Adopting Blockchain Technology for Electronic Health Record Interoperability

Submitted by Cognizant Technology Solutions
Authors: Nitesh Gupta, Anand Jha, and Purna Roy

Introduction

Most healthcare data lives in silos, each with its own storage structure and descriptive semantics. That reality makes it difficult for patients, providers, payers and other stakeholders to freely, yet securely share clinical and administrative data, let alone assemble an interoperable electronic health record (EHR) exchange or repository. This inability to make patient data available when and where it is needed is expensive. Multiple sets of patient demographic data may be stored by different providers in the same health system. Tests are duplicated. Prescription data is incomplete, increasing chances for adverse drug interactions. Physicians lack historic context for treatment decisions. Population health and case managers must manually collate data from different systems to piece together a portrait of a patient's total health.

The Office of the National Coordinator for Health Information Technology (ONC) has identified interoperability of health IT systems as a potent cure for these issues. However, achieving that interoperability has been challenging. Healthcare has many competing electronic health record vendors with proprietary systems, and many intermediaries with different data priorities and formats, such as claims clearinghouses and pharmacy benefit managers. Privacy, compliance and security issues also have slowed interoperability.

Blockchain technology has the potential to address interoperability challenges in clinical and research settings as well as administrative. Defined very simply, blockchain enables the creation of digital transaction ledgers that can be securely shared among a wide group of stakeholders. The technology enables these parties to directly exchange data via a shared ledger using proven public and private key cryptography. Furthermore, it uses a "proof of work" concept among ledger keepers, who are known as "miners," to validate transactions and ensure a virtually impenetrable and immutable, yet public, ledger. The impenetrability results from the fact the amount of compute cycles needed to corrupt or break the ledger is prohibitive. "Permissioned" blockchains, in which key stakeholders are verified and agree to follow common policies and procedures, may use a more limited consensus-building process that relies on smaller groups of trusted entities to achieve proof of work.

While blockchain capabilities are applicable across the healthcare value chain, EHR interoperability is a critical area to address. Here blockchain could offer an array of benefits and capabilities that align with ONC, Personalized Medicine Initiative (PMI) and Patient Centered Outcomes Research (PCORI) objectives as well as the industry's need to reduce costs, improve quality and shift to value-based, patient-centric care while maintaining the security and privacy of personal health information (PHI).

This white paper explains how blockchain could enable a comprehensive, interoperable and secure EHR data exchange in which health consumers are the ultimate owners of their EHRs. It reviews the blockchain's growing maturity and healthcare industry developments that could enable its wider adoption as a cornerstone for EHR interoperability. It also examines the underlying technology that powers blockchain security, privacy and data integrity.

Blockchain in Brief

Blockchain may be best known as the technology that underlies crypto-currencies such as Bitcoin. However, blockchain has a more general-purpose role resulting from inherent properties such as immutability and integrity of records and strong confidentiality and authorized access. It is based on cryptography, public and private key infrastructure (PKI), distributed peer-to-peer processing and an algorithmic protocol known as "proof of work" that safeguards the ledger's immutability. These extend blockchain's potential far beyond funds transfers to exchanging clinical test results, physician orders, prescriptions, patient queries, etc. It could even support intelligent medical documents with built-in rules to enforce value-based reimbursement contracts and bundled payment programs.

A block may contain transactions or other records (such as an EHR), or metadata records (data about data) about the actual data, such as patient ID, visit number, provider ID, etc. These transactions and records are created by different nodes on the network, such as a provider or a consumer uploading health data. Only after a block is validated is it time-stamped and added to the chain of other validated blocks. Further, the new block is inextricably linked to the block ahead of it. Altering one block in the chain would require changing all the blocks in the chain. This gives reasonable confidence to parties across the healthcare ecosystem that data on the blockchain is authentic and immutable (please see the sidebar following the conclusion for more about building consensus and chaining blocks).

Applying Blockchain to EHR Interoperability

Two distinct approaches have emerged for solving EHR interoperability via blockchain thinking and technology:

1. One scenario envisions the blockchain as a data repository. In this vision, the EHR is stored directly in a blockchain purpose-built for the healthcare industry. The blockchain's use of digital signatures to create a unique patient identifier ensures all records on the chain bearing that identifier are linked to create a comprehensive EHR for that patient across his/her providers and payers. Stakeholders with the appropriate permissions may access the EHR as well as contribute to it. The drawback to this approach is that it would require blockchain infrastructure to scale massively to support complete EHRs.

2. Another scenario envisions storing only the metadata about health and medical events on the blockchain (let's call this the "health metadata blockchain"), such as patient identity, visit ID, provider ID, payer ID, etc. along with a pointer to the actual EHR record stored in a separate universal health cloud (let's call this "Health One Cloud"). The health metadata blockchain avoids the scalability challenges that placing data-intensive EHR records in their vast numbers directly on the blockchain may impose on the technology. The health metadata blockchain and Health One Cloud together comprise a holistic

solution that enables secure exchange of EHR data and overcomes incompatibilities among systems at the provider level.

This would be superior to today's common level of interoperability via health information exchange, illustrated in Figure 1.

EHR Interoperability through a Health Information Exchange

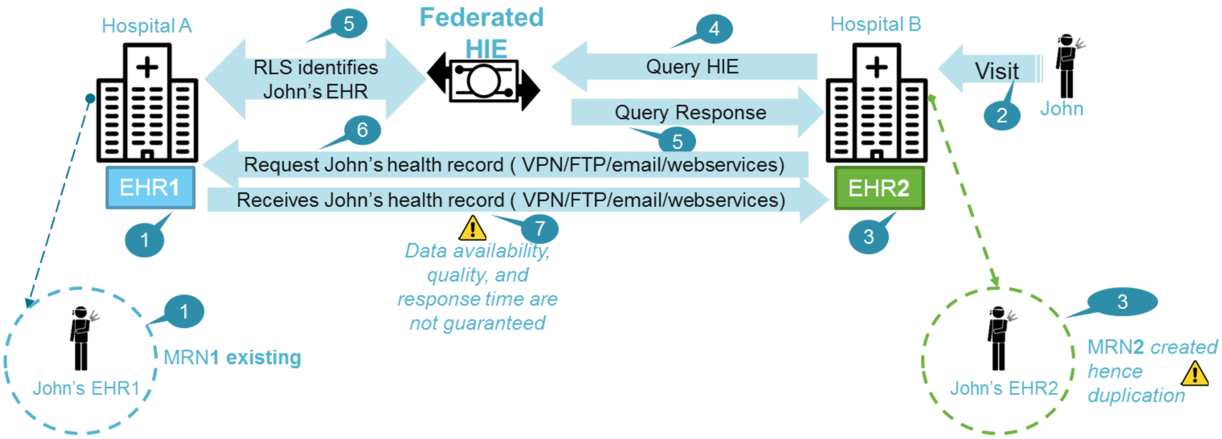

Hospital A
5
RLS identifies John's EHR
Federated HIE
4
Query HIE
Hospital B
Visit
John
2
Query Response
5
6
Request John's health record (VPN/FTP/email/webservices)
EHR1
Receives John's health record (VPN/FTP/email/webservices)
EHR2
1
7
Data availability, quality, and response time are not guaranteed
3
1
MRN1 existing
John's EHR1
3
MRN2 created hence duplication
John's EHR2

Figure 1

As shown above, Hospitals A and B have different EHR systems and use a federated health information exchange (HIE) to exchange data. John's first consultation (1) is with Hospital A; the EHR is thus owned by hospital A. John later visits Hospital B (2). Hospital B creates and owns a new EHR for John (3). Now two records and two separate patient identifiers exist for the same person.

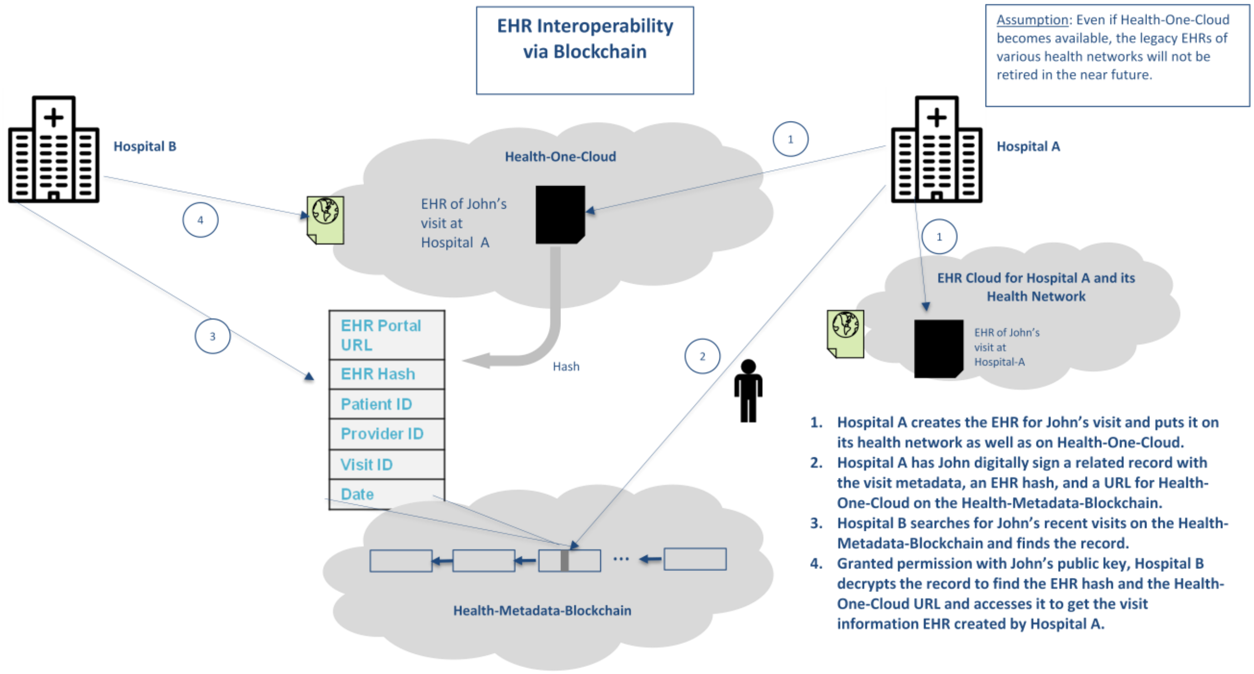
Hospital B queries the HIE record locator service (RLS) to identify past clinical data about John (4). The HIE identifies the existence of Hospital A's EHR for John and communicates this to Hospital B (5). Hospital B contacts Hospital A to get the information (6). Hospital A sends the data through secure email or web services or virtual private network or File Transfer Protocol (7).

While limited interoperability may be achieved in this scenario, the detail of John's follow-up encounter at Hospital B might not be shared with Hospital A. There is also no mechanism to prove which provider or clinician updated the record or to determine whether data has been altered.

EHR Interoperability with Blockchain and Health One Cloud

The scenario becomes quite different when blockchain thinking and technology are applied. As illustrated in Figure 2, Hospital A creates a new EHR for John, a new patient, in its EHR system of record as well as on Health One Cloud, a universal, cloud-based EHR available to all participants in the health metadata blockchain (1). The hospital also creates a digital record containing a hash of John’s EHR entry plus his universal patient ID, the visit ID, the hospital ID and date.

John has a unique digital ID or signature, i.e., a pair of private and public keys. Hospital A asks John to use his private key to sign the digital record with the EHR hash it created (2). This key could be stored on John’s PC or on a flash drive, so he could sign via email or on-site, respectively.


EHR Interoperability via Blockchain
Hospital B
Hospital A
Health-One-Cloud
EHR of John’s visit at Hospital A
1
1
2
3
4
EHR Cloud for Hospital A and its Health Network
EHR of John’s visit at Hospital-A
EHR Portal URL
EHR Hash
Patient ID
Provider ID
Visit ID
Date
Hash
...
Health-Metadata-Blockchain

Assumption: Even if Health-One-Cloud becomes available, the legacy EHRs of various health networks will not be retired in the near future.

1. Hospital A creates the EHR for John’s visit and puts it on its health network as well as on Health-One-Cloud.
2. Hospital A has John digitally sign a related record with the visit metadata, an EHR hash, and a URL for Health-One-Cloud on the Health-Metadata-Blockchain.
3. Hospital B searches for John’s recent visits on the Health-Metadata-Blockchain and finds the record.
4. Granted permission with John’s public key, Hospital B decrypts the record to find the EHR hash and the Health-One-Cloud URL and accesses it to get the visit information EHR created by Hospital A.

Figure 2

This signed record is tagged with the metadata of the visit (patient ID, visit ID, provider ID, date) in the clear and can then be pushed into the health metadata blockchain. The clear metadata tags make the record searchable using the metadata as search keys. The metadata about John’s visit to Hospital A is available to all the participating stakeholders, or nodes, on the blockchain. However, only stakeholders with John’s public key may decrypt the block/record to find the EHR hash.

When John later visits Hospital B, personnel there search the health metadata blockchain using John’s universal patient ID and find John’s Hospital A digital record, described above. John provides his public key to Hospital B, thereby granting access to decrypt the found record. Once Hospital B decrypts this record, it sees a hash of Hospital A’s EHR for John’s visit. Using the hash, which functions similarly to an authorization token or barcode, Hospital B can find John’s EHR in the Health One Cloud.

It should be noted constructing the Health One Cloud would require the industry to agree on universal EHR data standards, and individual institutions are likely to maintain their own underlying EHR systems of record. As an interim step toward realizing the Health One Cloud, the EHR pointers of the health metadata blockchain could point to portals into the EHR systems of record maintained by individual providers. The pointers could be combined with a hash of an EHR itself and as described above, the hash would act like an authorization token or barcode for accessing records via provider portals.

This concept could be piloted with a small control group to help understand how to incorporate blockchain record creation into clinical and administrative workflows and gauge its impact on clinician and patient experiences.

Blockchain EHR Data Exchange Interoperability and the ONC Interoperability Goals

This EHR metadata blockchain and its complementary technology offer benefits that can enable the healthcare industry to overcome some of the most persistent roadblocks to interoperability and help further the goals of the ONC, PMI and PCORI in creating patient-centered, value-driven care.

Patient Benefits

- **A patient-owned and portable EHR**. A blockchain-referenced EHR would be uniquely linked to an individual health consumer vs. an institution. Any clinicians with blockchain access can publish encrypted metadata linked to the consumer's unique digital identifier. With the individual's permission and public key, other caregivers may access and add to this data so the record can be comprehensive. Finally, no matter how often consumers change physicians or health plans, their blockchain-referenced EHRs, EHR metadata and unique identifiers will follow them.

- **Confidentiality, authorized access and trust**. The use of multiple digital signatures via PKI and cryptographic hashes ensures health metadata and EHR hashes travel the network securely and are accessible only to those parties with the correct public keys to access them. Multi-signature technology layered onto the blocks can offer different levels of access and data entry rights (e.g., physicians may add prescriptions; pharmacies may only read them). The data and transactions on a blockchain are made tamper-proof via the cryptography and time stamping, making blockchain data trustworthy.

- **Smart contract enforcement**. Smart contract technology coded into the metadata blocks can carry instructions and data about insurance data, emergency contacts, living wills, etc., so patients have assurance their rights and wishes will be carried out even in emergencies.

Provider Benefits

- **Unique patient identifier, identity proofing and authentication.**
With the EHR metadata blockchain, every provider, patient, payer, health system, record, medical device, wearable, etc., will have its own, unique digital signature created with the combination of private and public keys. These capabilities will help achieve the ONC's goal of "accurate individual data mapping" by making it much easier to assimilate all data belonging to a single patient, device or institution regardless of its source.

- **Data integrity.** The EHR hash stored on the blockchain is a one-way hash, i.e., there is no way to reverse engineer the EHR from its hash. No two EHRs will produce the same hash either. This fact, along with the immutable quality of the blockchain public ledger, ensures no one can alter the provider's EHR record after the fact.

Public Health/Research Organization Benefits

- **Research facilitation**. Multi-signature records on the chain can control and grant EHR access permissions to researchers and institutions. The unique digital signatures carried by all stakeholders, data and transactions in a blockchain will streamline the process of creating aggregated—and accurate—research data sets by preventing information fragmentation and enabling correct merging of records.

- **Secure access to timely data**. With proper permissions, researchers with PMI and other initiatives will be accessing up-to-date records. Apps and application programming interfaces on top of the blockchain infrastructure could allow research organizations to use the EHR metadata blockchain to request and securely receive EHR data.

Industrywide Benefits

- **Audit and compliance**. Blockchain technology can track and timestamp each access of and addition to an EHR, providing an immutable audit trail while ensuring the most recent version of the record is always used.

- **EHR update alerts**. These can be broadcast to all participating stakeholders via the blockchain's distributed ledger and peer-to-peer communication.

- **Reduced costs via disintermediation**. Blockchain's distributed peer-to-peer verification of blocks ensures that many nodes on the network build consensus and verify the transaction or data. This eliminates the need for centralized sources of verification, such as records vendors and clearinghouses, while still ensuring data security.

- **Data redundancy**. A block cannot be deleted once it is added to the blockchain, and the replication of metadata at all the nodes, plus distributed storage of the blockchain-referenced EHR in the cloud, ensures a single point of failure is not catastrophic.

Creating the EHR Metadata Blockchain: Challenges and Opportunities

A multi-modal EHR metadata blockchain would link the EHRs of multiple healthcare entities and consortiums to deliver the most comprehensive EHR and record interoperability. It would include the most stakeholders, who would mutually grant each other permission to participate, and preserves the decentralization of data verification that is essential to blockchain security and value. It could also connect to complementary industries, such as finance, to incorporate payments and reimbursements.

However, greater technology maturity and clear governance and regulations are necessary to spark industry-wide adoption of the EHR metadata blockchain. Issues to address include:

- **Creating a healthcare-specific metadata blockchain**. An EHR metadata blockchain would require much greater throughput rates and processing speeds than blockchain-for-Bitcoin achieves (Bitcoin carries a very small fraction of the world's financial transactions). The blockchain metadata structure would also need great flexibility and capacity to manage metadata about hundreds of thousands of EHRs.

- **Public adoption and usability challenges**. Managing private keys could be challenging for health consumers and other stakeholders. Each private key is randomly generated and thus unique; there is no "reset password" function in cryptography. Further, if a private key is lost or stolen, a person has lost their digital health identity and as yet, there is no recourse to restoring that identity. A central authority (i.e., secure vault) could hold master access to retrieve or otherwise manage lost private keys. However, entrusting private keys to the vault breaks the blockchain principle of elimination of trusted third parties.

- **System integration.** The industry would adopt the EHR metadata blockchain with a "deploy and surround" approach vs. rip and replace because of stakeholders' extensive investments in EHR systems. Important integration issues to address include linking existing EHRs in various systems to unique digital patient identifiers; integrating EHR metadata elements into clinician workflows at the point of care; and assimilating developments such as data generated by wearable devices and the Fast Healthcare Interoperability Resources (FHIR) application programming interface for exchanging health records.

- **Blockchain to blockchain communication**. Developing a way to create references between related records in distributed blockchain ledgers in different industries will be important. A payment record on a financial services chain could be linked to an EHR, and outcomes data from EHRs to a clinical trial on a pharmaceutical or academic chain. These links would make it easier to identify data relevant on various chains to the work of PCORI and the PMI, population health programs, disease surveillance, clinical research, supply chain traceability, evidence-based care evaluations, etc.

- **The type of block chain model** the industry will adopt, its costs, and which stakeholders will decide on policies, procedures and operating standards. Policies must define the entities who can participate in proof of work consensus building; which entities can share transactions; and set standards for syntax, semantics and transport services.

- **Determining blockchain technology compliance** with existing regulatory requirements, such as whether the pseudonymity provided by cryptography aligns with HIPAA requirements.

- **Providing legal clarity** about whether blockchain's concept of built-in trust may replace existing contract methods among trading partners, such as business associate agreements, memorandum of understanding, memorandum of use, etc.

Blockchain EHR Interoperability: A Compelling Value Proposition

While some stakeholders, including EHR vendors and transaction intermediaries, may be disintermediated via blockchain EHR interoperability, many others should see the strong value of the concept.

- Patients have more control over their records and privacy.
- Large providers may preserve their existing EHR systems investments while still leveraging and participating in the efficiencies of the blockchain.
- Small providers would not need their own EHR systems but could view and edit records via the blockchain.
- Health plans and government payers can reduce fraud and waste when immutable claims are linked to immutable encounter records.
- Government, community health agencies and researchers would be assured EHR data is up to date and immutable; further, it will be easier to track permissions and aggregate data for studies with greater confidentiality.

Current projects and proof of concepts around the world can provide lessons for the U.S. healthcare industry in adopting blockchain.[i] Practices also are emerging from the financial services industry that healthcare can build on. Based on our work creating blockchain proof of concepts, we have observed the following:

- Blockchain for private enterprise does not necessarily require a proof of work; a permissioned, private blockchain is best suited among trusted trading partners.
- Blockchain in a private-public partnership model will require proof-of-work/proof-of-stake so a public permissioned consortium blockchain would be appropriate.
- Distributed applications, or “Dapps,” are a way for stakeholders to interface with blockchain; a blockchain app store could be developed.
- Next-generation blockchain solutions are required for better integration of blockchain with enterprise systems.
- Smart contracts on blockchain are a potential area of vulnerability and so the quality of the code and standards used to create them are critical.
- Specialized health “wallets” could be created to streamline EHR metadata management on the blockchain and help consumers and institutions track their EHR transactions.

Conclusion

An overarching governing body including public and private entities should own the EHR metadata blockchain and verify the entities allowed to act as “permissioned” blockchain participants to build consensus and also help create and enforce standards about privileges granted to specific types of nodes (i.e., patients will only have access to their EHR but entities like providers can access EHR for all patients, etc.). Early proof of concepts could focus on trials of the EHR metadata exchange concept and blockchain’s unique patient identifier within a small network of trusted parties to collect data about user acceptance and how blockchain could become part of the clinical work flow.

Finally, health stakeholders should take advantage of the light-speed pace of digital technology advances by participating in cross-industry development of blockchain and evaluate emerging complementary computing platforms, applications and open application programming interfaces. Blockchain may well reshape how industries adjacent to healthcare conduct business, from supply chain and logistics players, through hard goods manufacturers, to financial services firms to higher education institutions. By creating a blockchain specific to its requirements, the healthcare industry will be positioned to participate in a wider blockchain mesh to gain still more efficiencies and economies of scale.

Sidebar: A Deeper Look at Blockchain and Its Proof of Work Concept

The blockchain-enabled EHR data exchange discussed in this paper envisions a “permissioned” blockchain. This blockchain would have a governing authority to verify participants and their data access permission levels. Permissioned participants creating metadata transaction blocks could agree to accept encrypted and signed blocks from each other as authentic and forgo the “proof of work” consensus-building step that is an integral aspect of the Bitcoin blockchain.

Given healthcare’s strict privacy and security requirements, however, a health blockchain governing body might still leverage the proof of work concept in some fashion, such as using a small group of trusted entities to act as “miners” and build consensus to ensure stakeholders are following the agreed-on operating principles. Further, some form of consensus-building may yet be required of health blockchain participants when they wish to share data with other industry blockchains.

So it is worth reviewing proof of work and where it fits into the more typical blockchain-based transaction model. (Note that in the following description of the proof-of-work blockchain process, “record” is italicized to differentiate it from an EHR or other medical record. “Records” in blockchain may be transactions, data, etc.)

1. **Defining the transaction.** An entity wishing to add a new *record* to the blockchain public ledger will use its private key to encrypt and transmit the *record*. The private key would create a unique digital signature that authenticates the message.

2. **Authenticating the transaction.** The blockchain network receives the message. This network is comprised of thousands of computers and their users who offer some of their computers’ processing cycles to validate blockchain transactions. These nodes authenticate the validity of the message by using the entity’s distributed public key to decrypt the digital signature. In essence, the network itself agrees the new *record* is authentic vs. a single institution or clearing house doing so.

3. **Creating the block**. The newly authenticated *record* is not immediately placed in the ledger. Instead, it is virtually placed in a digital holding area with other recently authenticated *record*s. Many nodes in the network create a “block” that contains a list of recently authenticated *record*s; a header, which is a reference code to the previous block in the chain; and a nonce—literally, a random number.

4. **Verifying the block**. The blockchain network's thousands of nodes now literally compete to validate the new block and add it to the chain through the iterative process called "proof of work."

   Each competing node puts the *list of records*, the header and the nonce from the new block through a secure hash algorithm to generate an output value. If the output value is less than a specific target threshold, the block is validated. If not, the node changes the nonce value and tries again, repeating this process until the calculated output value is less than the threshold.

   If proof-of-work sounds inefficient, that is by design. Solving the hash problem is computing-cycle intensive, and any party wishing to co-opt or corrupt a transaction would need more than 51% of all the nodes' computing power to do so. Further, because the "winning" output value is utterly random, no single node can game the system.

5. **Chaining the block.** The winning node, the first one to solve the puzzle, gets to time-stamp and add the block to the chain and announces this to the network. That block is "chained" by virtue of the fact it is linked to the block ahead of it in the chain, which in its turn is linked to the one before it. Anyone trying to alter one block would thus need to also alter the block ahead of it and the one ahead of that, and so forth. The computing power required to achieve these alterations would be so costly that it is more valuable to participate in the network than to attempt to subvert it.

   In payment blockchain networks, the winning miners receive a commission. An open question is what incentives to provide to miners in any healthcare blockchain to persuade them to offer their compute cycles to validate blocks and achieve distributed consensus.

# # #

About the authors:

Nitesh Gupta, Consulting Manager, Cognizant Business Consulting-Healthcare, Cognizant Technology Solutions

Anand Jha, Director, Cognizant Business Consulting-Healthcare, Cognizant Technology Solutions

Purna Roy, Senior Director, Consulting, Global Technology Office, Cognizant Technology Solutions

Cognizant Technology Solutions has its world headquarters in Teaneck, New Jersey.

[i] Current health blockchain pilots and initiatives include: Guardtime's Keyless Signature Infrastructure (KSI) technology for Estonia e-Health authority; the Philips and Tierion collaboration for data storage and verification using blockchain; Factom and HealthNautica collaboration for creation of secured medical records and audit trails; collaboration between Healthbank (Switzerland), Noser Health (Germany) and Netcetera (Switzerland) to mature a global health data transaction platform.