# Blockchain in health

## How distributed ledgers can improve provider data management and support interoperability

September 2016

EY
Building a better working world

Table of Contents

# I. Executive summary

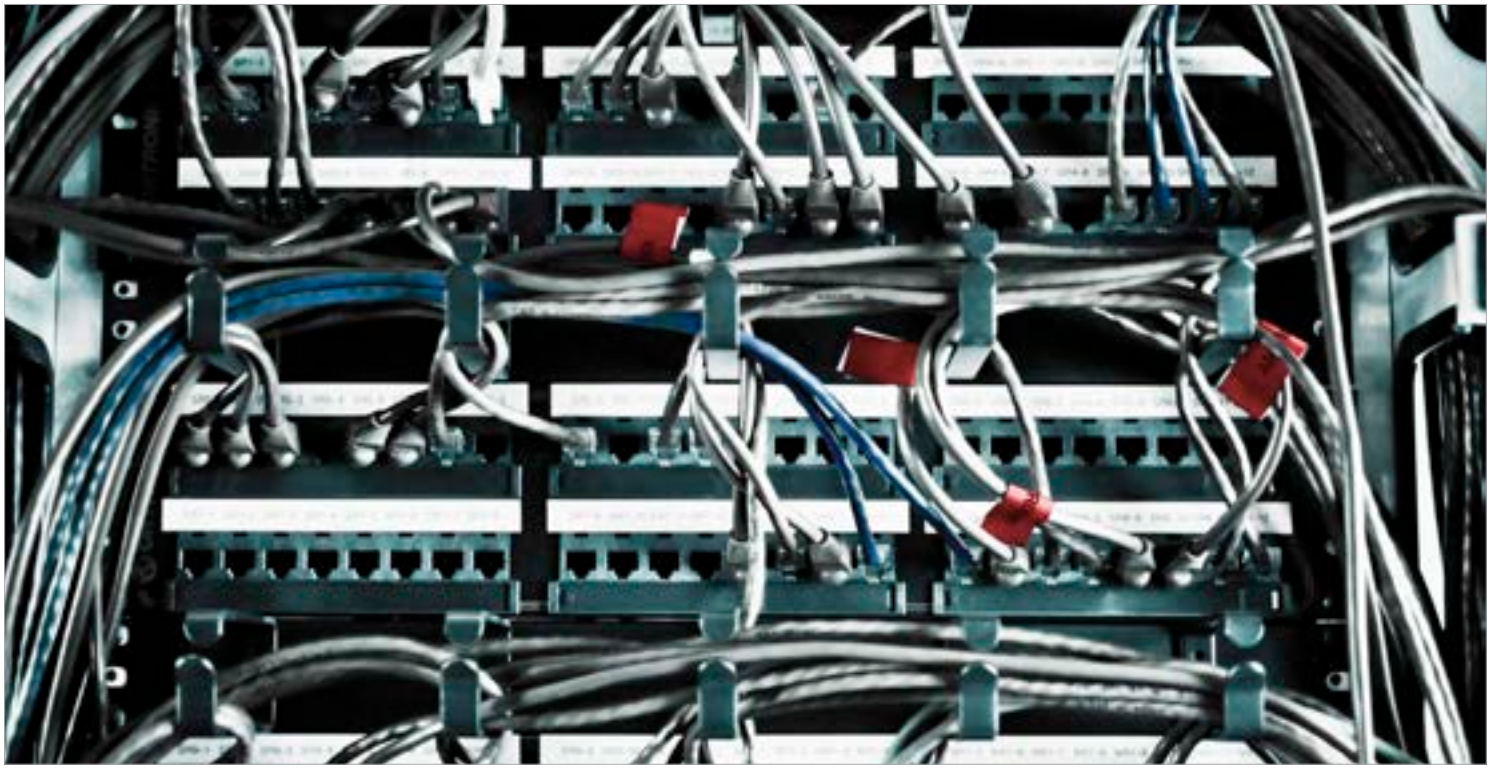
In 2015, the Office of the National Coordinator for Health Information Technology (ONC) published the Shared Nationwide Interoperability Roadmap, laying out a path for the health care industry to improve interoperability over the next 10 years.[1] The ONC acknowledged that the industry had made advances in precision medicine, telehealth and adoption of electronic health records and big data analytics, but there is still progress to be made.

To achieve this future state, the roadmap put forth 16 areas of focus for the industry going forward, including identity, authorization and access, data formats, data transmission, longitudinal health information, and provider workflows. This future will only be achieved by an open technology infrastructure that enables and supports sharing, collaboration, and connectivity.

Blockchains, by providing a trusted environment for data recordation and exchange, are network enablers, providing a foundation and set of technology standards that connect stakeholders, and support the applications used by clinics, hospitals, pharmacies and insurance companies to manage the wealth of data created by the industry. Blockchain technology will fundamentally change how payers and providers share claims information, how provider data is updated and matriculated through a network, how a patient's medical records are shared and updated as she moves through the care continuum (from a primary care provider, to a specialist, to a pharmacist), how population health data is aggregated and analyzed, how clinical trial data is recorded, and how prescription drugs are tracked and monitored through the supply chain.

This paper focuses on one problem that is ripe for remedying: provider data management. Provider data serves as the foundation of payers' provider directories, and it is referenced and relied upon during the claims adjudication process. For years, the industry has struggled to maintain accurate and uniform provider data, due in large part to the fact that the information regularly changes as physicians move locations, join new networks and adjust care offerings.

In this paper, we demonstrate how blockchain technology supports a distributed network of payers and improves processes for maintaining and sharing provider data. We discuss how the identity components inherent to blockchains, combined with credentialing data, can serve as a foundation for a unified provider ID, how cryptography can support the secure permissioning of provider data across payers over the career of a physician, and how blockchain technology can automate and eliminate many of the internal quality control and change request processes at a payer. Leveraging a shared infrastructure can provide new efficiencies to payers and providers and ultimately impact labor costs, reconciliation efforts, auto-adjudication rates, and overall member experience.



[1] National Interoperability Roadmap, The Office of the National Coordinator for Health Information Technology, 2015, https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

# II. Introduction to provider data

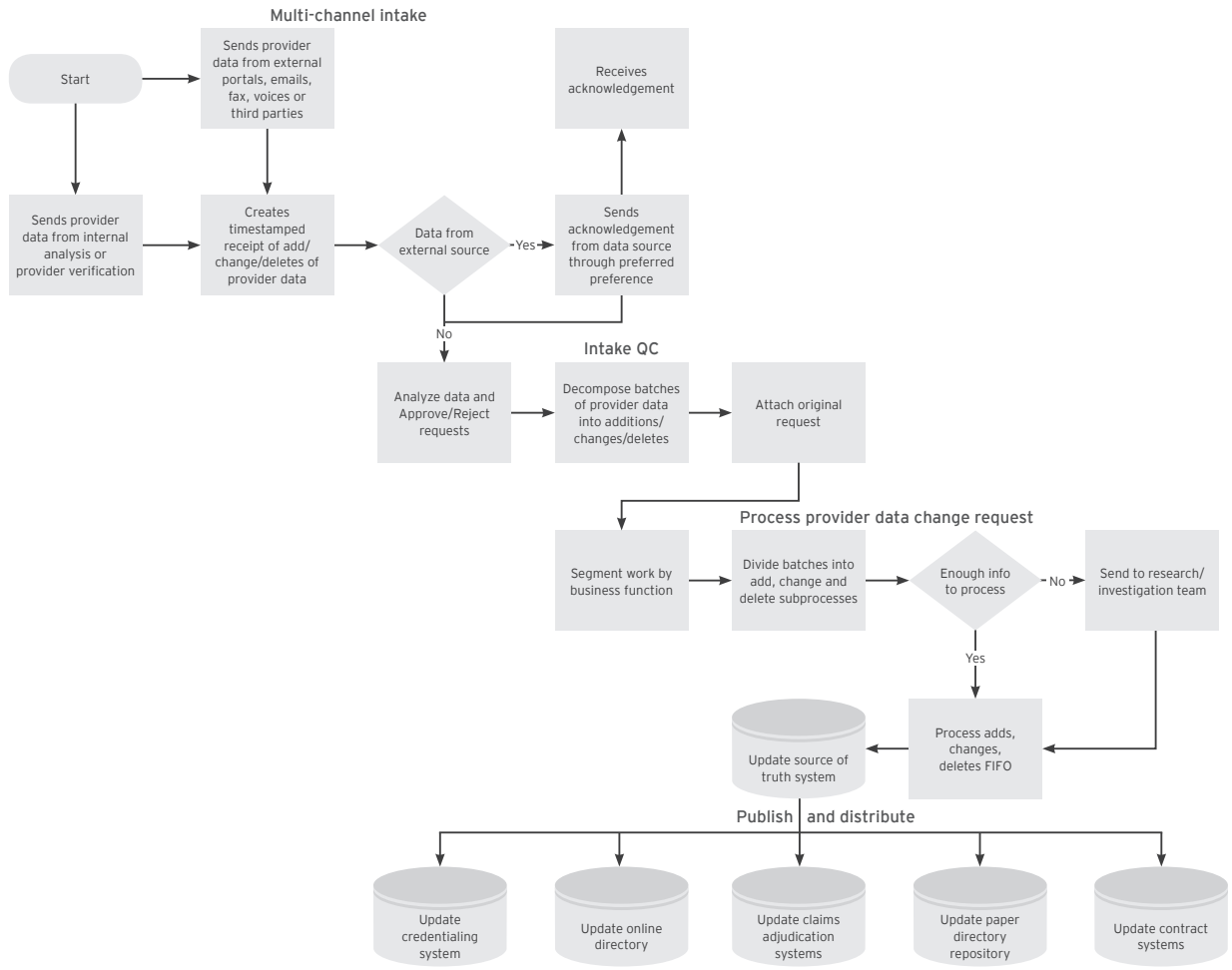
Provider data is a cornerstone of the health information system. Provider demographic information, such as office addresses, provider hours, phone numbers, specialties, and certifications, is used to populate provider directories, which are in turn used by members to find relevant and in-network physicians in their area. Provider data is also critical for claims adjudication. A payer must verify that a reimbursement request came from a credentialed, in-network doctor and that the care delivered is reimbursable under the policy. Maintaining and disseminating accurate and up-to-date provider data is paramount for the industry.

Unfortunately, the quality of provider data is not always commensurate with its value to the industry. Recent studies show that up to 40% of a payer's provider records contain errors or missing information.[2] This is a direct result of providers constantly entering and exiting networks and changing hours and locations. Processes exist for tracking and updating provider information, however, they are manual and extremely siloed due to numerous systems that have to be completely and accurately updated.

The image below shows a typical workflow for updating provider data in a payer's "source of truth" system and related databases.

For a physician participating in multiple networks, updating fields as simple as demographic information is onerous. Each payer reaches out to physicians on a semiannual/annual basis to request confirmation of their demographic information on file. If the information has changed, the physician will provide the payer with updated data. Unfortunately, there is no reliable mechanism for disseminating the physician's demographic

## Typical payer workflow for updating provider data




[2] "A Business Case for Fixing Provider Data" (Whitepaper), LexisNexis. https://www.lexisnexis.com/risk/downloads/whitepaper/fixing-provider-data-issues-whitepaper-wp.pdf

data across multiple payers. The process of verifying and updating the data is repeated by each payer, multiple times a year. In addition to the obvious inefficiencies, there is also a high risk of error. The likelihood of a physician or payer making a mistake during data intake goes up each time it is handed downstream to be updated on web portals, electronic medical record databases, and claims adjudication systems. Another issue is uniformity. Irrespective of errors, the same provider information may be formatted differently across payers. In an industry with a growing focus on interoperability, having standard provider data formats will improve quality and sharing.

This example is meant to highlight how manual and repetitive the process of maintaining and updating provider data can be, and the inefficiencies and risks that are introduced as a result. As mentioned above, provider data is embedded in a number of different health care functions, and poor-quality data can have significant consequences for payers, providers and members. Payers incur the costs of correcting bad provider data, which often involves outreach via phone, email or fax. Payers also incur additional costs associated with manually processing reimbursement claims that fall out of the auto-adjudication process because of inconsistent or mismatched information. Providers may suffer direct financial consequences if members are unable to find or contact them because of bad information. From a member perspective, if provider data is inaccurate or incomplete, this can result in choosing a provider that is actually out of network and/or limiting options of providers to choose from, ultimately increasing cost and decreasing quality of care for members.

Provider data issues are known, and the industry is taking steps to improve both the quality of, and the process for updating, the information. The Centers for Medicare and Medicaid Services (CMS) has imposed new rules on health plans relating to the frequency and manner in which provider directories are updated and accessed. Qualified health plans (QHPs) are required to update their publicly available directory on a monthly basis. Medicare Advantage organizations are also required to contact providers once every three months to verify provider contact information, as well as whether they accept new patients.[3] CMS also requires that health plans make provider directories publicly available in a machine-readable file and format to allow for the creation of user-friendly, aggregated information sources. This level of transparency and accessibility encourages the development of new tools that leverage this information.[4] Plans that do not comply with the new CMS rules could face stiff penalties in the form of fines. Third-party "repositories" have also emerged to assume and consolidate the responsibility of maintaining and updating provider information.

Issues about the quality and dissemination of provider data are clearly top of mind for the health care industry, and while progress is being made, significant investment in technologies and processes that improve the entry, sharing, updating and auditing of provider data is necessary.

# III. Overview of blockchain technology

Database technology is not new; distributed databases have been around for a decade, and relational databases have existed for even longer. Blockchains are another form of database, and while they share many elements with more traditional forms, it is the differences that make them truly innovative. By design, blockchains are intended to be shared, by individuals, organizations, even devices. In a digital world, where databases are the infrastructure, blockchains are common infrastructure — shared "plumbing" through which many data types can be stored, referenced, and transferred — and a mechanism by which that activity can be immutably recorded. The unique aspects of a blockchain are discussed in more detail below:

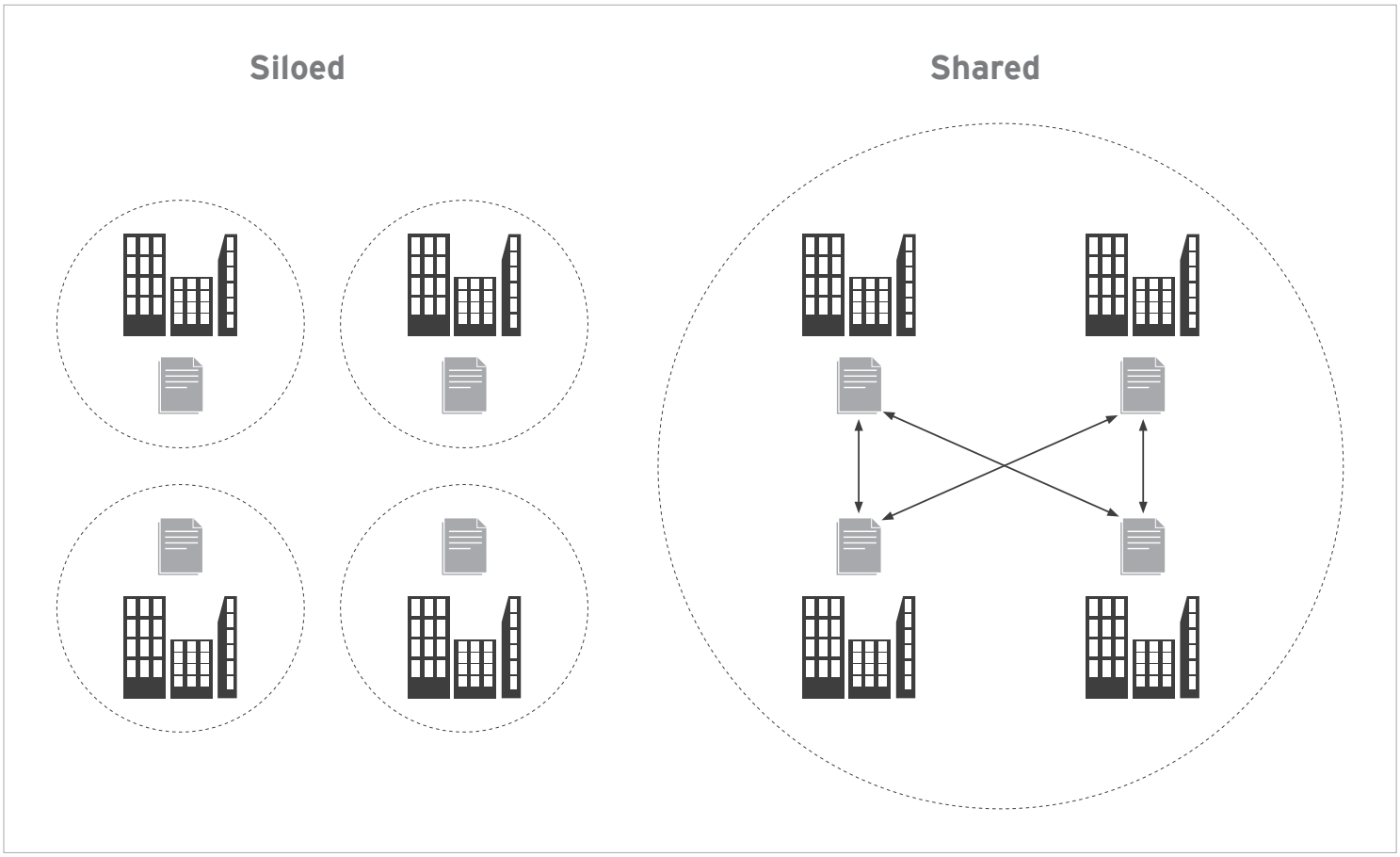
## Identity

Blockchains contain a built-in identity mechanism — a cryptographically secure public-private key pair — used to associate activity on the network with a specific participant (e.g., person, entity, device). By itself, the key pair is pseudonymous, not revealing the participant's actual identity. However, supplemental information, such as name, contact information, or professional credentials, can be associated with a key pair, merging on-chain and off-chain identities. In a health care context, blockchains' unique identity mechanism could provide the foundation for a unified patient ID across payers and providers.

## Permission gradient

Using the identity system as a foundation, permissions can be assigned to participants on a network. Permissions correspond with certain abilities on the blockchain, such as the ability to read or write data. Permissions can be attributed to individuals at the most granular level; for example, an individual could be granted the permission to read and write to Document A, but only the ability to read Document B. Due to the fact that these permissions are also stored on the blockchain, a participant in the network can be certain that the data he or she has uploaded is only accessible by the party to whom access was granted, despite this data being hosted in a decentralized manner.

[3] FierceHealthcare, "CMS tightens provider directory rules for 2016," http://www.fiercehealthcare.com/payer/cms-tightens-provider-directory-rules-for-2016
[4] Final 2016 Letter to Issuers in the Federally-facilitated Marketplaces, February 20, 2015, Center for Consumer Information and Insurance Oversight (CCIIO), Centers for Medicare & Medicaid Services (CMS).




## Immutability

One of the most valuable features of a blockchain-based network is the audit trail, or transaction record. Transactions, or actions (in a non-financial context), on the network are grouped together into blocks for batch processing. These actions may include any amount and type of data, and may range from a simple transfer of a token, to the deployment of a smart contract with complex privileges and abilities. Over time, the blocks of actions form a chronological chain, where each new block necessarily references information contained in the previous block, similar to how each link in a chain fence necessarily overlaps with portions of adjacent links. Because of this "referencing overlap," an attempt to change information in a previous block will necessarily alter the information in all subsequent blocks.

This chronological chain of activity is shared — everyone participating on the network can maintain a complete activity history. In a financial context, this would mean multiple parties can collectively maintain a shared copy of a transaction ledger.

## Transparency (public vs. private)

With blockchains, one size does not fit all. A blockchain-based system can either be open and public, or private and permissioned. Public blockchains are open to anyone. No permission is required to join and participate in the network. They are also inherently transparent; all actions on the network must be validated by, and visible to, all participants on the network. If any action is not visible to all participants, the action cannot be properly validated.

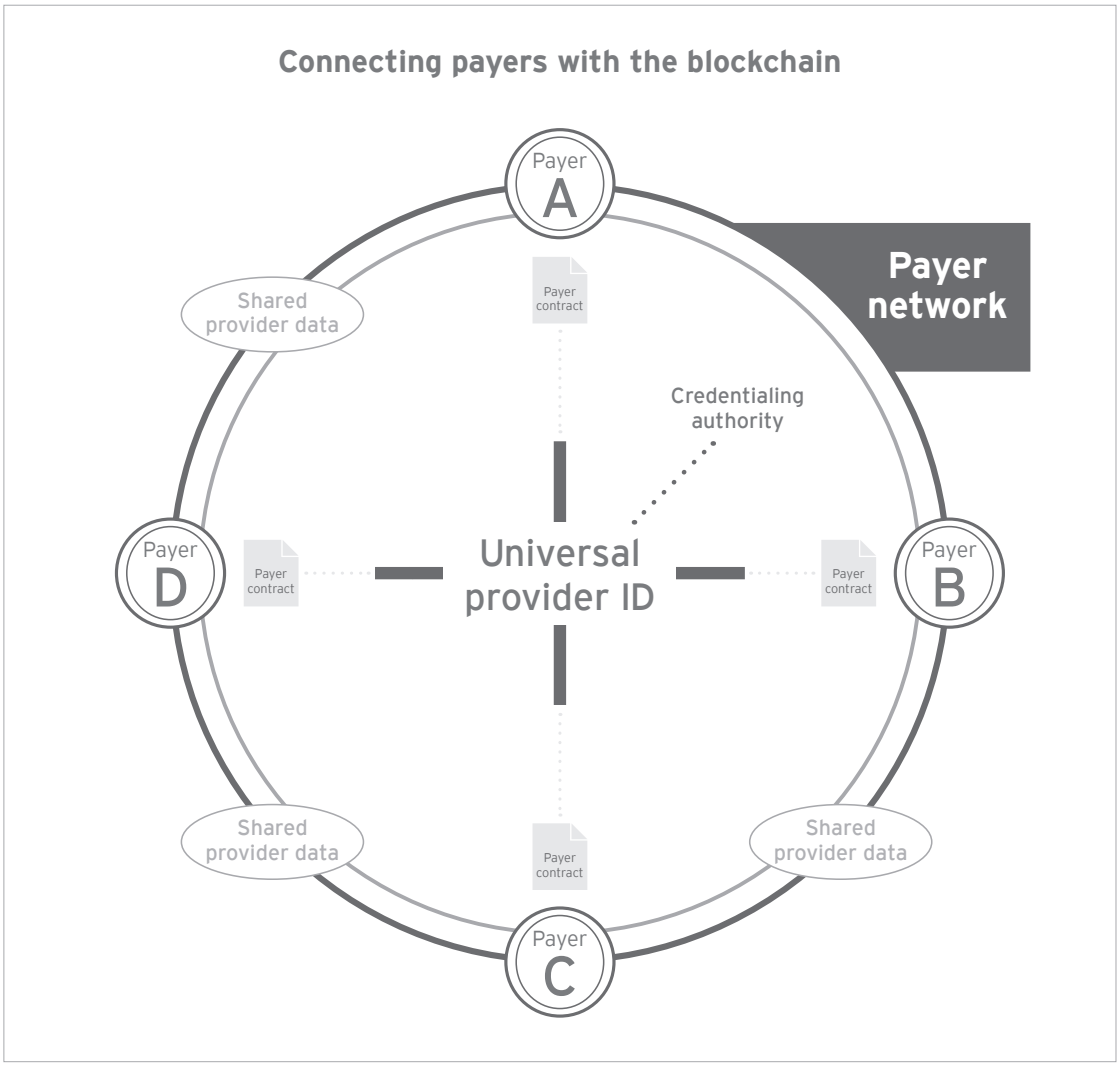
Private, permissioned blockchains are quite the opposite. Permission is required before a participant can join, and thus participate, in the network. As mentioned earlier, participants may be assigned a mix of read and write permissions. Certain participants can have the ability to read and write, whereas others may only have permission to read or write. The ability to assign a variety of permissions to network participants is particularly suited for use in more commercial contexts, like health care, where certain actions and information are not intended to be public. In this example, participants would retain the benefit of a shared infrastructure while maintaining a level of security and privacy.

# IV. A blockchain-enabled solution for provider data

How can blockchain technology be applied to provider data management? Below, we will explore how distributed ledgers can support a network of payers, and manage the exchange of provider data as physicians update their information and move in and out of networks.

## Blockchain as an identity and permission management system

Even though blockchains are technically databases, they are not very efficient at storing large amounts of data due to the inherent duplication required for each participant to maintain a shared copy of the ledger. Large data transactions can take time to fully confirm, and the process can get quite expensive. Instead of storing provider data on the blockchain, we can leverage existing data stores and a blockchain's identity and permissioning features to connect existing "source of truth" databases at payers and securely communicate provider data updates across the network. The result is a network of payers, collectively maintaining a single copy of a provider's data file, and broadcasting changes to the network. The value of shared infrastructure to each participant on the network increases as the network grows. The more payers on the network, the larger the collective pool of provider data. Let's take a closer look at the elements of this new payer network.



## A. Unified provider ID

If a group of payers are going to share provider data, they need a standard for identifying providers across the network. Public keys are helpful, but are usually intended to help the system reconcile updates and permissions, and don't contain the credential and demographic information needed by a payer. Medical licenses on the other hand are the common denominator of all providers, regardless of location, and contain relevant demographic and specialty data. At any point in time a provider could establish its on-chain identity by associating its public key with a valid medical license. The license, now tied to a public key, would be available to any payer on the blockchain network.

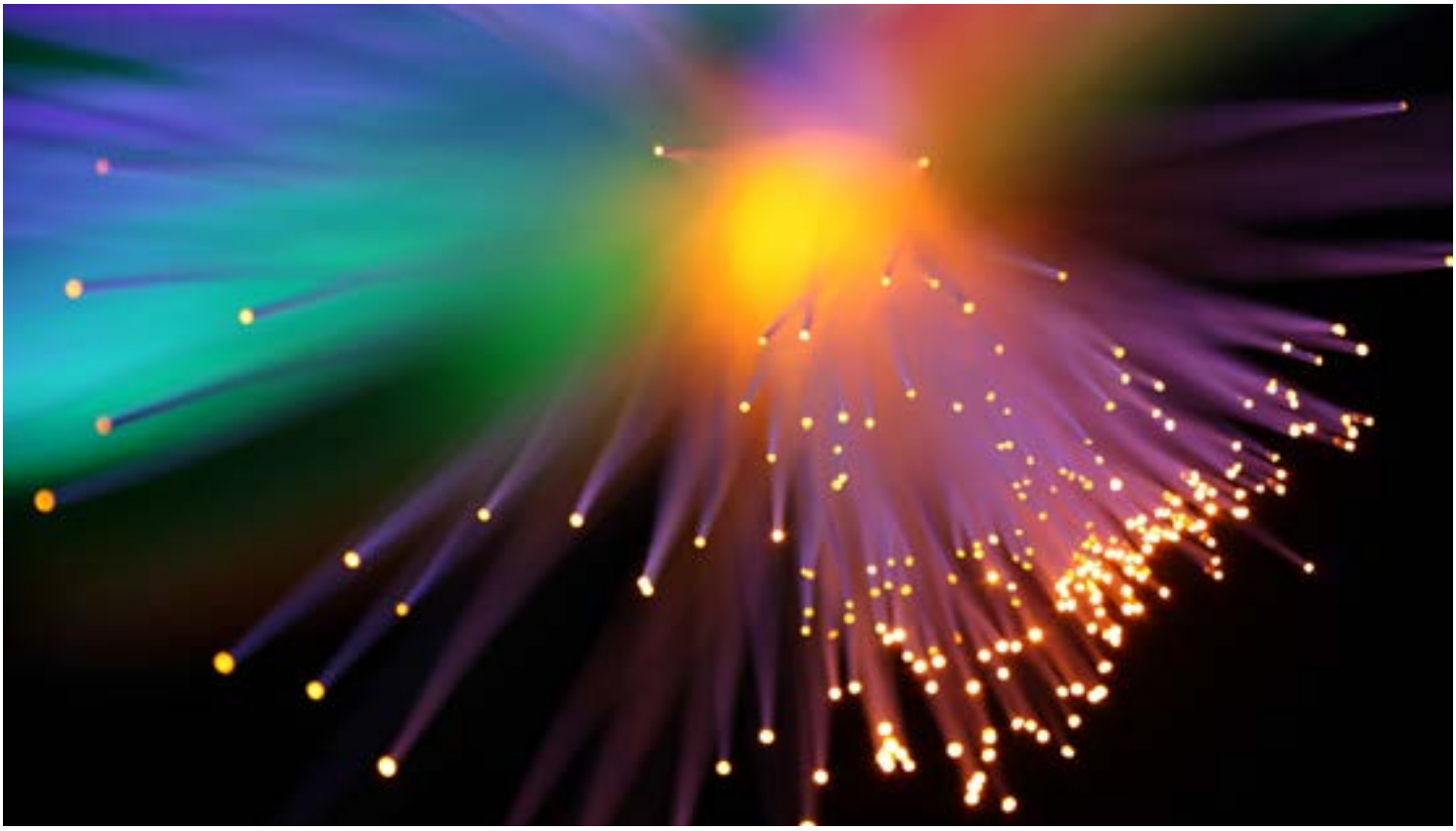
Re-credentialing can occur in the same way. A medical board with authority to credential a provider can submit a new license to the network, automatically updating the provider's record at respective payers. Any suspension or expiration of a license could be updated across the network in a similar fashion. With this model, any change to the status of a license gets distributed to relevant parties on the network in a matter of minutes, as opposed to the periodic, manual updating that is required today.

CMS's National Provider Identifier (NPI) is an alternative data point that could be used to supplement medical credentials and identify a provider. Other attributes, whether they be affiliations or specialty certifications, could also be used to strengthen on-chain identity. Once provider identity is established, other networks and systems can, in theory, be anchored to this blockchain and leverage the existing identity components.

## B. Access

As providers join new payer networks, payers would receive permission to access portions of that provider's data profile that reside with other payers. To illustrate this process, assume a provider has an existing relationship with Payer A. Payer A would maintain a complete and accurate copy of the provider's data file, including credential and demographic information. If the provider joins a second network, Payer B would receive permission to access relevant provider information stored at Payer A. This process would repeat when the provider joins networks operated by Payer C and Payer D.

Provider data can be grouped into categories (demographic data, or credential information, for instance), and providers can assign permissions to relevant categories based on the terms of a network agreement. If certain data is payer-specific, such as contract payment rates, permission to that information would not be granted to other payers on the network. To minimize manual permissioning, smart contracts – small pieces of executable computer code deployed on a blockchain — could be used to automate the granting and revocation of access as providers move in and out of networks.



## C. Updates

Another advantage of using blockchain technology to support a provider data network is the efficient dissemination of additions, changes and deletions to a provider's data file. Because each participating payer maintains "access" to an in-network provider's distributed data file, any payer with access to a portion of a provider's data file would automatically receive the updated information when a payer or provider commits an update to the network.

For example, imagine a provider has just relocated offices. Instead of manually updating her business address for each payer, she makes one update to her demographic data, and the updated information is automatically disseminated and available to all payers with access to her data file. The same process could be applied to the re-credentialing process. Each payer would automatically receive notification and access to the provider's updated medical license within minutes of being renewed by the state medical board. An update anywhere on the system would be broadcast to the network and accessible to permissioned payers.

This process of streamlining changes enables every payer associated with a provider to access to the most recent version of the provider's data profile.

## D. APIs and smart contracts

Health care companies use a myriad of different technologies and systems to support every aspect of their operations. Even in a blockchain-enabled world, some of these technologies and systems (or a subsequent version) will be necessary. Communication across these technologies and systems will be key for interoperability.

A blockchain-based payer network can utilize standard application programming interfaces (APIs) to connect existing data systems. These standard APIs can feed provider data into smart contracts — pieces of executable computer code representing business logic (i.e., payment terms) embedded on a blockchain — to automate portions of the update and permissioning process.

## Cost implications

Provider data management involves many manual processes — provider data intake, quality control, and reconciling updates and changes with all necessary directory and adjudication systems. There are real labor costs associated with these processes that could be eliminated to some extent with the use of a blockchain infrastructure. The intake process would be spread across all payers on the network, decreasing the outreach and intake work performed by any one payer. There is real savings potential from a claims adjudication standpoint as well. Research has suggested that between 4%–6% of all reimbursements claims fall out of the auto adjudication process due to errors with provider data.[5] Improving data uniformity and decreasing manual claims processing can have a tangible impact on the overall cost of adjudication.

Providers are impacted as well. From an administrative efficiency standpoint, instead of updating information with every payer every quarter, providers could submit to any payer on the network, and that update would be propagated to the other network participants. Additionally, having uniform data across a network of payers could have significant revenue cycle management benefits. Uniform data can improve the auto adjudication process, shortening the time between claims submission and payment.

# V. Limitations

For all of its promise, blockchains today are limited by the nascent state of the technology and certain design elements inherent to distributed systems.

## On-and off-chain data

Because a blockchain is technically a shared ledger, a copy of the ledger is maintained by each node on the network. This means that any data stored on the blockchain is duplicated at each node. For this reason, it would be inefficient, and unnecessarily duplicative, to store large amounts of data on a blockchain. Instead, as we suggest in this paper, blockchain technology can be used to connect off-chain data stores, acting as an identity and permissioning fabric between parties on the network.

## Scalability

Activity on blockchain networks has increased every year since bitcoin was released in 2009, but the protocols that exist today are not quite ready to support the speed and volume requirements of the health industry. In a blockchain context, speed and security are often inversely related — more of one means less of the other. This is due in part to a blockchain system's need to have consensus, or agreement on the current state of the ledger. In bitcoin, we look for consensus as to the state of bitcoin balances across all addresses on the network. In the context of a distributed payer network proposed here, we look for consensus as to the state of payer access permissions to provider data files across the network. In either case, consensus requires some amount of computation and time. The amount of each will decrease over time, but it is a limitation of current blockchain systems and something that must be overcome before a blockchain can replace current production systems.

## Technology standards

Before blockchain-based applications can be widely adopted, a set of technology standards must be developed. At the moment, there are several competing protocols that exist — bitcoin, Ethereum, Hyperledger, etc. There are also a handful of other proprietary middleware and application development suites for each protocol.

[5] A "Business Case for Fixing Provider Data," (Whitepaper), LexisNexis; https://www.lexisnexis.com/risk/downloads/whitepaper/fixing-provider-data-issues-whitepaper-wp.pdf

The health care industry would be well served to experiment with different protocols and testing environments, but meaningful vertical development and scalability will only be achieved once a standard has been established.

## Impact dependent on middleware and application layers

The internet as we know it is built on foundational protocols such as TCP/IP and DNS (internet and domain name protocols, respectively). These protocols support and enable consumer-facing applications such as the Web and email. Like TCP/IP and DNS, blockchain is an infrastructure technology, and its value for health care will only be realized by the middleware and consumer-facing applications it supports. The provider data management approach we propose in this paper is one example of an application, and there will be countless others, but development takes time.

# VI. Conclusion

In this paper, we looked at how blockchain technology can improve the process for accessing and updating health care provider data. We discussed how the identity mechanism inherent to a blockchain can support the creation of a unified provider ID, how cryptography can support the secure permissioning of data across a distributed network of payers, and the effect streamlining these processes can have on the cost of provider data maintenance and claims adjudication.

Infrastructure technologies will play a major role in supporting the development of these new networks. As the health care industry looks for novel ways to improve interoperability, blockchain technology is an exciting innovation that can drive efficiencies across the care continuum.


## Ernst & Young LLP contacts

**Dan Gietl**
Americas Health Advisory, Principal
dan.gietl@ey.com
+1 317 681 7483

**Paul Brody**
Americas Stategy Leader, Technology Sector
Global Blockchain Leader
paul.brody@ey.com
+1 415 894 8046

**Angus Champion de Crespigny**
Financial Services Blockchain Strategy Leader
angus.championdecrespigny@ey.com
+1 212 773 6717

**Andrew Beal**
Blockchain Strategy
andrew.beal@ey.com
+1 415 894 4929

**EY** | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.



SCORE 03011-161Gbl
1609-2041699
ED None



**ey.com**