How Healthy is Blockchain Technology?

Stephen Wilson[i] and David Chou[ii]

i. Constellation Research, Sydney, Australia
ii. Children's Mercy Hospital Kansas City, MO, U.S.A.

HIMSS AsiaPac17, 13 September 2017, Singapore

Abstract

Blockchain captured the imagination with a basket of compelling and topical security promises. Many of its properties – decentralization, security and the oft-claimed "trust" – are highly prized in healthcare, and as a result, interest in this technology is building in the sector. But on close inspection, first generation blockchain technology is not a solid fit for e-health. Born out of the anti-establishment cryptocurrency movement, public blockchains remove 'people' and 'process' from certain types of transactions, but their properties degrade or become questionable in regulated settings where people and process are realities. Having inspired a new wave of innovation, blockchain technology needs significant work before it addresses the broad needs of the health sector. This paper recaps what blockchain was for, what it does, and how it is evolving to suit non-payments use cases. We critically review a number of recent blockchain healthcare proposals, selected by a US Department of Health and Human Services innovation competition, and dissect the problems they are trying to solve.

Background

The origins of blockchain

Blockchain emerged a little less than a decade ago, with a technical paper self-published by the pseudonymous Satoshi Nakamoto [16]. The system proposed by Nakamoto was designed to support a novel type of cryptocurrency called Bitcoin. While various forms of electronic cash had been proposed for at least 30 years, Bitcoin was designed not only to provide purely digital currency but to do so free of any centralized monetary authority. All e-cash schemes until then relied on a "digital mint", comparable to the reserve bank in a government-backed (i.e. "fiat") paper money system, to prevent Double Spends.

Nakamoto invented a novel scheme that, in effect, crowd sources the oversight of Double Spends. Bitcoin (abbreviated BTC) employs a peer-to-peer "trustless" network of thousands of nodes, across which every attempted spend is broadcast. A public history of all transactions is kept by the network, allowing the Bitcoin community to detect attempted Double Spends. Once each new spend has been vetted and agreed to, the network collectively commits to that spend, and updates the shared history.

Each update is in the form of an agreed block of transaction data (including sender, receiver, currency amount, and some optional metadata) which is appended and cryptographically bound to the previously settled history, thus forming a permanent chain. The huge pool of participants creates an infeasible burden for would-be fraudsters trying to manipulate the ledger or create fake transactions; under reasonable assumptions (which for brevity's sake need not be reviewed here), the ledger is therefore immutable. The Bitcoin blockchain is distributed and synchronized across a global network, making it redundant and highly available.

Running the blockchain network entails major computing resources. A particularly clever aspect of Nakamoto's blockchain is that it provides incentives for nodes to participate, in the form of a periodic Bitcoin lottery, where the chance of winning is proportional to the computational work that a node contributes to the community.

Blockchain's childhood

The original Bitcoin blockchain inspired the technically more sophisticated Ethereum platform. Ethereum founder and leader Vitalik Buterin argued in 2013 that blockchain needed a more powerful scripting language, with which to develop "Smart Contracts" and other trading features. Buterin launched the Ethereum blockchain in 2015. Like Bitcoin, Ethereum runs on a public ledger, with a large pool of nodes reaching consensus about the order of entries. Its native cryptocurrency is known as *Ether* (ETH).

The two pioneering public blockchains may be regarded as the first generation of the new class of distributed data management tools (sometimes referred to as Distributed Ledger, Shared Ledger, or Synchronous Ledger Technologies[1]). Both the Bitcoin and Ethereum platforms are supported by volunteer open source core development teams, and have attracted large communities of application developers. Ethereum is probably the most popular system for non-payments blockchain application development, thanks to its more sophisticated scripting language.

Blockchain's promise

Nakamoto solved what was thought for decades to be an unsolvable problem: the supervision of e-cash movements without a central administrator. Partly because of the sheer intellectual achievement and partly because of the excitement that goes with disintermediating banks and governments, expectations quickly grew that blockchain would be transformative far beyond payments. Certain technical features of blockchain, such as its redundancy, availability and resilience, are of course valuable in fields like healthcare (although these properties come at an unusually high price and with qualifications).

It is also widely believed that blockchain creates new ways to "trust" people online; its advocates have high hopes that it can improve social infrastructure like land registries, voting, and healthcare systems. We suggest that much of the hype around "trust" is misplaced, for the simple reason that blockchain was designed so that complete strangers could reliably exchange electronic money, without relying on any third parties. Blockchain is a complex mechanism that performs a difficult task *without trust*.

A great many applications for blockchain have been proposed and trialed in recent years, while in parallel, sober analysis has been building around its detailed properties. The broad

[1] See also "What do we mean by blockchain?" https://www.constellationr.com/blog-news/what-do-we-mean-blockchain.

hopes for blockchain are being refined, and new ledger techniques being developed in response, as we discuss later in this paper.

Blockchain's idiosyncrasies

The early blockchains share some idiosyncrasies and limitations that are not fully appreciated and which affect the applicability of the algorithms, especially in healthcare.

The "consensus" that characterizes the blockchain ledger is often exaggerated by non-technicians. Crucially, consensus is reached in public blockchains about one thing only, namely the order of entries in the ledger (for that is sufficient to resist Double Spend of either Bitcoin or Ether). The "validation" that is done of public blockchain entries is limited to checking their format and then voting on the order in which the entries were attempted. It is important that overly general claims not be made about consensus and validation; these terms have highly qualified, technical meanings within the blockchain architectures (although more advanced ledger technologies are beginning to allow for more nuanced types of consensus to be reached about data sets).

A subtle point is that the consensus algorithms deployed by public blockchains are shaped by *the starting assumption* that they operate without central administration. Many thousands of nodes participate in reaching agreement on the state of the Bitcoin or Ethereum only because the founders of these systems rejected fiat money systems. When hybrid blockchain systems are proposed, to meet non-cryptocurrency requirements such as encryption or permissions, architects should consider if there is any advantage in having the great networks reaching consensus when an administrator might be more efficient. Nakamoto him/herself said in the abstract of the seminal Bitcoin paper that "the main benefits [of the blockchain] are lost if a trusted third party is still required to prevent double-spending" [16].

Of special interest to health IT architectures is the fact that public blockchains are transparent and permissionless. Everyone sees everything on the ledger; anyone can participate in the network by running a node, using public domain software. Additional access controls and encryption are reasonably straightforward to graft onto a blockchain[2] but as discussed, the elaborate consensus algorithm then becomes disproportionately expensive. Note also that blockchains are quite unlike conventional databases. On the one hand, they lack the normal search, analysis and reporting tools native to regular databases; on the other hand, blockchains are more than mere storage mechanisms. The *raison d'être* for blockchain is to resolve the order of entries without an administrator; the act of making a successful blockchain entry results in confidence about the order of the entry.

Blockchain's adolescence

There have been several recent significant advances in blockchain practice, and changes of emphasis. It has been realized that non-cryptocurrency applications require confidentiality [18], permissions, different forms of consensus, and much smaller pools of participants. Newer Synchronous Ledger Technologies are emerging rapidly to realize these needs, but they alter the balance of properties delivered. For example, the oft-mentioned "immutability" of the public blockchains is qualified when smaller pools of nodes are

[2] Remember that most non-cryptocurrency data stored on a blockchain is inserted into dummy transactions, using interfaces that allow for descriptive and other metadata to be recorded along with spends. Encryption, if desired, needs to be taken care of "off chain" before the transaction is composed.

involved. To maintain security, the advanced architectures will feature additional layers of encryption and cryptographic key management.

We return to these developments later in this paper.

The ONC Blockchain Challenge

The US Department of Health & Human Services Office of the National Coordinator (ONC) operates a technology lab and periodically conducts innovation challenges.[3] In July 2016, the ONC called for white papers to be submitted on the topic of blockchain technology and its "potential use in health IT to address privacy, security, and scalability challenges of managing electronic health records and resources".[4] The ONC Blockchain Challenge aimed to investigate the cryptography and other fundamentals of the technology, and explore its potential to advance interoperability, augment Patient Centered Outcomes Research and the Precision Medicine Initiative, delivery system reform, and deliver other healthcare needs. Over 70 submissions were received, fifteen of which were awarded cash prizes of up to $5,000.

In September 2016, the ONC and the National Institute of Standards and Technology (NIST) convened a two-day workshop on "The Use of Blockchain in Healthcare and Research", at which a selection of the challenge winner presented their work.[5] One of us (Wilson) attended the workshop, made a presentation on the evolution of blockchain use cases and architectures[6] and participated in discussions.

The fifteen winning ONC challenge papers, and the workshop discussions, provided a snapshot of the state of blockchain thinking in the health sector, and the basis for this research paper.

Method for this study

We critically reviewed the fifteen winning blockchain challenge proposals. We appraised each paper against the technical capabilities of known blockchain technologies, with some reference to the expectations of the new and emerging Synchronous Ledger Technologies. We identified which security claims made for blockchain can be substantiated, and which, at this time, cannot. We also looked at how the papers expressed the particular needs of healthcare systems and how the properties of blockchain match those needs.

Characterizing the papers

The major affiliations of the authors may be categorized as follows:

[3] See https://oncprojectracking.healthit.gov/wiki/display/TechLabI/ONC+Tech+Lab+Innovation+Home.

[4] See https://www.healthit.gov/newsroom/blockchain-challenge.

[5] See https://oncprojectracking.healthit.gov/wiki/display/TechLabI/Use+of+Blockchain+in+Healthcare+and+Research+Workshop.

[6] "Blockchain's Challenges in Real Life", Steve Wilson, September 26. 2016, http://bit.ly/2gVtukZ.

Technology Business	6
University or Hospital	4
Non provider Health Business	2
Non Government Organisation	1
Independent Adviser or Analyst	2

Table 1: Blockchain paper author affiliations

Most of the papers proposed using one of the first generation public blockchains – Bitcoin or Ethereum – or an evidently similar type of system, without being specific. Two of the papers presented in outline brand new consensus algorithms operating in otherwise Bitcoin-like decentralized ledger algorithms. Three of the papers anticipated next generation ledger algorithms which, at the time, were beginning to emerge.

Bitcoin blockchain	2
Ethereum blockchain	3
Novel blockchain of the authors' design	2
Other existing blockchain	1
Non-committal but well specified[7]	3
Generic or poorly specified[8]	4

Table 2: Proposed blockchain types

Results and Analysis

In overview, a significant number of the fifteen blockchain proposals assume security properties of the first generation blockchain that cannot in fact be sustained beyond cryptocurrency, in e-health applications. Most papers accept without question that the core blockchain security promises of immutability and decentralization will be maintained even as the systems are hybridized with conventional systems. For reasons that are not clear, many proposals expect that "interoperability" will be delivered by blockchains and rescue healthcare from the problems of Health Information Exchanges (HIEs). Above all, it is not clear how the "trustlessness" of public blockchains should sit with the highly administered and regulated environment of healthcare. As a result, we found most proposals are overly optimistic about blockchain's applicability to healthcare.

We now analyse these shortcomings in detail.

Interoperability

Naturally, the most common theme across all of the winning papers was interoperability, for this is one of the top objectives of the ONC and a long-standing challenge in the sector. Disparate health systems famously use different terminologies and codes for the same

[7] These papers described precisely what they saw as characteristics of blockchain technology and argued their applicability to healthcare applications. Some of these were alert to developments beyond Bitcoin and Ethereum, such as R3 and Hyperledger; some provided selection criteria for applicable blockchains.

[8] A number of the papers described blockchain so loosely that it was not possible to tell if the authors had any actual platform in mind, or were instead imagining what was possible.

medical procedures. As one paper states, "disparate use of healthcare terminology limits data comprehension" [12].

Adoption of new standard terminologies and messaging standards, like HL-7[9] and ICD,[10] is infamously slow, often taking a decade or longer. Large clinical systems are notoriously complex to implement, and along the way invariably see major customization, which makes each installation peculiar to its setting, and resistant to interfacing with other systems. In the U.S. especially, HIEs have been a common response to these problems, the basic idea being that an intermediary switching system will broker compatibility between disparate e-health programs. But health information exchange has been easier said than done.

While all fifteen ONC blockchain papers stressed interoperability, only Peterson et al [12] go into the topic in any detail. In particular, they were the only participants to even mention *semantic* interoperability; that is, the question of what terms mean across systems. This is the crucial issue in e-health interoperability.

It is not clear how any blockchain is supposed to bring a breakthrough here. None of the ONC challenge proposals explains how a ledger will mechanically deal with any aspect of e-health interoperability. Public blockchains create specific protocols to addresses the order of entries in a distributed ledger, to prevent Double Spend without an administrator. Nothing about blockchain's fundamentals relates to messages, medical coding standards or healthcare semantics. Blockchain is not actually concerned with interoperability, for in its native form, it only promises to create a siloed cryptocurrency system.

Re-Structuring How Health Data is Stored

The next most prominent theme at the blockchain challenge and workshop was healthcare information silos. Several proposals emphasize that data is fragmented, siloed, concentrated in local repositories, and hard to find when needed. There is merely an implication in many of the works that patient data will be reorganized under blockchain architectures to make it more accessible and less dispersed. One presentation[11] at the workshop highlighted the "discrepancies, expensive reconciliation and storage costs" associated with siloed healthcare data; one of the papers asserted that "blockchain eliminates data silos and aggregates clinical data from EMR" [8].

None of the papers however set out exactly how blockchains could help restructure health records management. Most papers were scant on detail, although one proposed explicitly storing patient data in bulk on a blockchain [9] (before going on to elaborate that "a suitable blockchain infrastructure for healthcare does not currently exist"). The Accenture presentation described a "target state" where blockchain technology would enable a "central store or 'golden state' of data".

The workshop afforded the opportunity for detailed discussion of the implications of storing patient data on a blockchain. The transparency of public blockchains poses a clear confidentiality problem; a less obvious problem is that the limited block size of all

[9] The "Health Level 7" standards facilitate the exchange, integration, sharing, and retrieval of electronic health information; see http://www.hl7.org/implement/standards.

[10] The World Health Organization's International Classification of Diseases; see http://www.who.int/classifications/icd/en.

[11] "Blockchain: Securing a New Healthcare Interoperability Experience", Accenture, http://bit.ly/2gToQ2U.

conceivable blockchains makes it impossible to store whole medical images and similar large files. And so consensus was reached as the workshop proceeded that personal information and Protected Health Information (PHI) should not in fact be stored on the blockchain. Generally speaking, most attendees settled on the notion that blockchains might hold only pointers to patient records (or perhaps hashes or other "fingerprints" of the raw data).

If patient metadata is being stored on blockchains rather than data, then the point of the exercise needs to be reconsidered. Patient records might be more easily discoverable in this sort of scheme, because with the right API, anyone anywhere in the world can readily interface to the ledger. But then the security promise of blockchain becomes compromised. If patient data stays put, then it is not made immutable by a blockchain index, nor redundant, and thus the siloed and expensive current arrangements will persist. The blockchain doesn't even make records more accessible. Records today are out-of-bounds to unauthorized personnel across organizational domains, and there is nothing that blockchain will do about that. Therefore, we conclude that the ONC challenge proposals will not in fact lead to significant improvements to health record management.

It is notable that one of the challenge team's presentations did allude to more subtle benefits of storing healthcare metadata on a blockchain. IBM described[12] applications in clinical trials and consent management (amongst other things) where agreement on the state of the healthcare metadata and the timing of changes to the data may be critical.[13]

Key Management

A third problem area we identified for all blockchain challenge proposals was the omission of *key management*. This is the central administrative challenge of almost every cryptographic security system: how do we get the right encryption keys and credentials into the right hands, and keep them there, so all participants can be sure of who and what they are dealing with?

A special, perhaps unique feature of the original blockchain is that it dispensed with key management for the special use case of peer-to-peer cryptocurrency. Nakamoto's architecture allows people to exchange e-cash reliably without needing to know anything about each other, and with no dependency on administrators or regulators. But when we do need to know who's who in a health system (at the very least to be sure all the carers, researchers, insurers and patients are properly authorized) then key management has to part of the security system.

Yet the fundamental design tenets of the public blockchains do away with authority structures. Blockchain is "trustless": it achieves its security promises without the sort of administration normally required in any transaction system (which is why thousands of participants are required to keep the blockchain networks running safely). Textbook information security is based on a threefold mix of 'Technology', 'People' and 'Process' but blockchain protects its assets with technology alone.

On the other hand, healthcare is intrinsically hierarchical. Inherent to the system are management structures, authorizations, credentialing bodies, quality assurance and audits –

[12] "Blockchain: The Chain of Trust and its Potential to Transform Healthcare", IBM, http://bit.ly/2jglT18.

[13] We now know that IBM had been working on advanced blockchain techniques in the Hyperledger Fabric project around the time of the ONC challenge, and a more evolved vision for healthcare data management is emerging there.

all the things that Nakamoto, Buterin and like-minded blockchain proponents expressly reject. And as mentioned above when a blockchain deployment still has to involve third parties, then the benefits of the algorithm are lost.

Discussion

When considering whether first generation blockchain algorithms have a place in e-health, we should bear in mind what they were designed for and why. Bitcoin and Ethereum are intrinsically political and libertarian; their outright rejection of central authority is a luxury only possible in the rarefied world of cryptocurrency but is simply not rational in real world healthcare, where accountability, credentialing and oversight are essentials.

Despite its ability to transact and protect pure "math-based money", it is a mistake to think public blockchains create trust, much less that they might disrupt existing trust relationships and authority structures in healthcare. Blockchain was designed on an assumption that participants in a digital currency would not trust each other, nor want to know anything about each other (except for a wallet address). On its own, blockchain does not support any other real world data management.

The newer Synchronous Ledger Technologies – including R3 Corda, Microsoft's Blockchain as a Service, Hyperledger Fabric and IBM's High Security Blockchain Network – are driven by deep analysis of the strengths and weaknesses of blockchain, and then re-engineering architectures to deliver similar benefits in use cases more complex and more nuanced than lawless e-cash [18][19]. The newer applications involve orchestration of data streams being contributed by multiple parties (often in "coopetition") with no one leader or umpire. Like the original blockchain, these ledgers are much more than storage media; their main benefit is that they create agreement about certain states of the data. In healthcare, this consensus might be around the order of events in a clinical trial, the consent granted by patients to various data users, or the legitimacy of serial numbers in the pharmaceuticals supply chain.[14]

Conclusion

We hope healthcare architects, strategic planners and CISOs will carefully evaluate how blockchain technologies across what is now a spectrum of solutions apply in their organizations, and understand the work entailed to bring solutions into production.

Blockchain is no silver bullet for the challenges in e-health. We find that current blockchain solutions will not dramatically change the way patient information is stored, because most people agree that personal information does not belong on blockchains. And it won't dispel the semantic interoperability problems of e-health systems; these are outside the scope of what blockchain was designed to do.

However newer blockchain-inspired Synchronous Ledger Technologies show great potential to address nuanced security requirements in complex networks of cooperating/competing actors. The excitement around the first blockchain has been inspirational, and is giving way to earnest sector-specific R&D with benefits yet to come.

[14] "How two California startups are preparing pharma companies for blockchain", March 30, 2017, http://medcitynews.com/2017/03/two-california-startups-preparing-pharma-companies-blockchain.

ONC Blockchain Papers

See http://www.cccinnovationcenter.com/challenges/block-chain-challenge/view-winners

[1]. *Blockchain and Health IT: Algorithms, Privacy, and Data* Allison Ackerman Shrier, Anne Chang, Nadia Diakun-thibault, Luca Forni, Fernando Landa, Jerry Mayo, Raul van Riezen, and Thomas Hardjono

[2]. *Blockchain: Securing a New Health Interoperability Experience* Brodersen C, Brian Kalis, Emily Mitchell, Eril Pupo, and Andy Truscott

[3]. *Blockchain Technologies: A Whitepaper Discussing how Claims Process can be Improved* Kyle Culver

[4]. *Blockchain: Opportunities for Health Care* RJ Krawiec, Dan Barr, Jason Killmeyer, Mariya Filipova, Allen Nesbitt, Adam Israel, Florian Quarre, Kate Fedosva, and Lindsay Tsai.

[5]. *A Case Study for Blockchain in Healthcare: "MedRec" Prototype for Electronic Health Records and Medical Research Data* Ariel Ekblaw, Asaph Azaria, John D. Halamka, and Andrew Lippman

[6]. *The Use of a Blockchain to Foster the Development of Patient-Reported Outcome Measures* Jason Goldwater

[7]. *Powering the Physician Patient Relationship with 'HIE of One' Blockchain Health IT* Adrian Gropper

[8]. *Blockchain: The Chain of Trust and its Potential to Transform Healthcare – Our Point of View* Srinivas Attili, Susheel K Ladwa, Udit Sharma, and Anthony F. Trenkle

[9]. *Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records* Drew Ivan

[10]. *ModelChain: Decentralized Privacy-Preserving Health Care Predictive Modeling Framework on Private Blockchain Networks* Tsung-Ting Kuo, Chun-Nan Hsu, and Lucila Ohno-Machado

[11]. *Blockchain for Health Data and Its Potential Use in Health IT and Health Care Related Research* Linn L, Koo M

[12]. *A Blockchain-Based Approach to Health Information Exchange Networks* Kevin Peterson, Rammohan Deeduvanu, Pradip Kanjamala, and Kelly Boles

[13]. *Adoption of Blockchain to enable the Scalability and Adoption of Accountable Care* Ramkrishna Prakash

[14]. *A Blockchain Profile for Medicaid Applicants and Recipients* Kathi Vian, Alessandro Voto, and Katherine Haynes-Sanstead

[15]. *Blockchain & Alternate Payment Models* King Yip

General References

[16]. *Bitcoin: A Peer-to-Peer Electronic Cash System* Satoshi Nakamoto, 2008, https://bitcoin.org/bitcoin.pdf

[17]. *Untraceable electronic cash* David, D, Fiat, A., and Naor, M. Proceedings on Advances in Cryptology—CRYPTO '88, Lecture Notes in Computer Science **403** Springer-Verlag, pp. 319–327, 1990

[18]. *Introducing R3 Corda: A Distributed Ledger Designed for Financial Services*, Richard Gendal Brown, R3, April 5, 2016, https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services

[19]. *Protecting Private Distributed Ledgers*, Steve Wilson, Constellation Research, 2016.

About the Authors

Steve Wilson leads the Digital Safety and Privacy business unit at the independent Constellation Research. His career spans 30 years in R&D leadership and advisory roles, in Australia and the USA. For most of that time he has been involved in healthcare. For the past 22 years he has specialized in digital identity and privacy. His advisory clients include state & federal health departments, public sector human services organizations, public and private insurers, and numerous healthcare IT start-up businesses. Steve has been awarded nine patents for identity and privacy technologies, and is currently undertaking a PhD on the evolution and ecology of digital identity, at the University of New South Wales.

Wilson attended the ONC Blockchain Challenge in Gaithersburg USA, September 2016; the Department of Health and Human Services paid for his travel and accommodation.

David Chou is Vice President / Chief Information & Digital Officer at Children's Mercy Kansas City. Children's Mercy is the only free-standing children's hospital between St. Louis and Denver, and provides comprehensive care for patients from birth to 21. It is consistently ranked among the leading children's hospitals in the United State and was the first hospital in Missouri or Kansas to earn the prestigious "Magnet" designation for excellence in patient care from the American Nurses Credentialing Center. Prior to Children's Mercy, David was CIO at University of Mississippi Medical Center, that state's only academic health science center. David also served as senior director of IT operations at Cleveland Clinic Abu Dhabi, and CIO at AHMC Healthcare in California. His work has been recognized by several publications, and he has been interviewed by a number of media outlets. David is one of the most mentioned CIOs on social media, and is an active member of both CHIME and HIMSS.