ARK INVEST | RESEARCH

Gem

HOW BLOCKCHAIN TECHNOLOGY CAN ENHANCE EHR OPERABILITY

SEPTEMBER 29, 2016

RESEARCH WHITE PAPER BY

CHRIS BURNISKE, BLOCKCHAIN PRODUCTS LEAD | ARK INVEST

EMILY VAUGHN, DIRECTOR OF CLIENT SERVICES AND MARKETING | GEM

JEFF SHELTON, DIRECTOR OF PRODUCT | GEM

DR. ALEX CAHANA, MD, MAS, FIPP, THEME DEVELOPER | ARK INVEST

SPECIAL THANKS to our contributors:

Catherine Wood / Brett Winton / Kellen Carter / Sebastian Benkert / Lisa Dodd / Joseph Bradley

ARK Invest
155 West 19th, 5th Floor
New York, NY 10011
info@arkinvest.com
www.ark-invest.com

Gem
120 Mildred Ave.
Venice, CA 90291
hello@gem.co
www.gem.co

JOIN THE CONVERSATION

@ARKblockchain

@ARKinvest

@gemhq

Introduction

In healthcare, information is not only private, it is proprietary. While doctors and patients yearn for a digital and unified patient record, the infrastructure required to accomplish this doesn't exist yet.

A blockchain could be a public catalog of health records that references databases, fitness and medical devices, mobile phones, and laptops. It could be used to connect every patient, healthcare provider, and payer to a secure, yet public network.

A blockchain also could enable the interoperability of private health networks. Users would be able to trust the blockchain infrastructure in a healthcare context because it would automate the integrity of the data exchange. Not only would users know if their data had been manipulated, they would see exactly how it was done.

I. Healthcare Innovation

A Brief History of Falling Short

Over the past century, we've introduced innovations in an attempt to reform American healthcare, but for the most part have been disappointed by the results. These innovations have included employer sponsored coverage, the Social Security Act, Health Maintenance Organizations (HMO) Act, and the Affordable Care Act (ACA) [1]. Despite persistent efforts to the contrary, national healthcare expenditure (NHE) continues to rise per capita and as a percent of GDP. The situation may not improve, with analysts projecting NHE to grow 5.8% annually through 2025, at which point it will be roughly 20% of GDP [2]. With the rise of blockchain technology a new promise is on the horizon for healthcare, but will the results succeed where past innovations have failed?

Blockchain Technology's Potential Value to Healthcare

Introduced to the world through Bitcoin, blockchain technology provides a distributed database for managing unique digital assets among multiple parties [3]. Transacting bitcoin is merely an exchange of data using a blockchain, which opens the possibility of securely managing and transferring many types of data over unsecured channels.

Importantly, the technology does not require participating parties to trust one another with their data, because **trust automation** is built into the way information is appended to a blockchain. A blockchain ensures that information is immutable once appended and that all parties have a complete log of network activity. Because each stakeholder has the same view of the complete ledger, blockchains could become the basis of trust that underpins information exchange between related and unrelated parties.

Since the code underlying Bitcoin is open source, it has been downloaded and modified innumerable times to construct purpose-built blockchains that can secure and transmit different kinds of data. Recently, blockchain engineers and companies have been exploring how this technology can be applied to non-financial use cases, including universal digital identities [4], supply chain management [5], and healthcare orchestration [6]. In other words, blockchain technology has evolved beyond finance, and should be considered a general purpose technology [7].

Blockchain technology is in its infancy and has many nuances. That said, its potential within healthcare is becoming clear, perhaps most importantly as a way to facilitate electronic health record (EHR) operability. We believe that by using blockchain technology, the following three major features of EHR systems can be enhanced:

- Immutability via File Integrity
- Cybersecurity via Data Access Management
- Interoperability via Collaborative Version Control

In a time of increased electronic data, blockchain technology can organize access to that data in such a way that it can be recorded and verified only through **consensus** of all parties involved. For clinicians, blockchains can support universal identifiers for any data entered into an EHR, which is then available to other authorized providers and care team members. Patients can monitor their own health information, approving, denying or sharing changes to their data, ensuring a higher level of privacy and engagement. Researchers will benefit from better data integrity and reliability, creating a 'platform of trust' for data sharing. Payers will have better data reconciliation, fewer errors and frauds, reduced administrative and claim processing costs, and the potential to reach underserved markets [8].

To describe what's possible with blockchain technology, we can imagine a situation where a patient, Alice, faints and knocks her head while hiking in Oregon. While her primary care doctor, Dr. Nguyen, is unavailable, she can give her emergency room doctor, Dr. Francis, access to her EHR by adding him as a permissioned user. The blockchain records this change in "permissioning" and enables Dr. Francis to view Alice's EHR temporarily, and append information to it without changing the original EHR. Alice can authorize the same permissioning to her wearable device, if that information is useful to Dr. Francis. At the end of a predetermined window, Dr. Francis' access to the EHR would close. Alice's primary care doctor, Dr. Nguyen, then would have a complete and verified record of all events the next time he speaks with her, as would her insurance payer.

We will dive deeper into the specifics of a blockchain implementation relevant to EHRs after further describing the current landscape of healthcare information technology (IT). To avoid classic hype cycle thinking, it is important to first understand the existing landscape before unrealistic solutions are proposed.

Data Mobility and Security: The Realized and Unrealized Promise of EHRs

The EHR is a digital version of a patient's paper chart. It should facilitate sharing of protected health information (PHI) with authorized parties. EHR platforms also should allow healthcare providers to better engage with patients, make more efficient and accurate decisions about care, and streamline provider workflow in real-time [9]. Providers should be able to longitudinally and accurately store data through a shared network of information exchange. Such a system should extract medical data and facilitate both personal and population-based research.

The implications of effective EHR use should be positive for enabling macro and micro interconnected health services. The Health Information Technology for Economic and Clinical Health *(HITECH) Act* of 2009 provided a series of incentives to encourage widespread EHR adoption. By mandating standards for storing and sharing health records, the HITECH Act aimed to improve healthcare quality, safety, and efficiency.

Due to the HITECH act, the deployment of EHRs with "meaningful use" certified technology has been impressive [10]. To date, 175 certified health IT vendors have supplied certified EHRs to 95% of the 4,474 non-federal acute care hospitals in the US, and the percent of office-based physician practices demonstrating meaningful use continues to grow [11]. Furthermore, 104 hospitals applying meaningful use enjoyed a roughly 10% drop in per patient costs (i.e., $730) compared to other hospitals, thanks to more legible records, reduced prescription errors, improved access, and adherence to best practices [12].

While the HITECH Act has been effective in helping to digitize medical records, it did not anticipate the evolution of the EHR market. Initially, the HITECH Act emphasized the widespread adoption of EHRs, but not the infrastructure supporting them. Today a large number of proprietary EHR systems follow required privacy and security standards, but do so behind walled-data-gardens that inhibit the sharing of medical data. These walled-gardens have become silos of inefficiently duplicated personal health information, making patients' and providers' lives more difficult, and sacrificing a great potential benefit of digitization.

Beyond walled-gardens, EHR woes have been worsened by usability deficiencies, privacy concerns, data breaches, ransomware and prohibitive overall costs. Furthermore, the presence of maturing mobile platforms and internet-connected-devices have exacerbated EHR deficiencies. Most physicians complain that EHRs interfere with their workflow and communication with patients, contributing to job dissatisfaction and eventual burnout [13].

The Care Model Evolves Under the Affordable Care Act (ACA)

The realization that healthcare is not a privilege but a right was the main impetus behind comprehensive healthcare reform through the *Affordable Care Act* (ACA) of 2010 [14]. The ACA seeks to expand and improve medical coverage for the uninsured by reducing the burden of uncompensated care. It also aims to design a more competitive payer marketplace and reward healthcare professionals for coordinating care efficiently as a patient visits various providers.

Prior to the ACA, the HMO healthcare system, dominated by a 'fee-for-service' model, often led to increased spending on inefficiently administered care [15], and the prohibitive cost of healthcare caused an increase in the number of uninsured individuals. The ACA requires healthcare professionals and organizations to shift from the legacy 'fee-for-service' model to a 'pay-for-performance' reimbursement system. It offers alternative payment models to encourage accountable care organizations (ACOs) to coordinate care based on better outcomes with reduced waste, abuse, and fraud.

Proving quality of care requires reliable data about the doctor-patient interaction and course of treatment. To be effective, entities need to trust third party data, proving the quality of the health service provided. Doing so will present significant issues for current system architectures around data reliability, security, and transparency.

The Growth of Digitization and Value-Based Care Demands New Rails

A fully interoperable health ecosystem has yet to be realized largely due to antiquated, unsecured and opaque **information rails** for sharing data. Old information rails make it nearly impossible for the software programs that rely on them to keep pace with technological change, just as a bullet train couldn't run on rusty 19th century train rails. While some hospitals have seen a 10% drop in costs when utilizing meaningful use EHRs, not all EHR users are seeing cost savings or returns on investment (ROI). Today, EHR optimization is one of the most pressing technology-related problems facing physician practices [16]. Some hospitals are reporting they're 'trapped' by 'lackluster' EHR systems [17].

Much of this discontent reflects the difficulty of finding information in real time during the clinician's workflow. When patients enter the doctor's office without their previous medical records, caregiver information, latest laboratory results, or list of medications, healthcare providers find themselves spending a great deal of time trying to reconcile information already available elsewhere. Often, they rely on the patient's recollections of their health histories, either through input forms, hard copies of previous medical records, or verbal communication. With the fast pace of care delivery today and reimbursement models that demand coordinated and collaborative care, low-level data interoperability is not enough.

Value-based payments and delivery system reforms, both of which require fluid data transmission, are driving interoperability efforts [18]. The goal of **interoperable** EHRs is to enable disparate healthcare systems to exchange and use clinical information, under a standard set of guidelines, designed to coordinate patient care and reimbursements. A number of national cross-provider, cross-vendor interoperable data exchanges are evolving now: *Direct Connect, Carequality, Commonwell,* and *eHealth Exchange*, to name a few. Companies joining this effort are committed to facilitating the sharing of information [19], and failures to address interoperability can result in EHR and other health IT products being de-certified.

Blockchain technology may provide the solution to connect information on disparate networks to a common infrastructure, in order to create an integrated solution for existing health IT interoperability. It allows providers, patients and payers to share a **single version of the truth** about a patient's healthcare information. Multiple providers, in multiple sites, could access an uncorrupted, secure and universal patient record, avoiding redundant tests, procedures or prescriptions. Payers with the right permissions could have access to relevant information in order to process claims rapidly and with more precision. Patients would have transparency into the entire continuum of care. Importantly, blockchain technology would not be centralizing health information in healthcare exchanges, but instead, decentralizing the system in a securely and interoperable manner. We will detail how blockchain technology can achieve this **interoperability without centralization** now.

II. Healthcare Blockchains for Secure and Collaborative Data Management

Blockchains vs Blockchain Applications

A blockchain is simply a ledger of events replicated over a widely dispersed relay network. It does not do very much on its own. It does take instructions, which allows it to support and connect to applications. It's helpful to think of a blockchain like a computer's hard drive that anyone can use to access the same record of information. Like a computer's hard drive, it is rigid with minimal value add as a standalone data store. What makes it really useful are the operating system and applications that access the hard drive.

Gem builds and supports blockchain applications using GemOS, a blockchain "operating system." The blockchain's ledger is a shared registry of events and messages. GemOS provides layers of logic and privacy that leverage this shared information. Blockchain applications communicate with GemOS, which connects to the underlying ledger to facilitate information exchange among multiple parties. The entire system forms a network that connects all the users—in this case patients, healthcare providers and payers—to each other, to the underlying data, and to the useful applications, like EHRs.

A Tamper-Proof Audit Log

The blockchain is critical to the interconnection of disparate EHRs. A blockchain logs every single event that is entered into the EHR, including when a record is created, accessed, appended, or shared. A record could pertain to documentations, prescriptions, patient interactions, and payment requests, to name a few. All network interactions, including records and broadcasted messages, are time stamped as unique events in a blockchain, and assigned a **hash**.

The hash serves as a **unique record identifier** for that event, in alphanumeric form. It is not a randomly generated number, but instead is created by a cryptographic algorithm that crunches the contents of the

file into a fixed number of characters. If two files had the same exact information, then they would be **"hashed"** to the exact same string of characters. If the data inherent to the document changes, the algorithm will produce a different hash. Important to privacy, the contents of a file cannot be reverse engineered from the hash; others can see the hash without the underlying information being exposed (unless permission to view the information is granted).

Equally important to understand, the actual data file is **not** being stored on the blockchain. The blockchain simply records minimal information that validates content and points to *where* the rest of the record can be found. The *where* component is where the data actually is kept and can include an array of environments from Amazon's cloud to the on-premise servers of a family office. A hash is a **digital fingerprint** that can be used to track down the data.

This ledger of hashed records and user interactions creates a log that is replicated across every connection point—or **node**—in the network. In this sense, a blockchain is a distributed *relay* network with a widely replicated ledger. The complete blockchain and its user activity is maintained independently by all the participants. If one supporting node goes down, the network and data within the blockchain remains available to all other nodes.

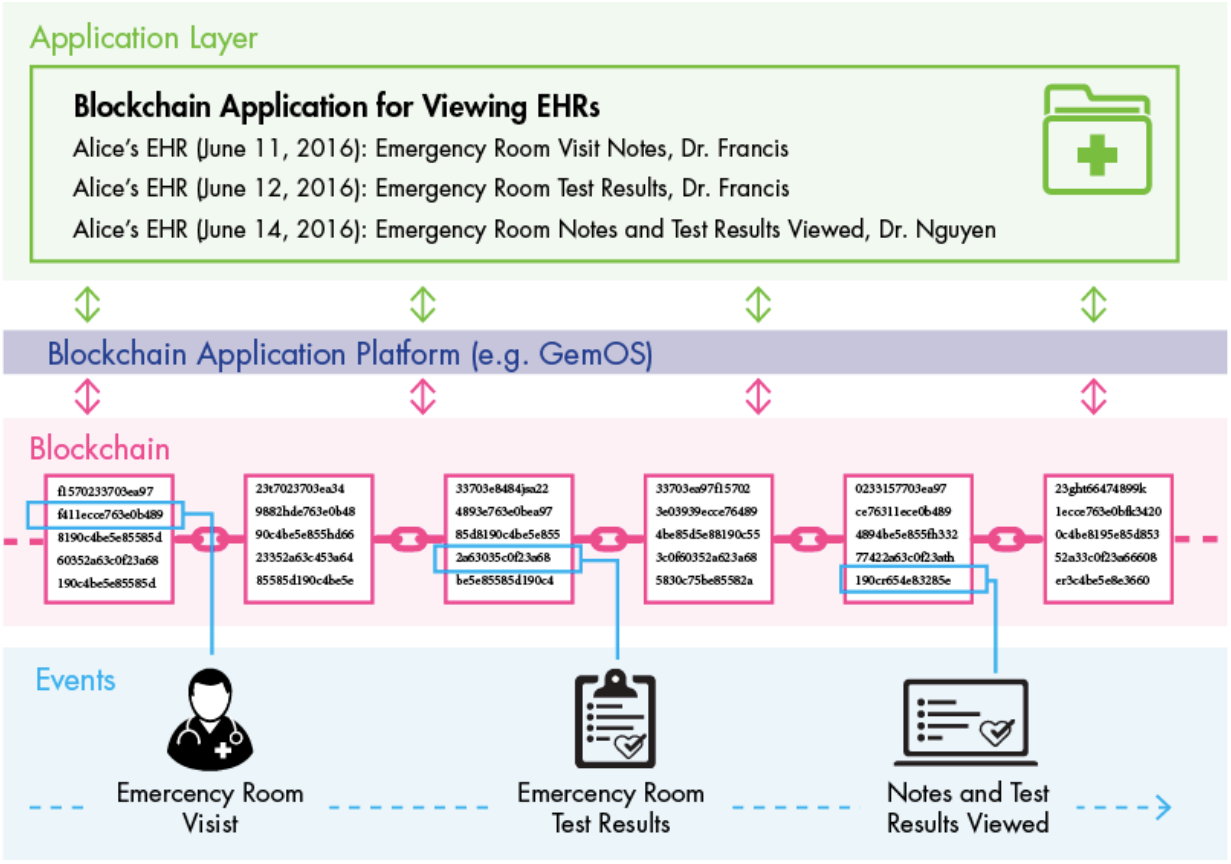
Events are bundled into blocks, and blocks are appended to the blockchain at a predictable rate. When a **block** is created, it receives its own hash which is comprised of a number of inputs, including the record of recent events and **the hash of the previous block**. Connection to the previous block is extremely important, because it links each new block to the blocks before it, and all the events therein. The linking of blocks explains where the word **"blockchain"** comes from.

Cryptographically linking events this way creates an immutable historical record. If a bad actor tried to change a previously recorded event, the event's hash would change, altering the hash of its block and causing a domino effect in which the connection between all subsequent blocks would break. Every node has a living copy of the blockchain and would identify this as an attempt to break the network, leading to rejection of the change.

This highly-redundant, tamper-proof ledger becomes the irrefutable audit log for the entire network of connected users and applications. The permanent and immutable nature of blockchain information matters because blockchains are shared utilities that connect non-trusting parties. These parties need the guarantee that their **data cannot be modified by bad actors.**

Immutability: File Integrity

Because the hash of an event is unique to the record's contents, it can guarantee the **integrity of the record**. When the hash is recorded, it enables future users to verify that the contents of the record have not been modified. If the document has been modified, it produces a different hash, which will not match the preceding hash. Revisions are added to the original record, creating an append-only revision history. Such revision history for a file is not something blockchains inherently do—they simply record a new hash for a new event—so the revision history is instead compiled by an application that pulls information from the blockchain, as shown below.



When combined with blockchain applications, including identity management tools, the ledger becomes the ultimate indicator of "who did what, when" on a blockchain. The unchangeable nature of recorded information makes it a basis of trust that every party can agree upon.

Cybersecurity: Data Access Management

When a record is registered on the blockchain, the hash can include more than the contents of the event. It can include additional information like user permission lists, which act as instructions for the blockchain applications. Patients, doctors, nurses, or any authorized user or device can control access to data by storing these user permissions on the blockchain. When applications search for a record using the hash, the blockchain retrieves the hash and the user permissions. The application checks the blockchain-recorded permissions against the credentials of the end-user, and then will authorize or deny access to that information.

Blockchain secured data with clear "permissioning" enables complex privacy controls around universally-registered data. Importantly, it enables data access management based on public, transparent rule sets without revealing private information to unauthorized users. In other words, it ensures that the right person has access to the right information at the right time, and it records every interaction with that data, while simultaneously assuring that private information doesn't fall into the hands of unauthorized persons.

Interoperability: Collaborative Version Control

Blockchains can eliminate the burden and costs of data reconciliation. Instead of each party maintaining a locally stored version of the EHR that they must reconcile against the others', each record registered to the blockchain is linked to the original, and then grants access to this continuum of information based on role

and responsibility. Establishing one record that everyone can access, and appending information to that record, greatly reduces the amount of duplicate or inconsistent records stored across private servers.

Once a record's hash is recorded to the blockchain, the contents of that specific record cannot be changed. In other words, the blockchain is an "**append-only ledger**" where nothing can be erased. So, when someone wants to update information within a record she must append a new record to the original. Applications that read and implement user access instructions from the blockchain enable multi-party collaboration on the same medical record. Every interaction with the record is recorded on the blockchain, guaranteeing a record of who added what changes, when. The blockchain gives doctors a collaborative version control machine for managing patient records among disparate IT systems.

III. Blockchain Proof-of-Concept for EHRs

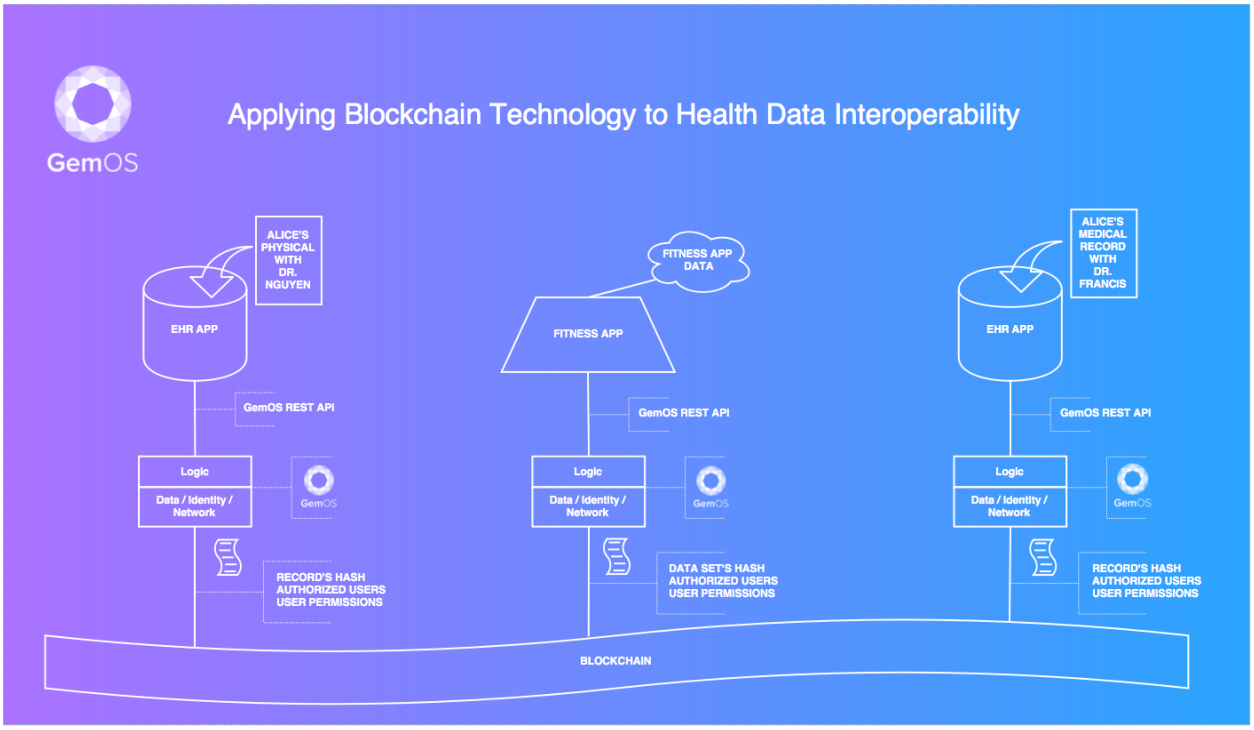
A proof-of-concept (PoC) helps to illustrate how blockchain technology can provide EHR systems with better immutability, cybersecurity, and interoperability characteristics.

Let's use the example of Alice, a 30-year-old female with an active lifestyle. During a hiking expedition in Oregon, Alice becomes faint, develops tunnel vision, and before she can find stable footing she falls and knocks her head. Unsure of her condition, her companions call for help, and she is taken to a local clinic. At the clinic, Alice begins to feel better, but Dr. Francis suspects she may have a minor concussion. In the absence of a medical record, Dr. Francis can provide only standard, non-personalized care.

Dr. Francis requests a few tests to find out what caused her to faint, but needs a full medical profile to treat her properly before he can discharge her. Alice authorizes Dr. Francis to request results from her latest physical, which was performed by her primary care provider, Dr. Nguyen. Dr. Francis also requests access to the data in her fitness wearable. The more data he can get, the fewer tests he may have to run and the quicker Alice can be on her way.

Gem can create blockchain infrastructure that will allow Alice the ability to grant Dr. Francis access to her files, which are in a variety of data stores.

The blockchain wasn't designed to store massive amounts of data; instead it is the baseline protocol that acts as a programmable communication layer connecting disparate data sources. GemOS acts as the connective tissue between the blockchain's communication layer and existing health and fitness software. GemOS can connect private data sources, reference identities across organizations or devices, construct rule sets, design templates and modules for end-user applications, and connect them all to the blockchain, as shown below.



A basic implementation of GemOS demonstrates how blockchains support health data interoperability. As shown above, GemOS has four components: *Logic, Data, Identity,* and *Network*. *Network* interacts directly with the blockchain, while *Logic* is abstracted from the blockchain and interacts with applications. Just as the internet has basic protocols that transmit bits, and then a stack of software to make those bits accessible to common applications, GemOS provides a stack of software that takes the information in blockchains and makes it accessible to healthcare applications that patients, providers, and payers utilize.

- Gem *Network, Data,* and *Identity* are the swiss army knives in the GemOS tool kit. They are agnostic tools that connect to data sources, registries and the underlying blockchain. *Data* connects GemOS with multiple third party data stores whether they are in Amazon S3 Buckets, Azure, or Bluemix. *Identity* covers the relevant users, roles, and groups at an organization to manage user access controls and registries of unique ID's. Identity could represent an organization, an individual, a device, etc. *Network* connects to multiple blockchains and manages the nodes supporting the blockchains.
- Gem *Logic* is what pulls these tools together. *Logic* pulls components from *Data, Identity,* and *Network* in order to model smart contracts, rule sets, and application data retrieval/delivery. *Logic* allows external applications to interact with one or many blockchains. It orchestrates document management and sends information via the blockchain to parties referenced within *Identity*. The element library that is managed within *Logic* enables blockchain applications to address unique business processes.

With this model in mind, we can demonstrate how blockchains can be used for file integrity checks, data access management, and collaboration. In Alice's example, her wearable data, her physical report, and her emergency room record will be recorded on the blockchain with unique hashes and user permissions. Healthcare providers will interact with applications that are tied to GemOS, and therefore the providers don't interact directly with the blockchain. Instead, GemOS orchestrates this information flow between the application and the blockchain. Information will be organized and recorded according to pre-determined instructions in the GemOS, integrating different applications, EHR systems, and in this case, a wearable

device. Existing IT systems and applications can leverage the blockchain's network by connecting to GemOS.

For example, the wearable data would have one permissioned user, Alice. She is the owner of the device and the data generated by the device. She can add Dr. Francis as a viewer by looking up his identity on the blockchain and provisioning read access through a friendly user interface. Alice is able to access her physical report from her patient portal app. Though she does not have the ability to edit the report, she can change the permissions to share it with another doctor. She adds Dr. Francis without having to contact Dr. Nguyen. All of these interactions are recorded on the blockchain.

If Alice were unconscious, a connected identity database could immediately route to a currently active and authorized provider in the vicinity that has been given the ability to unlock medical records in emergency situations. This provider could be sent proof of Alice's critical condition, potentially through a connected health device, and therefore have hard evidence of the need to grant emergency access. This extenuating grant of access would be recorded on the blockchain, giving a path to recourse if the emergency access was somehow abused.

When Dr. Francis uses his permissions to view her physical report, he can compare the hashes of the documents to make sure it has not been modified and, therefore, can assume that it must be accurate. He can use the physical report and the information from her wearable data to inform his diagnosis without running additional tests. When he creates his visit report, he registers it to the blockchain, appending it to prior physical reports and adds Alice's share permissions so she may easily share the report with Dr. Nguyen. Relevant providers and payers now have a record of Alice's emergency care that integrates data stored privately on disparate networks.

Conclusion: A Universal Library for Health Data

The promise of smartly constructed blockchain infrastructure for healthcare is simple: it can unite data across the continuum of care. While the guiding goal is simple, the implementation will be anything but, given the complexity of America's healthcare systems. To realize the full potential of what has been discussed above will require collaboration and standardization among entities that likely have divergent interests and needs. Furthermore, the question of who owns the health data—is it the patient, provider or payer—will likely become more pertinent, perhaps critical, in such a shared information system. Addressing such momentous problems will make many wonder what the associated costs will be, and whether blockchain will be another instance of healthcare innovation falling short.

We believe the best path forward will be to deploy blockchain technology incrementally, starting with small implementations. By harnessing standardized application programming interfaces (APIs) and modularized architecture, an interconnected tissue of compatible blockchains could be built out slowly to span healthcare systems. The only path forward is step by step, with rigorous testing and analysis to ensure sufficient returns from technological investments.

Certainly, such a colossal project is daunting, but prior to the advent of blockchain technology many in the healthcare industry could not fathom how an interoperable architecture of trust could evolve. Blockchain technology provides hope that such a system is possible. It differentiates from past solutions in its ability to facilitate health information exchange through a decentralized architecture. This decentralized architecture is tamper-proof and resilient when compared to centralized solutions, allowing for an immutable, secure and shared library of health data.

About the Authors

Chris Burniske | ARK Invest, Blockchain Products Lead
Chris serves as Blockchain Products Lead at ARK Invest, working on both research and business development. In 2015, ARK Invest became the first public fund manager to invest in bitcoin, offering the first two ETFs with bitcoin exposure. Chris frequently appears in media outlets including Forbes, CNBC, Bloomberg, Reuters, CoinDesk and more. He graduated Phi Beta Kappa with a BS from Stanford.

Emily Vaughn | Gem, Director Of Client Services snd Marketing
Emily leads Gem Health, the healthcare blockchain initiative, and oversees Gem's client education, partnerships, public relations, and marketing. Gem Health is a blockchain network for the global community of companies and individuals that take part in the continuum of care. Blockchain technology addresses the trade-off between personalized care and operational costs by connecting the ecosystem to universal infrastructure. Shared infrastructure allows us to create global standards without compromising privacy and security.

Jeff Shelton | Gem, Director of Product
Jeff serves as the Director of Product for Gem's blockchain application platform. In this capacity, he oversees core feature development to architect systems that enable and enhance business processes across a network of organizations. Gem's blockchain application platform transforms the way companies and industries connect to solve impossible problems by establishing levels of trust and transparency that will inspire new business models and services.

Dr. Alex Cahana, MD, MAS, FIPP | Ark Invest, Theme Developer
As a Theme Developer for ARK's Genomic Revolution theme, Alex focuses on the impact of technological innovations within the healthcare industry. Alex is the Director of Medical Affairs at the Center for Lawful Access and Abuse Deterrence (CLAAD), and the Subject Matter Expert for the Defense Veterans Center for Integrative Pain Management (DVCIPM). He is an affiliate Professor in Science Technology and Health Studies and adjunct Professor in Bioethics and Humanities at the University of Washington (UW). Alex promotes measurement-based care as standard of care in Pain Medicine and is a subject matter expert to the Department of Defense, the Veterans Administration, and is involved in State and Federal legislation to improve pain care.

Disclosure: ARK Theme Developers are not employees of ARK and do not receive compensation from ARK Invest.

Works Cited

1. Hoffman, Catherine. "National Health Insurance-A Brief History of Reform Efforts in the U.S. - Issue Brief." *The Kaiser Family Foundation* (n.d.): n. pag. Mar. 2009. Web. 3 Aug. 2016.
2. Keehan, Sean P. "National Health Expenditure Projections, 2015–25: Economy, Prices, And Aging Expected To Shape Spending And Enrollment." *Health Affairs*. Jane Hiebert-White, July 2016. Web. 3 Aug. 2016. <http://content.healthaffairs.org/content/early/2016/07/15/hlthaff.2016.0459>.
3. Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." (n.d.): n. pag. Web. 03 Aug. 2016. < https://bitcoin.org/bitcoin.pdf>.
4. "Identity for a Mobile World." *ShoCard*. Web. 03 Aug. 2016. < https://shocard.com/>.
5. "Blockchain Technology for Collaborative Commerce." *Skuchain*. Web. 03 Aug. 2016. < https://www.skuchain.com/>/.
6. "Gem I Health." *Gem*. Web. 03 Aug. 2016. < https://gem.co/health>.
7. Jovanovic, Boyan, and Peter L. Rousseau. "General Purpose Technologies." *Handbook of Economic Growth* (2005): 1182-221. Web. 3 Aug. 2016. <http://www.nyu.edu/econ/user/jovanovi/JovRousseauGPT.pdf>.
8. Sarasola, Magdalena Ramada. "Insights: Want to Get an Insurer's Attention, Just Say Blockchain." *Willis Towers Watson*. N.p., 4 July 2016. Web. 3 Aug. 2016. <http://textlab.io/doc/9601382/--willis-towers-watson'>.
9. "Benefits of Electronic Health Records (EHRs)." *Health IT*. N.p., 30 July 2015. Web. 03 Aug. 2016. <https://www.healthit.gov/providers-professionals/benefits-electronic-health-records-ehrs>.
10. "Meaningful Use Definition & Objectives." *Health IT*. N.p., 6 Feb. 2016. Web. 03 Aug. 2016. <https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives>.
11. "Quick Stats." *Health IT*. N.p., 31 May 2016. Web. 03 Aug. 2016. <http://dashboard.healthit.gov/quickstats/quickstats.php>.
12. Kazley, A. S. "Association of Electronic Health Records with Cost Savings in a National Sample." *National Center for Biotechnology Information*. U.S. National Library of Medicine, 1 June 2014. Web. 03 Aug. 2016. <http://www.ncbi.nlm.nih.gov/pubmed/25180501>.
13. Friedberg, Mark W. "Factors Affecting Physician Professional Satisfaction and Their Implications for Patient Care, Health Systems, and Health Policy." *RAND*. N.p., 2013. Web. 03 Aug. 2016. <http://www.rand.org/pubs/research_reports/RR439.html>.
14. Obama, Barack. "US Health Care Reform: Progress and Next Steps." *United States Health Care Reform: Progress to Date and Next Steps*. N.p., 2 Aug. 2016. Web. 03 Aug. 2016. <http://jama.jamanetwork.com/article.aspx?articleid=2533698>.
15. "The Effect of Medicaid HMOs on Spending and Health Outcomes." *The National Bureau of Economic Research*. N.p., n.d. Web. 07 Aug. 2016. <http://www.nber.org/bah/winter03/w9091.html>.
16. Misra, Saroj. "Physicians Practice 2016 Tech Report." *Physicians Practice: America's Practice Management Resource*. N.p., July 2016. Web. 07 Aug. 2016. <http://www.physicianspractice.com/technology-survey/physicians-practice-2016-tech-report>.
17. "Inpatient/Hospital Electronic Health Records Report." *Black Book Market Research*. N.p., 22 Sept. 2014. Web. 03 Aug. 2016. <http://www.blackbookmarketresearch.com/inpatienthospital-electronic-health-records/>.
18. "Interoperability in Healthcare Factsheet." *HIMSS EHR Association*. N.p., June 2016. Web. 7 Aug. 2016. <http://www.himssehra.org/docs/InteropStatus_FactSheet_Final_Links.pdf>.
19. "EHR Developer Code of Conduct." *HIMSS EHR Association*. N.p., Feb. 2016. Web. 3 Aug. 2016.

©2016, ARK Investment Management LLC. All content is original and has been researched and produced by ARK Investment Management LLC ("ARK") unless otherwise stated herein. No part of this content may be reproduced in any form, or referred to in any other publication, without the express written permission of ARK.

This material is for informational purposes only and does not constitute, either explicitly or implicitly, any provision of services or products by ARK. Nothing contained herein constitutes investment, legal, tax or other advice and is not to be relied on in making an investment or other decision. Investors should determine for themselves whether a particular service or product is suitable for their investment needs or should seek such professional advice for their particular situation.

All statements made herein are strictly beliefs and points of view held by ARK. Certain of the statements contained herein may be statements of future expectations and other forward-looking statements that are based on ARK's current views and assumptions and involve known and unknown risks and uncertainties that could cause actual results, performance or events to differ materially from those expressed or implied in such statements. In addition to statements that are forward-looking by reason of context, the words "may, will, should, could, expects, plans, intends, anticipates, believes, estimates, predicts, potential, projected, or continue" and similar expressions identify forward-looking statements. ARK assumes no obligation to update any forward-looking information contained herein. Although ARK has taken reasonable care to ensure that the information contained herein is accurate, no representation or warranty (including liability towards third parties), expressed or implied, is made by ARK as to its accuracy, reliability or completeness.

Any reference to a particular company or security is not an endorsement by ARK of that company or security or a recommendation by ARK to buy, sell or hold such security. ARK and clients as well as its related persons may (but do not necessarily) have financial interests in securities or issuers referenced. Investors should determine for themselves whether a particular security is suitable for their investment needs or should seek such professional advice for their particular situation.

Any descriptions of, references to, or links to other publications, sites, products or services do not constitute an endorsement, authorization, sponsorship by or affiliation with ARK with respect to any such publication, site, product or service or its sponsor, unless expressly stated by ARK. Any such publication, site, product or service have not necessarily been reviewed by ARK and are provided or maintained by third parties over whom ARK exercises no control. ARK expressly disclaims any responsibility for the content, the accuracy of the information, and/or quality of products or services provided by or advertised by these third-party publications or sites.