Blockchain and Health Transactions:
The Secure, Distributed Four-Party Health Services Ledger

Max Janasik, CPA and Nicole Cathcart, MA

Blockchain could represent one of the most disruptive and transformative technologies since the Internet, taking the digital world forward with a new distributed model that addresses more complex and secure applications[1]. Healthcare, where privacy, security and complexity are foundational, has natural applications for a technology that can create significant efficiencies and cost savings for the administrative processes driving non-value added costs, while providing the needed security and privacy citizens deserve.

While the potential is great, blockchain is in its infancy. Rapidly, major players in finance and technology are building the infrastructure, middleware, and tools needed to enhance security and broaden applications for blockchain technology. Notably, technology leaders IBM and Microsoft have launched their own projects, with their own models for security, privacy and cryptography.

While the application of blockchain to healthcare might seem distant, the market is moving quickly. Earlier this year data security company Guardtime announced a contract with the Estonian government to use blockchain to secure over 1 million citizen health records[2]. Gem recently launched Gem Health, powered by Ethereum, and partnered with the Philips Blockchain Lab to explore use cases in healthcare that break down silos and enable collaboration[3].

We propose that the true value and adoption of blockchain for healthcare, including the portability and enhanced usability of EHRs, occurs by systematically linking the entire value chain, notably the payment and transaction system, to health data. The initial result is a four-party ledger among consumer, provider, payer/insurer and government governed by smart contracts. The model has significant cost savings implications, supporting the development of a future, expanded Healthcare Consortium. We will also address portability, interoperability and security concerns while presenting Medicare and specific areas of utilization management as a clear first use cases for using blockchain and related technology to transform healthcare.

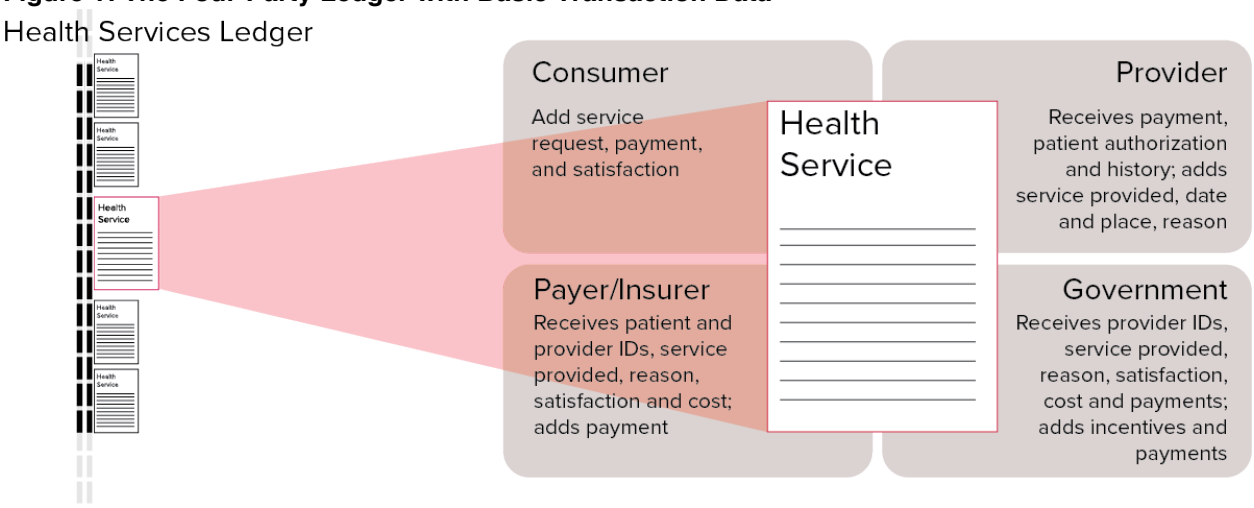
A Four-Party Ledger and The Future Health Consortium

The basic Four-Party Ledger addresses the critical players in the current health data and transaction ecosystem, plus the inclusion of critical data for population health research. The basic transaction in healthcare is a single health service. That service has a number of interconnected data points, including: receiver of care, giver of care, reason for service, service performed, date of service, place of service, cost of service, and associated health metrics and notes.

The first party, the consumer, and the second party, the provider, in the ledger are part of that data. Connected to the receiver and giver of care are existing relationships that address the cost of service—managed through a third party payer/insurer and/or government programs. The fourth party is a government entity that

can use the transactions themselves, devoid of PHI, to analyze health data, or when permission is granted, enrich the data with other patient variables not found in a health service or by allowing a combination of health service transactions related to a single patient. See Figure 1 for an illustration of the transactions in a single service, representing a block in the Health Services Ledger chain.

Figure 1: The Four-Party Ledger with Basic Transaction Data



The Patient-Centered Outcomes Research Institute's (PCORI's) 20 patient networks for chronic condition management[4] represent an ideal existing network of engaged patients and caregivers that may grant permission for research efforts. Ongoing surveys and labs can enrich health service data in the ledger, adding essential medical history or behavior, and also allowing for inclusion of genetic testing and genome mapping for precision medicine applications.

Fundamentally and simply, however, blockchain is a transaction ledger. The intelligence needed in analyzing data and finding meaning in health information to impact program development and improve outcomes would be processed through a different system, an analytics engine. Blockchain merely provides the secure, unique and uniform transactions that can simplify data analysis. Blockchain could take so-called Big Data to its next level of development, as the uniform, structured data it contains adds more accuracy to Big Data's current mix of structured and unstructured data. The opportunity is to fast forward to an era beyond analytics into predictive analytics. For healthcare and medicine, the implications of more advanced predictive analytics could help realize the promise of precision medicine—knowing the likelihood of disease, injury[5], treatment success, and positive outcomes.

The simple Four-Party Ledger is only a foundational element of a potential future healthcare data exchange and transaction network. Microsoft's Bletchley Project[6] posits the existence of future consortiums that transact across several blockchain networks; that framework applied to healthcare links the entire supply chain of healthcare transactions.

The creation of a such a consortium would expand past the major players in the ecosystem, potentially including drug manufacturers and pharmacy/prescription tracking, medical equipment suppliers for consumers and providers, clinic appointment

setting and optimization, and more. These chains could be governed by a series of Smart Health Contracts. The Four-Party Ledger is also the foundation for exploring use of Melanie Swan's Health Coin concept for healthcare transactions, where services are "paid" for using a new pseudo-currency that can add needed price transparency, even normalizing pricing across healthcare[7].

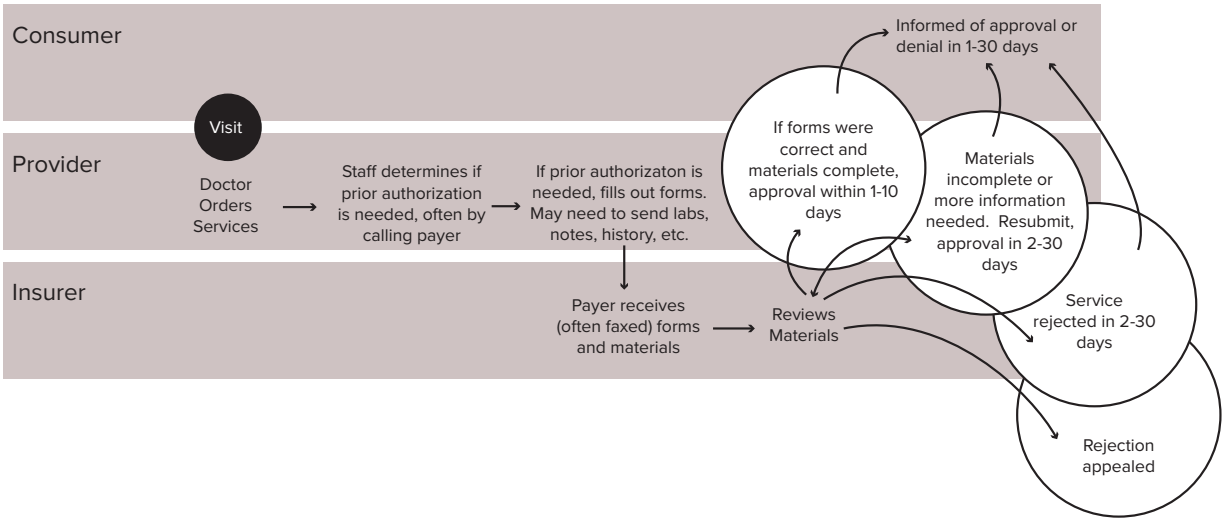
Smart Contracts Accelerating Reimbursement Transformation

Today's healthcare parties typically operate in an environment of low trust and high verification. Fraud is a serious concern, with estimates ranging from a $98 to $272 billion problem across the healthcare system[8]. Reimbursement rules are often vague and not well understood by all parties, and there is a sense of financial transactions interfering in patient interactions. A prime illustration of this in practice is the process of prior authorization, where providers must request and receive authorization from insurers prior to performing services where they seek reimbursement. While intended as a check and balance for patient safety and cost management, the inefficient nature of prior authorization leaves patients and providers confused and frustrated, often delays needed care, and burdens the whole population for the actions of a few bad actors.

Prior authorization also contributes to growing medical inflation, with estimates of 20 hours per week and $83,000 per year spent by practices on prior authorization related activities[9]. The use of prior authorization appears to be growing, particularly as new specialty drugs are offered. From 2007 to 2013, prior authorization for covered drugs under Medicare Part D increased from 8% to 21%[10].

Prior authorization is cumbersome (illustrated in Figure 2 below), often requiring phone calls and faxes to obtain approvals, and the requirements, forms and some processes typically varies by insurer. An AMA survey found that 20% of first-time prior authorization requests were rejected by insurers and 80% of those rejections required physician practices to initiate appeals[11].

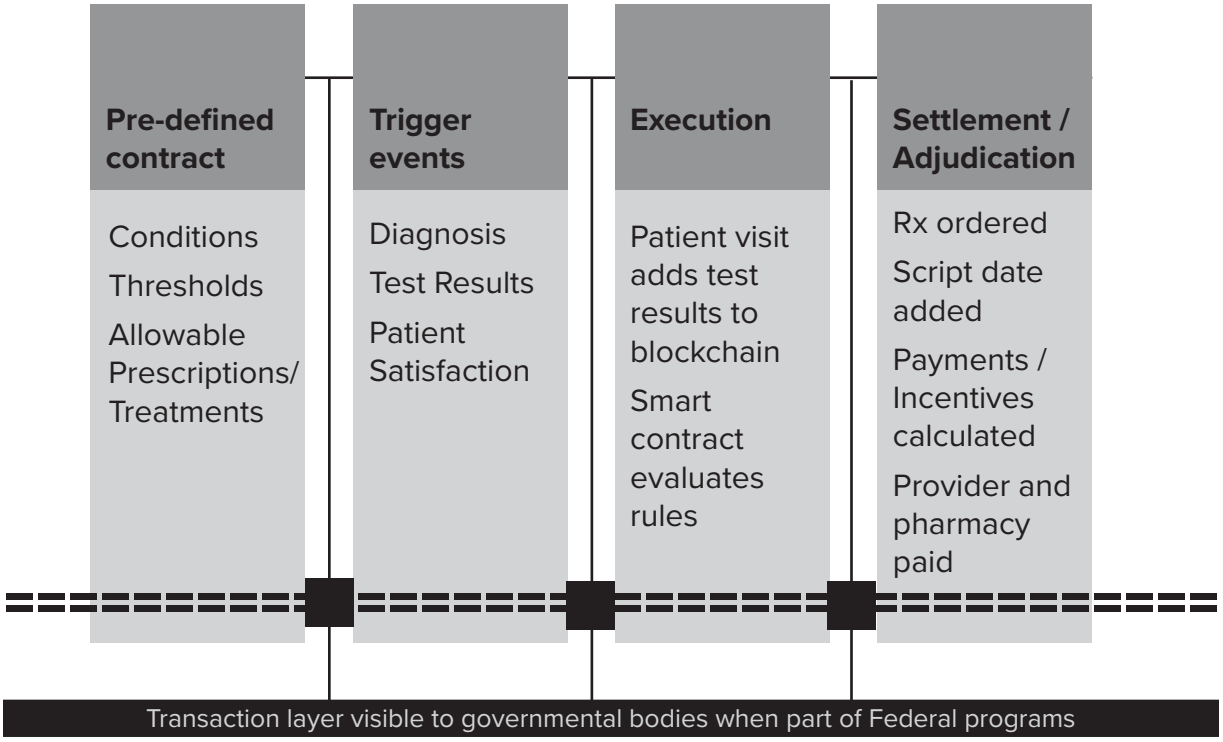
Figure 2: The Cumbersome and Opaque Current Prior Authorization Process



Adapted from American Medical Association, "Standardization of prior authorization process for medical services white paper," June 2011.

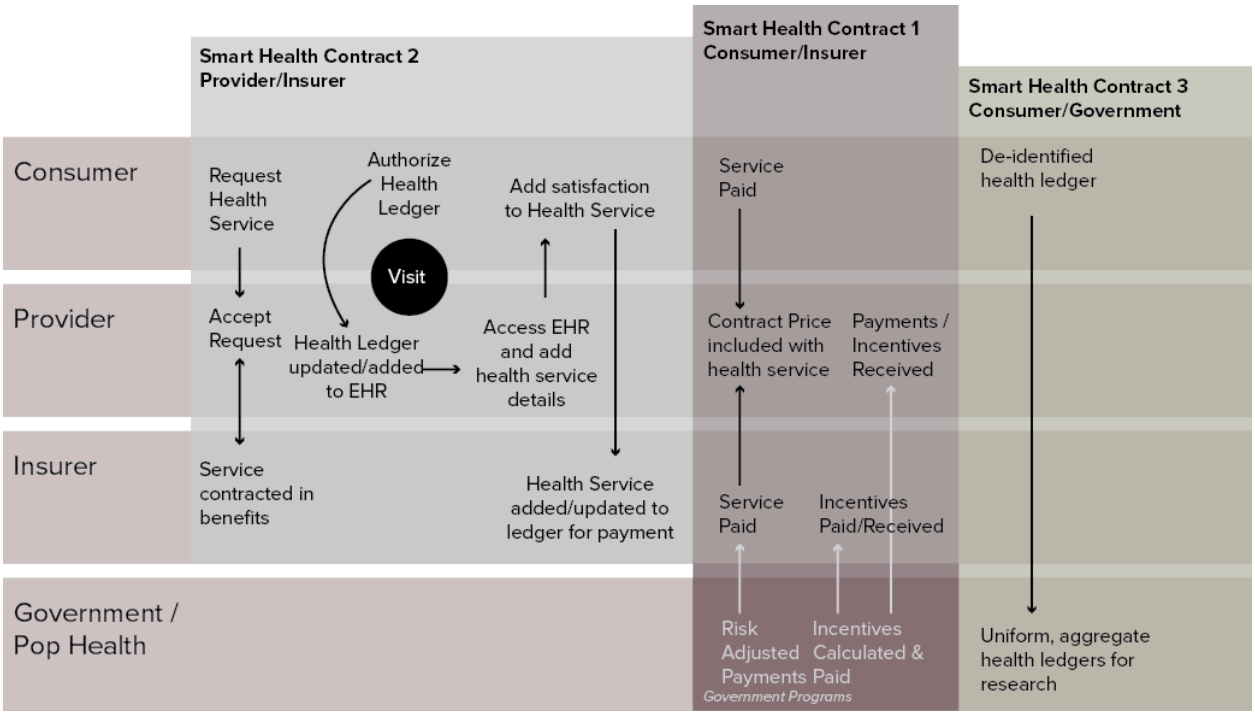
However, blockchain can materially impact prior authorization through the use of Smart Contracts. Smart contracts are emerging as one of the most promising applications in the early development of blockchain. Smart Contracts allow for rules, agreed upon by all parties in the exchange, to be codified and automated, and are specifically beneficial in low-trust environments. They transform typical legal contracts that must be interpreted and debated by humans into executable code interpreted and executed by machines. Instead of the highly manual and delayed current prior authorization process illustrated in Figure 2, Smart Contracts allow for automation and transparency as part of the natural transaction flow. The new transaction flow under Smart Contracts is illustrated in Figure 3.

Figure 3: Function and Process for Smart Benefits Contracts



While prior authorization represents a growing system pain point and reasonably isolated use case to begin using Smart Contracts, the entire benefits structure could benefit. Smart contracts could redefine and automate not just prior authorization, but also automate reimbursements, reduce the need for extensive audits, and accelerate the calculation and payment of incentives for delivering positive patient outcomes. Transactions are visible to all primary parties, but could also be accessible by trusted parties, like government entities for both research and verification of payments through programs like Medicare.

Figure 4: Service to Payment Governed by Smart Contracts



There are countless other use cases primed for transformation leveraging the capabilities of blockchain. For example, some insurers send armies of nurses into provider offices to do chart reviews to validate patient health conditions for risk-based contracts, Medicare audits each health plan to calculate STARS two years after the actual activity, insurers hire agencies to conduct home health assessments often for services already handled by a consumer's primary care physician due to lack of data visibility, and consumers receive separate explanations of benefits from their insurer and invoices from their provider and must reconcile them.

The new processes executed by a series of Smart "Health" Contracts allow for single transactions to replace many, greater ecosystem transparency, and the removal of subjective, intermediate actions. Figure 4 outlines how the Health Services Ledger and Smart Health Contracts combined can radically simplify the existing healthcare experience.

Enabling Data Portability, Interoperability and Security

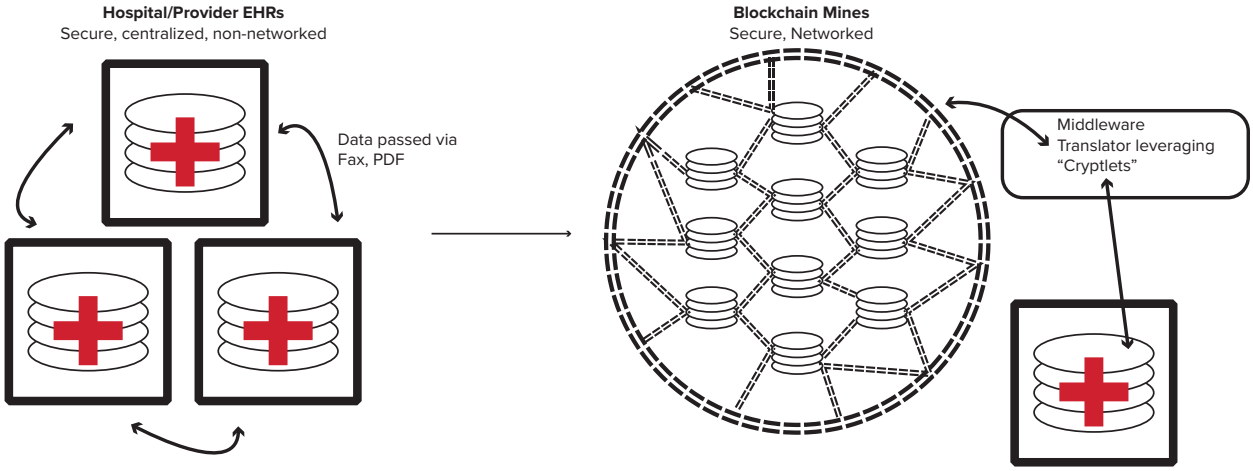
Blockchain provides the necessary infrastructure for a Four-Party health services ledger providing built-in data portability across providers, insurers, consumers, and the government. Block contents provide the flexibility to support secure health and payment data that can evolve and extend.

Illustrated in Figure 5, portability is inherent in the distributed nature of blockchain with the potential for significant efficiency and patient safety improvements by eliminating unnecessary outreach and tests, recording prescription history, and linking health transactions across provider interactions. The health services ledger benefits

from the strong cryptography inherent in the blockchain design as well as the reliability provided by the distributed network that provides fault tolerance by default as each node retains a copy of the distributed ledger. Cryptlets, introduced by Microsoft through Bletchley, may have an essential role in the development of middleware that can securely interact with the existing EHR infrastructure[12], potentially allowing the legacy centralized and future decentralized systems to operate together.

The health services ledger can also begin to limit or eliminate a range of services that seek to enable interoperability through less efficient means. Healthcare complexity and privacy regulations have led to the proliferation of "middleman" companies. Careful design of blockchain transactions and access keys could result in more direct transactions between parties, ultimately creating a less costly and more timely healthcare system. For example, in today's world, a physician and insurer have a connected relationship. Each has a relationship with a patient, and they have a contracted relationship with each other. Despite this, they must use a third party to determine the nature of each's relationship with the patient. This may be fundamentally unnecessary with smarter connections using blockchain.

Figure 5: Migration of Centralized Storage and Access to De-Centralized System



Adapted from Robi Dattatreya, Total Solutions, "Blockchain for dummies – a quick guide into the ledger technology," The Paypers. October 30 2015.

Security and Privacy Implications

Healthcare organizations are increasingly becoming the targets of cybercriminals. In 2015 alone, there were an estimated 253 breaches totaling 112 million records, led by Anthem's 78.8 million patient and employee records[13]. Some estimates put the cost of recent breaches at over $37 billion, a figure that is disputed, but even more conservative estimates assume approximately $30 billion has been spent cleaning up healthcare breaches since 2009, a number on par with the incentives paid to doctors and hospitals for investments in EHR that demonstrate meaningful use[14].

With greater interoperability demands, the importance of a platform that is secure

by design becomes even more critical. Blockchain offers layers of security such as cryptography and digital signatures, enabling capabilities like requiring a doctor and patient to approve before releasing sensitive records[15]. Distributed consensus enables "security by sharing", which spreads processing across nodes and reduces risk compared to single monolithic claims and EHR systems. Commercial entities are currently developing tools to further improve both the security of blockchain and new configurations that enable consortium and private blockchains. By leveraging some one-way hashed transactions within trusted networks, often with de-identified data, and private/public key-enabled one-to-one transactions, data can be seamlessly accessed when needed. Utilizing blockchain itself for personal data management and ownership, combined with off-chain storage is another potential solution for privacy and security concerns, where a separate service can manage and encrypt identity completely separate of a health-related chain[16]. This further increases the privacy and security of data.

Healthcare is a sensitive and personal topic, so building trust in blockchain technology will be essential in ensuring adoption from all parties. Additionally, individuals will need to manage their identities through a designated identifier, which is logically a government-issued ID. If government entities enable blockchain for their programs, trust will grow faster than through commercial means alone.

Applications in Medicare: An Impactful First Use Case

Medicare represents a system with the potential for material improvements through adopting elements of blockchain technology. Today, each party in the Medicare system operates off its own health ledger. The result is a system of expensive verification, unnecessary medical care, and overwhelming outreach to consumers. With the changes in reimbursement outlined in MACRA, CMS in particular has an opportunity to accelerate blockchain development and minimize the burden of reporting placed on providers while accelerating the analysis of additional outcome data.

In today's world, insurers need to document the conditions of their populations each year to ensure correct Medicare reimbursement. They attempt to catalog these health conditions based on claims history (acts as a closed-system health ledger for the insurer, as an EHR is to the provider). Since consumers can change insurance plans under Medicare, the insurer does not have access to claims history beyond the time that the consumer was part of their health plan. Also, since claims are an incomplete health record the insurer often lacks critical insight into health metrics, such as HbA1c. This lack of a complete historical health ledger causes the insurer to attempt to fill in the blanks through direct outreach to consumers or by contacting providers, a process further complicated by claims and reporting lag. Seniors find themselves being asked more frequently than needed to make appointments for screenings, like colonoscopies, which are typically only required every ten years in healthy individuals, due to a lack of visibility into historical records.

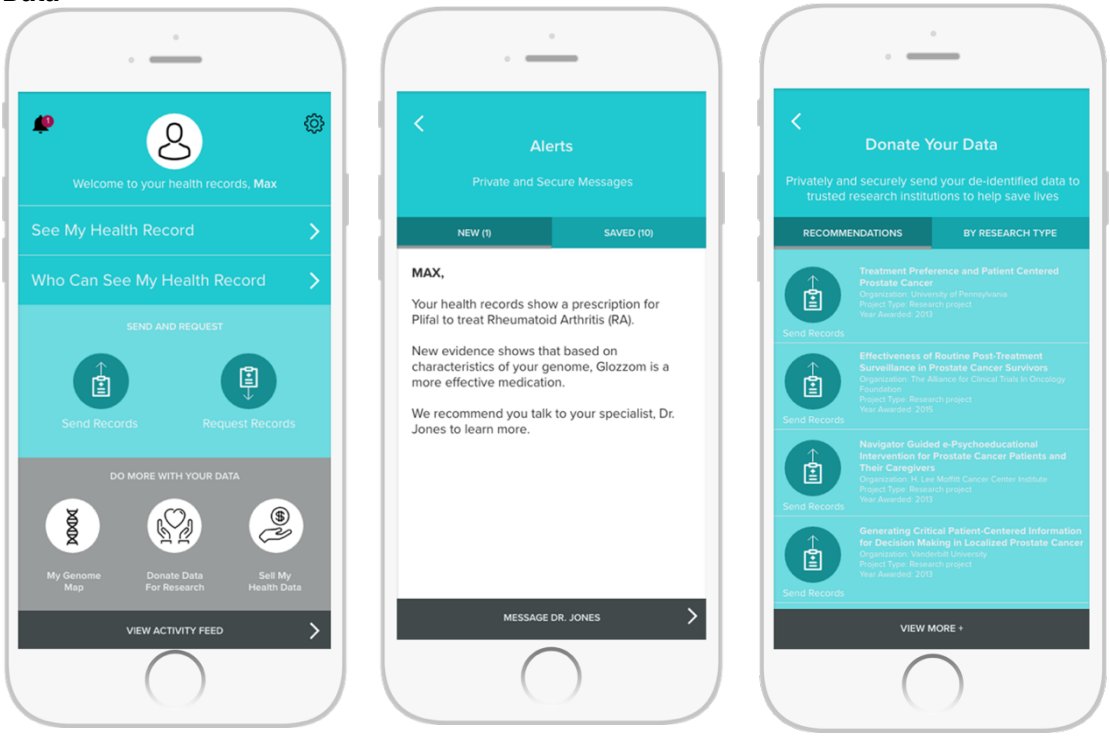
Providers maintain their own health ledgers in EHRs, and when a patient visits a new provider they face the same challenge as insurers face when consumers change health plans. Unless the patient happens to see a provider in the same system, or in

the unlikely event there is data exchange in place amongst practices, the patient record lacks essential information that can lead to non-value added processes. In most cases, the provider can either manually request prior records from the patient's other providers (often by faxing forms), or try to gather that information from the patient through dialogue. This error-prone and inefficient model often leads to unnecessary testing, limited prescription history, and an incomplete picture of a patient. For both insurers and providers, the lack of data portability has high costs, wastes time, and creates risk to patients.

Today's Medicare member is inundated with outreach calls for services they often don't need, providers' offices are overwhelmed with records requests, insurers are guessing at progress towards incentive measures thus throwing more and more resources at the consumer and provider, exasperating this viscous cycle. Meanwhile, providers are struggling to collect consumer out-of-pocket payments, and delays and challenges with reimbursement are further straining their financial viability and distracting from what they want to be doing – helping patients.

By leveraging a four-party ledger and Smart Contracts, these multiple parties can share data, automate and streamline payments, and spend more time with patients than with administrative tasks. Additionally, seniors would avoid the overwhelming volume of calls they face today for various interventions (e.g., home health visits, tests, extra check-ups) and their providers will have the information they need to ensure they don't prescribe conflicting medicine or miss an important health condition or preventative service.

Figure 7: Mobile App for Consumer Access of Health Ledger to Enable Patient Sharing of Health Data[17]



In Figure 7, a new experience for Medicare consumers and caregivers shows how consumers can control the disbursement and access of their health information seamlessly and continuously, and research entities can benefit from easy access to structured health data. This model supports the Health Research Commons envisioned by Swan[18]. Additionally, consumers can benefit from analytic services that add significant value to health data, such as genomic-based alerts that can be conversation starters for treatment plans. In this model, consumer can even sell their own data to private entities (such as pharmaceutical companies). Underlying that notion is the beginning of the data economy envisioned by Doc Searls—starting with the premise that consumers own their own data and release it by permission, including for financial gain as opposed to non-permission-based marketing[19].

Highlighting the Medicare market is not coincidental—as Medicare reimbursement transformation is often adopted by the commercial markets and other government agencies, the adoption of blockchain technology by Medicare could pave the way for transformation of the broader commercial and government health segments. Additionally, the Alternative Payment Models (APMs) outlined in MACRA could be governed by individual Smart Contracts that include the program-specific reporting needed. This will allow for condition- and specialty-specific APM outcome reporting processes without undue burden—and allow for the physician and provider organization to focus on clinical duties.

Conclusions

As an emerging technology, Blockchain development does not yet easily lend itself to wide scale use. However, designing the future infrastructure and transaction engine for healthcare must begin, especially considering the cost savings implications for government-funded programs. It may be prudent to first experiment with private blockchains[20] while evaluating market readiness for public blockchain implementations. A private blockchain addressing prior authorization for the Medicare market, for example, is a use case that could be prototyped and rolled out to a narrow market for testing.

While blockchain demands rapid development in security, that development is underway by trusted contractors in the government market. This technology could correct some of the problems with past interoperability spending and programs by connecting legacy, closed systems, with a new, networked technology.

Most importantly, government must explore and invest in this area to pave the way for commercial adoption in healthcare. Medicare has already demonstrated that innovation in reimbursement models can translate from the government sector into commercial markets. Blockchain represents an even greater opportunity for transformative leaps in improving healthcare efficiency, interoperability, and security, and is worthy of innovation investment to design and test new operating models to benefit citizens.

Notes and Sources

[1] IBM Institute for Business Value. (2016). Fast Forward: Rethinking enterprises, ecosystem and economies with blockchains, *IBM*: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03757USEN
[2] Palmer, D. (March 3, 2016). Blockchain Startup to Secure 1 Million Health Records in Estonia. *Coin Desk*: http://www.coindesk.com/blockchain-startup-aims-to-secure-1-million-estonian-health-records/
[3] Prisco, G. (April 26, 2016). The Blockchain for Healthcare : Gem Launches Gem Health Network with Philips Blockchain Lab. *Bitcoin Magazine*: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938
[4] PCORI's mission is to improve the evidence that drives health decisions. Their patient groups are part of PCORnet at http://www.pcornet.org/patient-powered-research-networks/
[5] Risk assessment modeling using the STRATIFY tool has already been proven to accurately predict falls for the elderly, a significant predictor of future health problems and cost. Oliver, D., Briton, M., Seed, P., Martin, F.C., & Hopper, A.H. (1997). Development and evaluation of evidence based risk assessment tool (STRATIFY) to predict which elderly inpatients will fall: case-control and cohort studies. *BMJ*, 315, p. 1049.
[6]Gray, M. (June 7, 2016). Introducing Project "Bletchley" at https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md
[7] Swan, M. (2015). *Blockchain*. O'Reilly Media (Sebastopol, CA), 250.
[8] The Economist (May 31, 2014). The $272 billion swindle: Why Thieves Love America's Health-care System. *The Economist* at http://www.economist.com/news/united-states/21603078-why-thieves-love-americas-health-care-system-272-billion-swindle
[9] Bendix, J. (July 8, 2014). The Prior Authorization Predicament. *Medical Economics.*
[10] NORC/Social & Scientific Systems analysis of data from CMS
[11] American Medical Association (June 2011). Standardization of prior authorization process for medical services white paper.
[12] Gray, M. (2016)
[13] Munro, D. (2015). Data Breaches in Healthcare Totaled Over 112 Million Records in 2015. *Forbes* at http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#247cbdd07fd5
[14] Wall, J.K. (August 7, 2015). Costs of Data Breaches, Just This Year, Outstrip Subsidies to Digital Health Care. *Indianapolis Business Journal* at http://www.ibj.com/blogs/12-the-dose/post/54343-costs-of-data-breaches-just-this-year-outstrip-subsidies-to-digitize-health-care
[15] Donnelly, J. (Jan 12, 2016). Healthcare: Can the Blockchain Optimize and Secure It? *Bitcoin Magazine* at https://bitcoinmagazine.com/articles/healthcare-can-the-blockchain-optimize-and-secure-it-1452624836
[16] Zyskind, G., Nathan, O., Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data at http://web.media.mit.edu/~guyzys/data/ZNP15.pdf
[17] Icons used designed by Freepik and distributed by Flaticon. Drugs mentioned are fictional; any similarity to real prescription drugs is coincidental. PCORI logo and real research studies used for illustration purposes only.
[18] Swan, 2015.
[19] Searls, D. (2012). *The Intention Economy: When Customers Take Charge*. Harvard Business School Publishing (Boston, MA).
[20] Buterin, V. (August 7, 2015). On Public and Private Blockchains. Ethereum blog at https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/