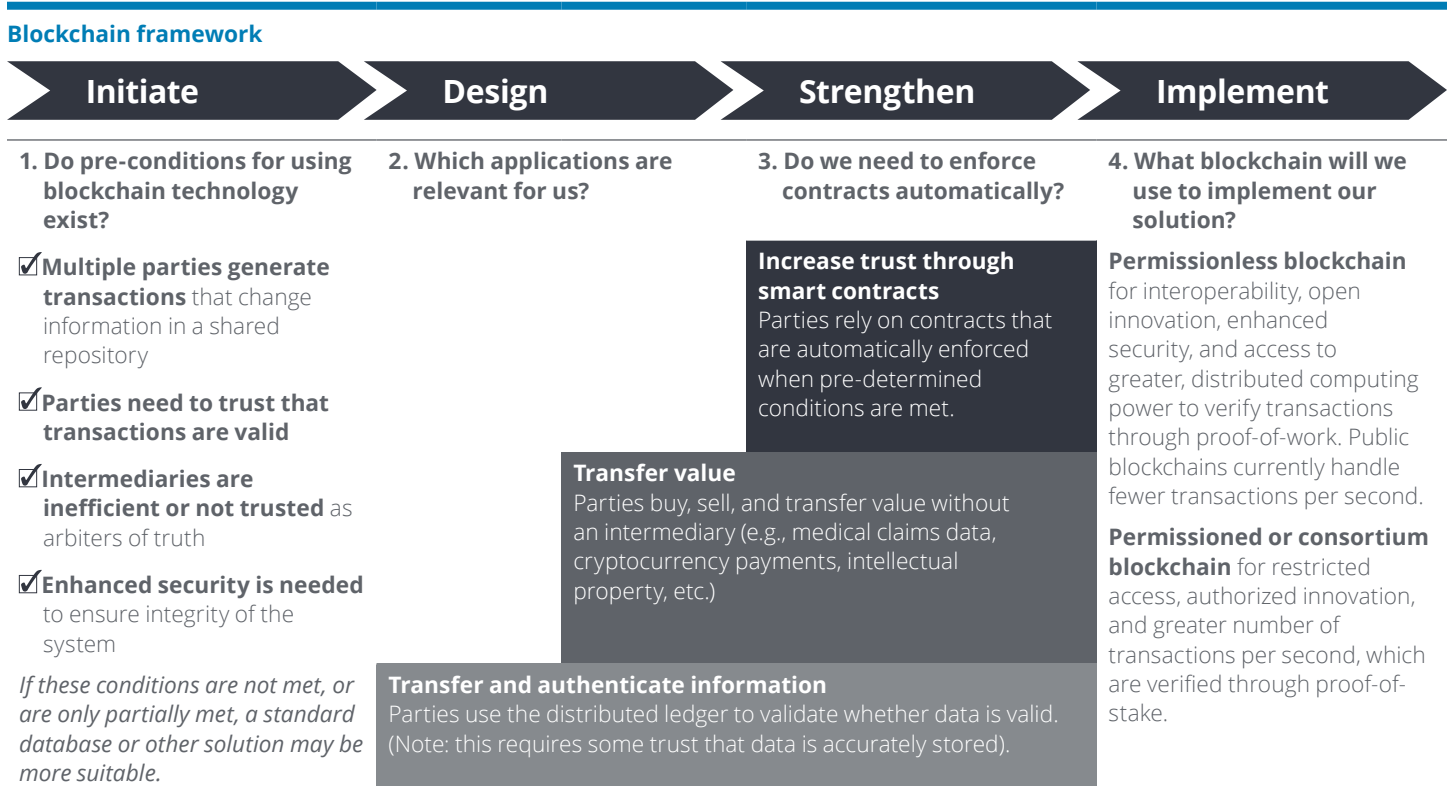


Figure 1: Deloitte Blockchain Decision Framework

In the first use, organizations may consider blockchain technology to verify a patient's digital identity, genetics data, or prescriptions history. Prescrypt, a proof-of-concept developed by Deloitte Netherlands, in collaboration with SNS Bank and Radboud<sup>3</sup>, gives patients complete ownership of their medical records, allowing them to grant and revoke provider access to their data. Providers, in turn, can issue prescriptions on the blockchain. In the second application, organizations can use the technology to transfer value, such as cryptocurrencies or intellectual property rights. Deloitte, in collaboration with Loyyal, developed a prototype that incentivizes

Finally, to **implement** a blockchain solution, organizations may choose to use a permissionless blockchain, such as the Bitcoin blockchain, or a permissioned blockchain that restricts access to a pre-determined group. Consortia such as R3 in the financial services industry are experimenting with permissioned blockchains, and R3 has recently completed a successful transfer of commercial paper between banks<sup>4</sup>.

Implementation also requires selection of a blockchain protocol—the underlying blockchain technology and framework that guides the structure of the blockchain and development of applications. Platforms such

solutions are not optimized for high volume data that needs absolute privacy and instantaneous access within a single organization. Blockchain solutions are designed to record specific transactional data events that are meant to be shared across a network of parties where transparency and collaboration are mission critical. The Blockchain Framework highlights these preconditions.

In the health care landscape where the United States Department of Health and Human Services (HHS) operates, blockchain technology has transformative potential. Nationwide health information interoperability could be realized through a consortium blockchain, which can leverage a leading protocol and create a standardized transaction layer for all organizations. Blockchain technology has the potential to advance HHS's strategic goals<sup>7</sup> and investments to standardize health care information by establishing a transaction layer on which all stakeholders can securely collaborate.

Organizations considering blockchain technology may find the aforementioned framework useful as a guidepost and a part of an iterative decision process; however, it is not intended to be an exhaustive, prescriptive list. The four steps outlined above are intended as a forcing mechanism to apply disciplined consideration of requirements, limitations, and alternatives before launching costly and time consuming experiments.

Deloitte's blockchain framework<sup>1</sup> serves as a simple guide for organizations interested in utilizing blockchain technology.

desired behaviors using gamification and behavioral economics principles. In the future, health ecosystems may emerge where providers, plans, or fitness centers co-develop programs to incentivize and reward patients for healthy behaviors.

In the third stage of the blockchain framework decision making process, organizations have an opportunity to **strengthen** the system through smart contracts that automatically execute when conditions are met. This application is increasingly sophisticated, using algorithms to fully customize conditions that determine when to exchange value, transfer information, or trigger events. This serves as the foundation for more sophisticated applications of blockchain technology in health care, including prior-authorizations and auto-claims processing.

as Ethereum provide the ability to create decentralized applications built on top of blockchain architecture; it is a leading blockchain protocol for both permissioned and permissionless blockchain development<sup>5</sup>. Additionally, Hyperledger is an open source project created by the Linux Foundation seeking to create a platform for corporate based blockchain platforms and other standards<sup>6</sup>. The choice of blockchain protocol is important, because it will influence the range of possible applications and the number of users participating on the network.

While blockchain may have significant potential to improve data interoperability, security, and privacy, it is important to note the boundaries of the technology. Blockchain is not a substitute for an enterprise database. Blockchain powered

# 3 **Blockchain** as an enabler of nationwide interoperability

The Office of the National Coordinator for Health Information Technology issued a Shared Nationwide Interoperability Roadmap, which defines critical Policy and Technical Components needed for nationwide interoperability, including (1) Ubiquitous, Secure Network Infrastructure, (2) Verifiable Identity and Authentication of All Participants, (3) Consistent Representation of Authorization to Access Electronic Health Information, and several other requirements. However, current technologies do not fully address these requirements, because they face limitations related to security, privacy, and full ecosystem interoperability.

The current state of health care records is disjointed and stovepiped due to a lack of common architectures and standards that would allow the safe transfer of sensitive information among stakeholders in the system. Health care providers track and update a patient's common clinical data set each time a medical service is provided. This information includes standard data, such as the patient's gender and date of birth, as well as unique information pursuant to the specific service provided, such as the procedure performed, care plan, and other notes. Traditionally, this information is tracked in a database within a singular organization or within a defined network of health care stakeholders. This flow of information originating from the patient through the health care organization

The current state of health care records is disjointed and stovepiped due to a lack of common architectures and standards.

each time a service is performed does not need to stop at the individual organizational level. Instead, health care organizations could take one more step and direct a standardized set of information present in each patient interaction to a nationwide blockchain transaction layer. The surface information on this transaction layer would contain information that is not Protected Health Information (PHI) or Personally Identifiable Information (PII); rather, select and non-personally identifiable demographics and services rendered information could enable health care organizations and research institutions access to an expansive and data-rich information set. Information stored on the blockchain could be universally available to a specific individual through the blockchain private key mechanisms, enabling patients to share their information with health care organizations much more seamlessly. This deployment of a transaction layer on the blockchain can help accomplish ONC HIT's interoperability goals while creating a trustless, and collaborative ecosystem of information sharing to enable new insights to improve the efficiency of the nation's health care system and health of its citizens.

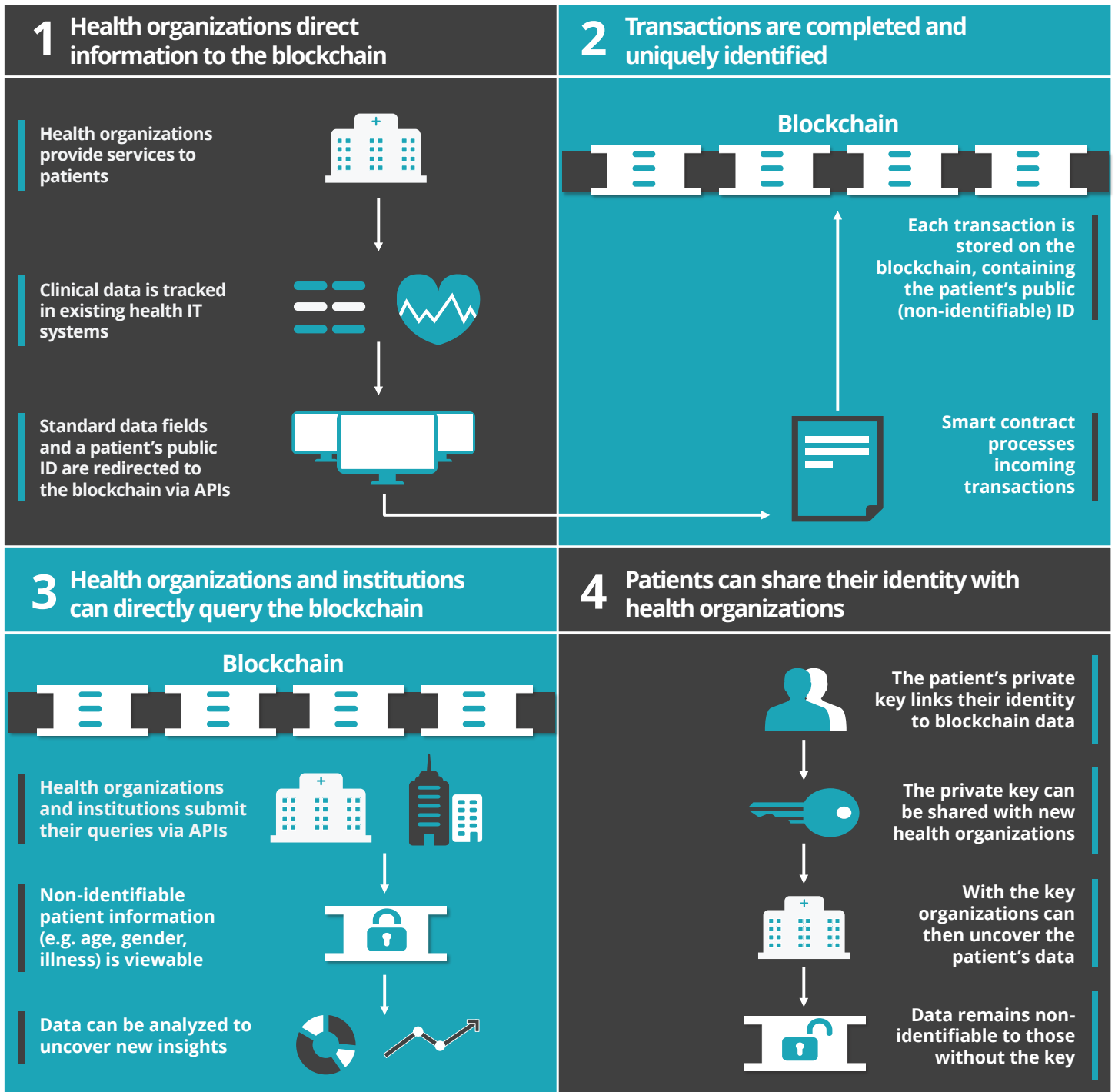





Figure 2: Illustrative Healthcare Blockchain Ecosystem

## Toward blockchain interoperability

As a transaction layer, the blockchain can store two types of information: (1) “On-chain” data that is directly stored on the blockchain or (2) “Off-chain” data with links stored on the blockchain that act as pointers to information stored in separate, traditional databases. Storing medical information directly on the blockchain ensures that the information is fully secured by the blockchain’s properties and is immediately viewable to those permissioned to access the chain; at the same time, storing large data files slows block processing speeds and presents potential challenges to scaling the system. In contrast, encrypted links are minimal in size and are activated once a user with the correct private key accesses the block and follows the encrypted link to a separate location containing the information. As an example, the blockchain cannot directly store abstract data types such as x-ray or MRI images: this type of data would require links to a separate location. Organizations considering how data should be stored should therefore carefully evaluate both technical and confidentiality constraints.

Creating interoperability requires frictionless submission and access to view data. As such, the blockchain could serve as a transaction layer for organizations to submit and share data using one secure system. This will be most effective if a specific set of standardized data were to be stored directly on the blockchain for immediate, permissioned access, supplemented by off-chain data links when necessary. A standardized data set could include information such as demographics (gender, date of birth, other data), medical history (immunizations, procedures), and services rendered (vital signs, services performed, and other data). As the field matures, further

	On chain data	Off chain data
<b>Data types</b> 	<ul style="list-style-type: none"> <li>Standardized data fields containing summary information in text form (e.g. age, gender)</li> </ul>	<ul style="list-style-type: none"> <li>Expansive medical details (e.g. notes) and abstract data types (e.g. MRI images, human genome)</li> </ul>
<b>Pros</b> 	<ul style="list-style-type: none"> <li>Data is immediately visible and ingestible to all connected organizations, making blockchain the single source of truth</li> </ul>	<ul style="list-style-type: none"> <li>Storage of any format and size of data</li> </ul>
<b>Cons</b> 	<ul style="list-style-type: none"> <li>Constrained in the type and size of data that can be stored</li> </ul>	<ul style="list-style-type: none"> <li>Data is not immediately visible or ingestible, requiring access to each health care organization’s source system for each record</li> <li>Requires Off-Chain micro-services and additional integration layers</li> <li>Potential for information decay on the blockchain</li> </ul>

evaluation and guidance will be needed to determine where and how each data type should be stored.

Once a standardized set of health care information is established, the specific data fields can be created in a smart contract to employ rules for processing and storing information on the blockchain, as well as stipulating required approvals prior to blockchain storage. Each time a patient interaction occurs, health care organizations will pass information to the smart contract —where the parameters of the contract will verify that valid information has been submitted. As an example, the smart contract can stipulate that all fields need to be provided prior to blockchain storage or that a specific field must contain a particular data type (e.g. numerical) to be valid. Once the smart contract validates that the correct data fields have been submitted, it will direct the transaction to the blockchain for storage.

## Blockchain strengthens data integrity and patient digital identities

An interoperable blockchain can strengthen data integrity while better protecting patients’ digital identities. In 2015, there were 112 million health care record data breaches due to hacking/IT incidents<sup>8</sup>. In 2016, it is estimated that one in three health care recipients will be a victim of a data breach<sup>9</sup>. The blockchain’s inherent properties of cryptographic public/private key access, proof of work, and distributed data create a new level of integrity for health care information.

Each participant connected to the blockchain network has a secret private key and a public key that acts as an openly visible identifier. The pair is cryptographically linked such that identification is possible in only one direction using the private key. As such, one must have the private key in order to unlock a participant’s identity to uncover



what information on the blockchain is relevant to their profile. Therefore, the blockchain public/private key encryption scheme creates identity permission layers to allow patients to share distinct identity attributes with specific health care organizations within the health care ecosystem on as-needed-basis, reducing vulnerabilities stemming from storing PII on all sides and allowing for data access time limits to be introduced by patients or providers.

Furthermore, potential hacking of a single patient's private key can limit the potential adverse damage, as the hacker would need to individually hack every single user to obtain unique private keys to access identifiable information of value. In an era of ubiquitous perimeter firewall breaches and ransomware, the process of asynchronous encryption protects patient identities moving across or within organizations.

Additionally, all health care organizations connected to the blockchain can maintain their own updated copy of the health care ledger—and as a result—if a historical block were to be adjusted, it would require 51% of network participants to approve the change, as every single copy of that blockchain would need to be updated to reflect the change. This feature improves security and can help limit the risk of malicious activity, because changes are immediately broadcast to the network, and distributed ledgers provide safeguard copies against harmful hacks.

#### **Blockchain supports frictionless connectivity, supported by smart contracts and consistent authorization to access electronic health information**

In this interoperable blockchain, smart contracts can be created to serve as the gateway to store standardized information, which can be immediately accessible to all organizations permissioned to the blockchain. This can be accomplished by

creating an application program interface (API) oriented architecture to feed the smart contract. The APIs will be published and made available to all participating organizations connected to the blockchain—enabling frictionless integration with each organization's existing systems. When the API is invoked, it will carry the contents of the patient interaction to the smart contract housed on the blockchain.

Querying information from the blockchain can also be done through a series of API calls that each connected organization can invoke. By invoking these APIs, organizations can immediately query specific blocks on the chain or submit defined query parameters (e.g. patients with ages over 25). The APIs can feed a standard portal that all connecting health care organizations access and use for direct integration to their own systems. The API oriented structure allows organizations to continue to focus on their internal systems while only requiring the redirection of specific data fields.

#### **Blockchain enables PCOR and precision medicine insights**

The blockchain transaction layer could enable immediate access to a rich set of standardized, non-patient identifiable information. As the range of stakeholders in the massive cohort necessary to make progress toward precision medicine proliferates, blockchain serves as the integrating factor without assuming storage or data standardization responsibility for the diverse range of stakeholders. This information can be made available to research institutions and existing government initiatives, and as blockchain executes on top of or within cloud environments, can be integrated into the evolving efforts of the Precision Medicine Initiative (PMI). Interoperability is one of the keys to unlocking the power of the data inherent in a historically-sized cohort, and

both the amount of data and the benefits from leveraging it in a timely manner have the potential to be exponential. Big Data analytics and cognitive computing/machine learning can be applied to this blockchain data set to further analyze the intersection of demographics, genetic markers, and a range of other data.

PCOR can leverage the standardized data set to shape its Data Access Framework initiative and use the information to conduct clinical research, patient safety event reporting and adverse event identification, and public health reporting. Additionally, due to the blockchain's privacy and security properties, PCOR researchers and partnering organizations can access a single source of truth of information that maintains integrity of the health care information for each patient.

The blockchain transaction layer could enable access to a rich set of standardized, non-patient identifiable information.

# 4 Implementation challenges and considerations

Blockchain technology presents numerous opportunities for health care; however, it is not fully mature today nor a panacea that can be immediately applied. Several technical, organizational, and behavioral economics challenges must be addressed before a health care blockchain can be adopted by organizations nationwide.

## Scalability constraints: tradeoffs between transaction volumes and available computing power

The Blockchain Framework suggests that organizations can roll out permissionless or permissioned implementations of blockchain technology. Permissionless blockchains are appealing, because they enable broader access, allow for open-innovation, and tap greater computing power across the network. At the same time, existing permissionless blockchains, such as Ethereum or Bitcoin, face transaction volume constraints. Today, the Bitcoin blockchain processes approximately seven transactions per second, yet there are over 10 million users and 200,000 daily transactions<sup>10</sup>. Many in the field are calling for the technology to evolve to allow faster processing times.

Permissioned blockchains, for their part, can expedite the transaction processing times, but they may face computing power constraints due to reduced participation in the network. Theoretically, HHS could supply the computing power necessary to process all blockchain transactions on one, permissioned network for select participants; however, this would result in HHS being the relative owner of the blockchain and could preclude the value of a truly decentralized system. A nationwide blockchain, with a large number of health care participants, would make the system not only more interoperable, but it would also make it more secure.

## Data standardization and scope

In addition to evaluating permissionless and permissioned blockchains, organizations should consider what information is stored on or off the blockchain. For health care information stored on the blockchain, the most immediate concern is the size of information stored on the blockchain. A free-form submission of data to the blockchain, such as doctor notes, could create unnecessarily large transaction sizes that could adversely impact the performance of the blockchain. Yet, the blockchain can still be efficiently operable with a specific, and confined set of data, such as demographic information, medical history, and codes for services rendered. To standardize data stored on the blockchain and to manage performance, organizations should align on a framework for defining what data, size, and format that can be submitted. In some cases, technical APIs can concatenate and de-concatenate the information stored and broadcasted to condense the data size. Lastly, participants can privatize the blockchain to restrict access only to registered and valid organizations.

## Adoption and incentives for participation

Two levels of incentives are necessary for blockchain to succeed. On a technical level, a network of interconnected computers (nodes) must be present to supply the computing power necessary to create blocks once a transaction is submitted. In a

permissionless blockchain, monetary incentives in the form of cryptocurrency encourage individuals to lend their computing power to the network. For permissioned blockchains, participation could be encouraged through financial incentives or access to blockchain data in exchange for processing transactions.

In addition to incentives for blockchain to work technically, further support may be needed to encourage organizations to adopt the technology and participate in a shared network. While some organizations are already testing the technology to verify and track medical records and claims internally, blockchain will be more powerful when the number of users on the shared network increases. Programs similar to the Center for Medicare and Medicaid Services (CMS)'s Meaningful Use program<sup>11</sup>, which incentivizes providers to switch to electronic medical records, could increase adoption and facilitate a nationwide blockchain health exchange.

## Costs of operating blockchain technology

While blockchain technology enables faster, near-real time transactions, the cost of operating such a system are not yet known. Health and government organizations spend a significant amount of time and money setting up and managing traditional information systems and data exchanges; requiring resources to continuously troubleshoot issues, update field parameters, perform backup and recovery

measures, and extract information for reporting purposes. Blockchain's open-source technology, properties, and distributed nature can help reduce the cost of these operations. Once a blockchain and its smart contracts are configured, the parameters become absolute, negating the need for frequent updates and troubleshooting. Since blockchain records are also immutable and stored across all participating users, recovery contingencies are unnecessary. Moreover, blockchain's transparent information structure could abolish many data exchange integration points and time consuming reporting activities.

### Regulatory considerations

Health care policy makers should consider deep collaboration with industry in order to understand and facilitate growth of the ecosystem within the bounds of the existing regulatory framework and new administration policy objectives. Considerations may include the implication of the distributed storage nature of the blockchain, who has ownership of records (and when does ownership change?), and how is access granted using the blockchain.

HHS, through HIPAA Privacy Rule, establishes national standards to protect individuals' medical record privacy. The Rule

specific individual. As an example, the potential to identify an individual with a rare health condition may be greater in a rural area as compared with a densely populated urban center. These concerns may be partially mediated through a permissioned blockchain. Nonetheless, as blockchain experiments advance, the questions will need to be carefully considered.

A blockchain solution could address the HIPAA Privacy Rule by separating and encrypting identity, PII, and PHI.

At the same time, a blockchain consumes significant computing power to process transactions. The cost of computing power is derived from the volume and size of transactions submitted through the network; further varying by the type of transactions occurring on the chain (e.g. data storage vs. value exchange). Beyond the Bitcoin blockchain, there are scarce blockchains in full production, and as such, it is difficult to forecast the possible costs of operating a blockchain at scale within a private enterprise or among a consortium of partners. Therefore, to understand the potential costs of a fully scaled blockchain, customized to meet HHS and partner needs, targeted experiments and common blockchain guidelines are needed to iteratively test the technology with a view to scale.

sets the conditions with which to protect the privacy of personal health information and sets limits and conditions on use and disclosures which may be made without patient authorization. Because of these conditions, a blockchain solution could address the HIPAA Privacy Rule by separating and encrypting identity, PII and PHI into segregated entities that can be accessed through the blockchain based on KSI hierarchies. As addressed in the interoperability section, patients can share distinct identity attributes with the health care ecosystem on as-needed-basis.

At the same time, the type of high level demographic information stored on the blockchain requires careful consideration; a combination of this demographic information paired with location data, could in theory allow for the triangulation of a

# 5 Shaping the **Blockchain** Future

Blockchain technology creates unique opportunities to reduce complexity, enable trustless collaboration, and create secure and immutable information. HHS is right to track this rapidly evolving field to identify trends and sense areas where government support may be needed for the technology to realize its full potential in health care<sup>13</sup>. To shape blockchain's future, HHS should consider mapping and convening the blockchain ecosystem, establishing a blockchain framework to coordinate early-adopters, and supporting a consortium for dialogue and discovery.

## **Map and convene the ecosystem**

Blockchain technology is evolving rapidly, and new developments emerge weekly. As the technology advances and new applications become possible, the Office of the National Coordinator can play a valuable role in convening stakeholders from health care providers, plans, life sciences companies, startups and academics to discuss progress, share lessons learned, and identify unanswered questions. To that end, HHS could develop a sensing mechanism to track promising new startups and establish a forum for connecting them to more established organizations to undertake experiments.

## **Establish a consortium to experiment**

HHS has an opportunity to support a health care consortium to test blockchain technology. As blockchain matures in health care, the financial services industry could offer valuable lessons learned. R3 CEV is a consortium comprised of financial services industry veterans, technologists, and over 40 financial institutions. A similar consortium could support the exchange of electronic medical records in early blockchain trials. HHS could play a vital role in forming and convening select players for experimentation.

## **Design and execute experiments**

Blockchain experiments could help HHS to determine what the technology can readily accomplish. The experiment design should look to addressing holistic work stream problem sets with transactions crossing multiple parties from creation to archival storage. Creating the experiment early and following it through complete transaction cycles can help developers and policy makers to address friction points and identify areas of advantage prior to nationwide implementation.

## **Consider the investment**

The investment into blockchain technology is growing in industry and the major consortium R3 recently requested \$200M in funding to pay for the blockchain enterprise experiments. The level of investment is fairly low if the estimated annual savings of \$20B becomes a reality<sup>12</sup>. The potential efficiencies, cost savings and increased security could save government and industry billions of dollars. In a resource constrained environment, however, existing capabilities or technologies could be leveraged for near-term benefits while targeted experiments can demonstrate where blockchain technology might create transformational, long-term value.

## **Establish suggested guidelines for blockchain in health care**

Similar to the Internet, blockchain's potential increases with the number of participants in the network; yet for all participants to derive value from the network, a common approach is needed. The Office of the National Coordinator may issue guidelines for standardizing and storing data on the blockchain. Specifically, ONC could evaluate which information should be stored on or off the blockchain and the format in which it should be stored.

Blockchain technology, while still nascent, presents numerous opportunities. A blockchain-enabled, trusted exchange of health information can provide longitudinal views of patients' health, generate new insights about population health, and support the move toward value-based care. With greater transparency, trust, and access to data, HHS can then also garner insights for better safety, effectiveness, quality, and security of foods, drugs, vaccines, and medical devices. The promise of blockchain has widespread implications for stakeholders in the health care ecosystem. Capitalizing on this technology has the potential to connect fragmented systems to generate insights and to better assess the value of care. In the long term, a nationwide blockchain network may improve efficiencies and support better health outcomes for patients.



## Endnotes

1. Deloitte Consulting LLP analysis.
2. If this condition is not met, a shared database may be a more appropriate solution.
3. Redman, Jamie. (2016, May 28). Prescript Brings Medical Prescriptions to the Blockchain. Retrieved August 3, 2016, from <https://news.bitcoin.com/prescript-blockchain-prescriptions/>
4. Higgins, S. (2016, March 3). 40 Banks Trial Commercial Paper Trading in Latest R3 Blockchain Test. Retrieved August 3, 2016, from <http://www.coindesk.com/r3-consortium-banks-blockchain-solutions/>
5. Ethereum. Retrieved August 3, 2016, from <https://www.ethereum.org/>
6. Linux Foundation. What is the Hyperledger Project? Retrieved August 3, 2016, from <https://hyperledger.org>
7. HHS Strategic Plan: FY 2014 - 2018. (n.d.). Retrieved August 03, 2016, from </about/strategic-plan/>
8. U.S. Department of Health & Human Services - Office for Civil Rights. (n.d.). Retrieved August 03, 2016, from [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)
9. IBM 2015 Cost of Data Breach Study. (2015). Retrieved August 03, 2016, from <https://securityintelligence.com/cost-of-a-data-breach-2015/>
10. Bitcoin - Daily Number of Transactions. (n.d.). Retrieved August 03, 2016, from <http://www.coindesk.com/data/bitcoin-daily-transactions/>
11. Meaningful Use | Introduction. (2016, May 26). Retrieved July 13, 2016, from <http://www.cdc.gov/ehrmeaningfuluse/introduction.html>
12. Williams-Grut, O. (2016, May 13). Blockchain startup R3 is raising \$200 million from big banks - but one of them is 'throwing stones' Retrieved August 03, 2016, from <http://www.businessinsider.com/blockchain-r3-raising-money-big-banks-pushback-2016-5>
13. This white paper was developed in response to the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology (ONC) ideation challenge—*The Use of Blockchain in Health IT and Health-Related Research*. It was selected as one of the winning papers from a field of over 70 submissions from a wide range of individuals, organizations, and companies addressing ways in which blockchain technology might be used in healthcare.

## Glossary

**Blockchain:** A shared, immutable record of peer-to-peer transactions built from linked transaction blocks and stored in a distributed ledger.

**Permissionless Blockchain:** A blockchain that allows anyone to join and that rewards miners for verifying transactions with tokens.

**Permissioned Blockchain:** A blockchain that requires users to be added by an administrator. It uses mining or a voting system to verify transactions, which are not necessarily incentivised with tokens.

**Keys:** Addresses used to validate and secure transactions. Public keys can only be used to view the balance and transactions. To make transactions, a private key is needed to verify ownership of an account.

**Node:** A computer connected to the blockchain network that stores a copy of the public ledger. Some nodes also mine to verify transactions.

**Mining:** The process of validating transactions on the blockchain network.



# Authors

**RJ Krawiec**  
Principal

**Florian Quarre**  
Senior Manager

**Jason Killmeyer**  
Senior Consultant

**Dan Housman**  
Director

**Dan Barr**  
Manager

**Adam Israel**  
Consultant

**Mark White**  
Principal

**Allen Nesbitt**  
Manager

**Lindsay Tsai**  
Consultant

**Mariya Filipova**  
Senior Manager

**Kate Fedosova**  
Senior Consultant

# Deloitte.

## About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

## About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2016 Deloitte Development LLC. All rights reserved.