Powering the Physician-Patient Relationship with HIE of One Blockchain Health IT

Adrian Gropper, MD

August 7, 2016

- Address whether there is a place in health IT and/or healthcare related research for the technology [1];

Physicians steer treatment together with patients and are responsible for the vast majority of decisions, and therefore expenditures, in healthcare. Yet the technology that mediates the physician-patient relationship today is not directly purchased or controlled by either the physicians or the patients. Electronic health records and health information exchange technology are sold as strategic assets to institutions, typically very large businesses, that currently have incentives to maximize institutional growth. We seek a better balance of institutional needs with the needs of physicians and patients.

It is widely accepted that reducing healthcare cost growth requires genuine practice reform. Few institutions, however, are planning to reduce their own size. By focusing health information technology and interoperability on the physician-patient relationship we bypass the inertia of institutions, fertilize the environment for value-based payment, and optimize care options among hospitals, the community, and home, as appropriate.

Blockchain is widely recognized for its ability to empower innovators and individuals on a large scale in an environment that includes the necessity of institutions. The appropriate application of blockchain technology to health IT can shift the balance to the physician-patient relationship. It’s hard to imagine a more effective lubricant for innovation in our complex privatized healthcare system.

- Describe the value of Blockchain to the healthcare system;

Blockchain has proven value at reducing transaction costs in trading systems and expanding the accessible market for innovators. It does this by shifting power to the edges of the network - the consumers. This paper describes a standards-based way for blockchain to shift decision making and purchasing power to physicians and patients.

Shifting control of health IT away from the hospital not only opens the market making it accessible to physicians and patients but it also opens the market for decision support at the point of care. For example, hospitals are reluctant to show physicians the cost of a medication or procedure when they’re about to order it. They are even less likely to present the physician with a list of alternatives. On the patient side, there’s no way to independently advise the patient of out-of-pocket costs, alternative sources, and typical risks while the patient and physician are engaged in making very costly decisions. Mobile devices in the physician-patient encounter and secure blockchain infrastructure enable the next generation of decision support apps at the point of care.

Our project, HIE of One, (Health Information Exchange of One) shifts the trusted intermediary role away from the hospital and into the blockchain. The blockchain can also provide the link between physician credentials and patient identity.

In the current health IT architecture, the hospital is responsible for both credentialing the individuals and securing the protected health information (PHI). In the HIE of One architecture, credentialing is done by institutions such as medical societies or state agencies that do not have or want access to PHI. Identity of physicians and of patients is managed on the blockchain without placing any PHI on the blockchain. (N.B. Identity is a write-seldom-read-mostly application that's ideally suited for the write seldom read mostly character of the blockchain where proof-of-work is only required to create or update an identity while use of the identity costs essentially nothing.) Finally, in the HIE of One model, the PHI stays in place wherever it was generated or is most convenient. HIE of One works with PHI in institutional EHRs, PHRs, regional health information databases, cloud wellness services, or the Precision Medicine Initiative.

HIE of One links patient PHI to blockchain identities and blockchain identities to verified credential provider institutions that don't have PHI and don't want the liability of PHI. This not only lowers transaction costs but it improves security for all participants. Data moves under the control of blockchain-mediated identity and trust.

- Identify potential gaps in standards created and/or resolved by Blockchain;

Practices that protect patient privacy have not kept up with the scale of today's hospital and HIE networks. When 5 or 10 Million patients and 50,000 staff have access to a single EHR system or delivery network, standards for consent, authorization, single-sign-on, and accounting of disclosures have proved elusive. At a national scale like the Precision Medicine Initiative, today's practices are insufficient.

High-level panels including PCAST and JASON concluded that separating access control from PHI stewardship will be necessary to achieve interoperability at scale. But this goes against the current role of hospitals as combined holders and controllers of PHI. The gaps in current standards are not incidental. They are the result of an imbalance of IT purchasing power in favor of hospitals and their EHR vendors.

Another obvious gap is the lack of identity standards in healthcare. There is essentially zero adoption of identity federation (single sign-on) for either physicians or patients. In addition, identity matching seems to be a problem unique to healthcare and has spawned expensive and unreliable probabilistic methods that harm privacy and will not scale to the needs of a nation.

Blockchain has some established identity standards to the extent that it is able to reliably maintain the integrity and accessibility of individual “wallets” but there are gaps in linking the cryptographic identity of blockchains to single-sign-on standards like OpenID Connect [2] and to verified claims [3].

HIE of One is working with multiple blockchains under the auspices of the World Wide Web Consortium (W3C) to advance blockchain ID standards [4] and to align them with the OpenID Connect capability already in HIE of One [5] and our FHIR-standard EHRs [6]. The initial demo of HIE of One based on HL7 FHIR - OpenID Connect - Kantara UMA standards was made to the OpenID HEART workgroup in February 2016 [7].

To fill the blockchain identity standards gap we are now working with the W3C Web Authentication [8, 9] and W3C Verifiable Claims [3] standards workgroups along with the W3C Blockchain Community [10] group and contributing to the HL7 FHIR [11] standards and UMA [12] development as well. This work will be presented at the Rebooting the Web of Trust meeting at the end of October 2016 [13].

- Discuss the effectiveness of Blockchain to function in the “real world.”

The effectiveness of managing blockchain private keys has had a great deal of “real world” experience because it is the core of blockchain wallet functionality. The use of private keys for identity authentication has been shown at scale by the FIDO Alliance products and is being adopted as WebAuthn / FIDO 2.0 by the W3C [8, 9].

The effectiveness of managing blockchain identity in the “real world” has not been established but second-generation systems already exist and two vendors (one Bitcoin and the other Ethereum based) have been selected for integration with the Microsoft Azure cloud platform [14]. Blockchain ID has been broadly available for over a year. [15]

The HIE of One system [16] does not store or manage PHI on the blockchain. Thus, it avoids serious privacy and scalability issues with blockchain technology. The HIE of One system uses FHIR [11], OAuth2 [17] , and UMA [12] together as in HEART [18] to secure and manage access to PHI. Although FHIR and UMA are young, the effectiveness of these standards in the real world is not in doubt [19].

The link between the user ID (physicians and patients both) and the PHI is managed by OpenID Connect in HIE of One. The effectiveness of this approach has had extensive real-world proof by Google [20] and many others [21].

In summary, the HIE of One approach uses blockchain conservatively for ID only and leverages the vast experience with OAuth2 and OpenID Connect to minimize the deployment risk. Blockchain ID is very low cost, on the order of pennies for account creation or changes of key attributes. Because our approach to PHI management does not modify the blockchain at all, it adds no proof-of-work cost and is therefore as cost-effective as any FHIR / OAuth data management scheme. HIE of One transaction costs will benefit from the large-scale of FHIR APIs in general in a way that proprietary PHI management APIs on or off the blockchain cannot.

- Discuss how Blockchain links to the stated objectives and national priorities.

Blockchain links the stated objectives in the Nationwide Interoperability Roadmap, PCOR, PMI, delivery system reform, and other national healthcare delivery priorities by enabling patient-directed exchange in a cost-effective and scalable way.

PMI, PCOR, and the Nationwide Interoperability Roadmap already recognize the need for patient-directed exchange. Delivery systems reform is not directly associated with patient-directed exchange, but HIE of One uses blockchain to put control of interoperability and decision support at the point of care in the hands of patients and physicians. As discussed at the beginning of this paper, this shift of control away from hospitals will lubricate delivery systems reform through competition and the reduction of transaction costs on a national scale.

- HIE of One Self-Sovereign ID Innovation

The current generation of standards-based identity providers (IdP), like Google and upcoming EHR FHIR implementations, manage user authentication and reputation together in one responsible institution. This makes the IdP bear the risk of a security compromise that exposes PHI resources and it requires the federated institutions to “trust” the IdP, often a competitor. A self-sovereign ID would enable verifiable reputation and attributes of physicians and patients without any institution bearing the risk of user authentication. Management of the private key used for authentication is entirely under the control of the individual person and supports the strongest levels of non-repudiation including recently adopted EU e-IDAS regulations [22]. With self-sovereign ID, the trust of a relying party is directly linked to an individual person's control of a secure element without any institutional intermediary. The power of this approach has already been shown by non-institutional trust systems like Bitcoin and FIDO [23].

Permissionless distributed public ledgers, like Bitcoin and Ethereum, can replace some aspects of institutional trust with cryptography. In particular, a person in control of his/her private key (in the e-IDAS sense of non-repudiation of control) can authenticate themselves with a high level of assurance if the private key can also be associated with a trusted reputation mechanism. This paper explores the application of blockchains in support of more complex transactions where the participants have reputation or a verified attribute and the information exchanged is private.

We use a licensed MD writing a prescription as an example transaction. Aside from the physician and the patient as self-sovereign individuals, the transaction also involves two institutions: the pharmacy and the verifier of the MD license. Success will mean that neither of the two institutions has to trust an institutional identity provider for either the physician or the patient as long as the jurisdiction they are in recognizes the authority of a blockchain-based identity and reputation [24].

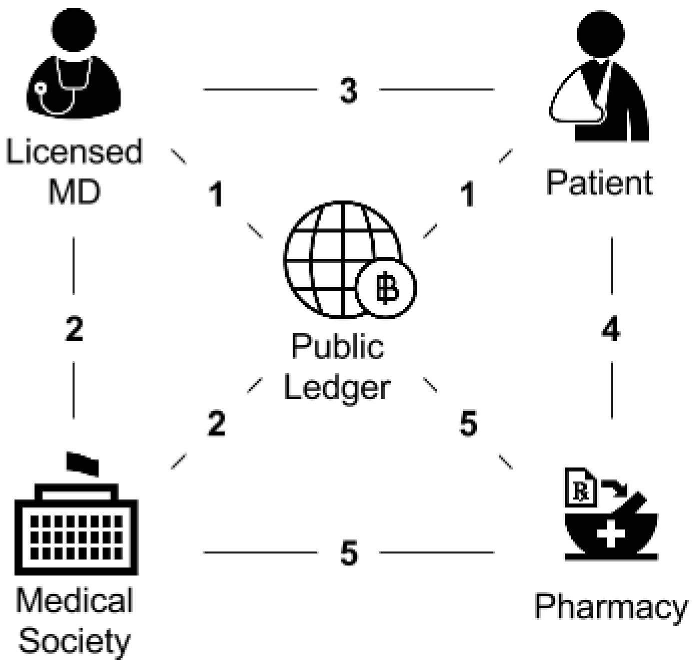

Fig. 1 - Personal and Institutional Trust

With reference to Figure 1:

1. The Licensed MD and Patient each has a self-sovereign blockchain ID.
2. The Licensed MD presents ID and license credentials to the Medical Society.
3. The Licensed MD writes a prescription to the Patient including a license claim.
4. The Patient presents the prescription to any Pharmacy.
5. The Pharmacy verifies the MD's license claim with the Medical Society.

Note that patient-specific protected health information (PHI) is only present in transactions 3 and 4. The Medical Society does not bear any risk of access to patient information. Transaction information is not present on the blockchain except optionally as a time-stamped hash representing a digital postmark as evidence in case of dispute.

A prescription illustrates the essential elements of identity: the MD has to have a valid license and a way to sign the transaction. The patient has to be identified in an accountable way either directly by the pharmacy or indirectly through the ordering physician. The transaction has to leave residual documentation acceptable in case of dispute. Finally, the contents of the transaction have to remain private to the parties directly involved. With the obvious exception of attribute verification, this paper proposes a path to meeting these requirements without recourse to hospital trust and dependency on a hospital information system. The method is based on each individual having total non-repudiable control over their self-sovereign support technology (SSST) and every actor having access to a distributed public ledger.

Blockchain technology is well suited for decentralized identity (DID) that does not depend on a centralized root of trust such as the Domain Name System or a small number of trusted registrars. DID extends blockchain methods to enable a lifelong practical and reliable identifier and attributes linked to that identifier under the self-sovereign control of the individual person. A number of DID systems based on the Bitcoin and Ethereum blockchains are coming on the market. This paper describes how technology under the total control of the MD and the patient respectively can leverage DID to allow for a prescription or equivalent regulated transaction.

A typical transaction between two self-sovereign blockchain wallets as value containers is illustrated in Figure 2.

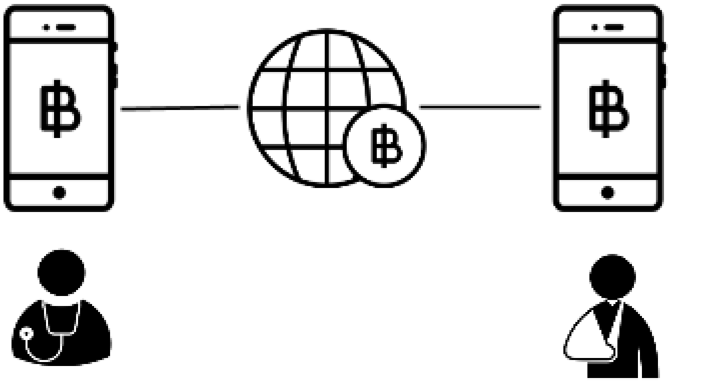

Fig. 2 - A Bitcoin transaction between two wallets

SSST describes an Identity Container (Figure 3) as a combination of a mobile user interface that controls the identity and an always-connected server that stores attributes, policies, and transaction receipts associated with that identity. Attributes, typically PHI like the contents of the prescription, are meant to be selectively shared. Policies are kept private but they control external access to attributes. Receipts are the signed result of transactions stored in case of audit or dispute.

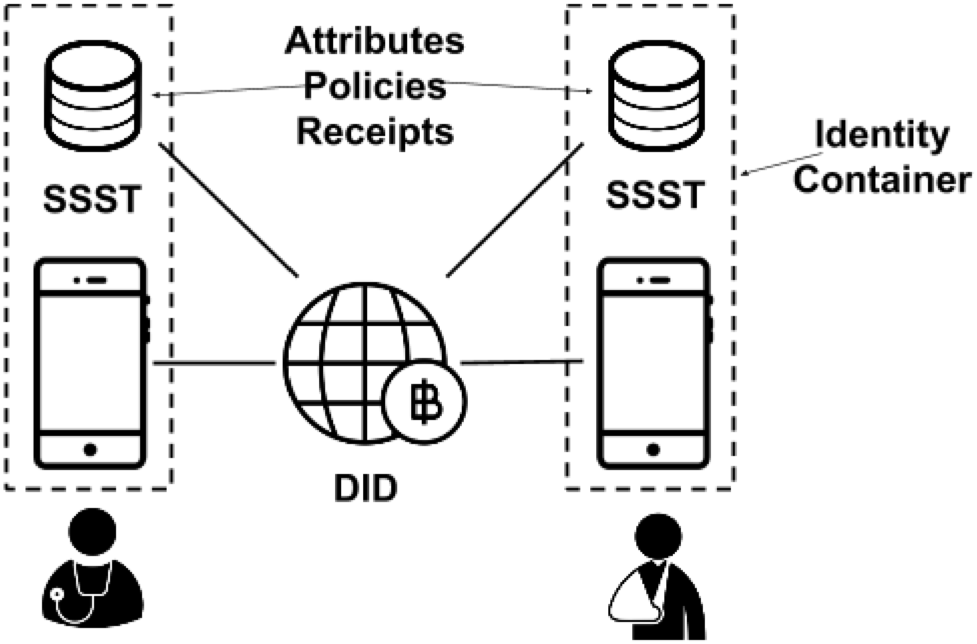

Fig. 3 - A Prescription transaction between two identity containers

Writing a prescription involves a number of steps (Figure 3):

1. The MD uses a DID-associated credential to sign-in to the electronic health records (EHR) component of her SSST.

2. The MD’s EHR displays a patient list with links to each patient’s SSST EHR.
3. By clicking on a patient in the list, the MD attempts to single-sign-on to the patient’s SSST EHR using her DID as the trusted identity provider.
4. The patient’s authorization server component of her SSST looks up the MD’s medical license number attribute via his DID, and verifies the medical license status against the state medical society’s physician directory server (not shown on Figure 3). (Note that the medical society directory service is not self-sovereign technology. Also, for physician privacy, access to the directory may be controlled by policies behind the MD’s SSST authorization server component.)
5. The MD creates a new prescription record in the patient’s SSST EHR including the patient’s DID and signs it with credentials linked to her DID. The MD’s signature is non-repudiable based on the mobile component of her SSST per applicable law as in e-IDAS.
6. The signed prescription is stored in both the MD’s and the patient’s SSST EHR.
7. The patient signs-in to a pharmacy (not shown on Figure 3) with her DID credentials. If the prescription is for a controlled substance, the patient’s prescription request is non-repudiable based on the mobile component of her SSST. Otherwise, the DID simply verifies that the patient that signed-in to the pharmacy matches the patient in the prescription.
8. A prescription is shipped to the patient. (Privacy note: Optionally, if an intermediate shipper or an insurance company is used, the patient’s address and payment details can be blinded from the pharmacy by the physician’s SSST.)
9. Access to the patient’s pharmacy records may or may not be permitted based on policies behind the patient’s SSST authorization server component.
10. In case of a dispute, either the patient or the MD can present the prescription as stored in the receipts component of their respective SSST.

A practical self-sovereign support technology will have other components not listed above. A series of workshops at the Internet Identity Workshop XXII resulted in a working list of 10 for consideration [25].

A partial list of software services in the SSST might include:

- Mobile Device
    - Secure element
        - DID, Signing, Encryption, Payment keys
    - User interface
    - Biometric (face recognition, iris, fingerprint)
    - Some verified attributes
    - Notification endpoint (SMS, email)

- Server
  - UMA Authorization Server
    - Secure policy store
  - Federated ID Client Support
    - DID
    - OpenID Connect
    - Whitelist of federated ID providers
  - Privacy-related server software - e.g. electronic health record
  - Protected attribute store
  - Transaction receipt store

SSST components will be provided by community-supported and commercial vendors:

- A mobile app to manage DID keys, biometric access controls, and key recovery.
- The online component of the SSST could be built from source, run as an executable from a trusted source, or outsourced to a service [26].
- Attribute verification would be operated as a medical society member service.

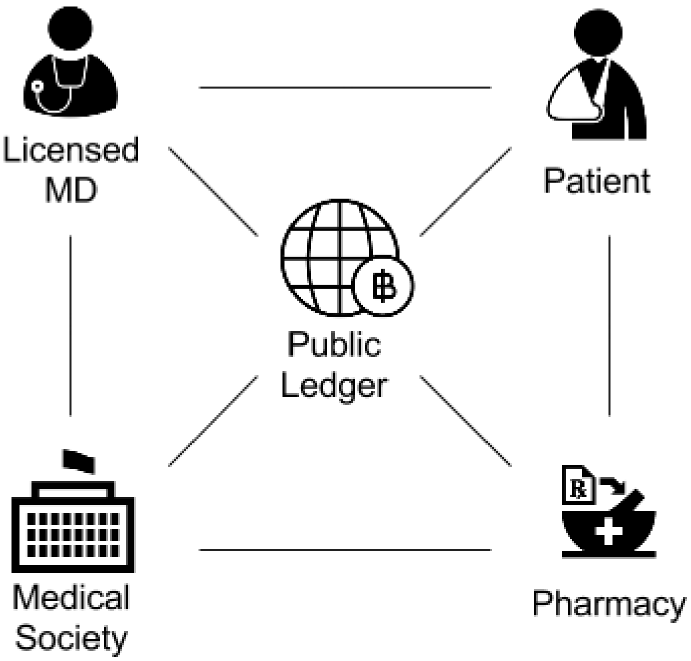

Fig. 4 - The Value Propositions for Self-Sovereign Support Technologies

With reference to Figure 4:

- The Medical Society offers a valuable credentialing service to members without risk of patient data breach.

- The Licensed MD has total control over her relationship with the patient and can practice to the full value of her professional license.
- The Patient can save money by choosing the pharmacy and can preserve privacy by working directly with a physician.
- The Pharmacy, and other health services providers, can innovate and add value without the mediation of intermediary hospitals and EHR vendors.
- Suppliers of SSST to physicians and patients can add value as app developers and support organizations without patient lock-in or inserting themselves into the institutional trust chain.

The major benefit of self-sovereign support technology in this example is the re-decentralization of the trusted relationship between the physician and the patient. The full value of the medical consultation is now available to the two principal parties, but each of them can manage their own policies to provide access to shared resources such as a physician directory or a pharmacy. A second benefit of this approach is security through diversity. All patients and all physicians can have different self-sovereign technology to support their security, privacy and economic interests.

Acknowledgements: Christopher Allen, Shannon Appelcline, and Rebooting the Web of Trust, Doug Schepers, Blockstack, Consensys, Evernym, YOTI, Eve Maler and the UMAnitarians, Philip Sheldrake and the hi:project, IIW, MITREID Connect, the VRM list, and the MIT Bitcoin Club as well as Michael Chen, MD who created and modified the open-source NOSH electronic health record and coded the UMA AS in support of our evolving proof-of-concept.

References:

1. http://www.cccinnovationcenter.com/challenges/block-chain-challenge/
2. http://openid.net/connect/
3. Verifiable Claims Use Cases W3C Editor's Draft 22 June 2016
4. Blockchains and the Web Report
5. https://github.com/shihjay2/hieofone-as
6. NOSH Charting System
7. https://www.youtube.com/watch?v=QX2JbYg2TZI&feature=youtu.be

8. H. Le Van Gong, D. Balfanz, A. Czeskis, A. Birgisson, J. Hodges, FIDO 2.0: Web API for accessing FIDO 2.0 credentials, World Wide Web Consortium (W3C) Member Submission, November 2015. https://www.w3.org/Submission/2015/SUBM-fido- web-api-20151120/.

9. Web Authentication: A Web API for accessing scoped credentials W3C First Public Working Draft, 31 May 2016

10. https://www.w3.org/community/blockchain/

11. https://www.hl7.org/fhir/

12. WG - User Managed Access

13. https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016

14. https://bitcoinmagazine.com/articles/microsoft-building-open-blockchain-based-identity-system-with-blockstack-consensys-1464968713

15. https://www.usenix.org/system/files/conference/atc16/atc16_paper-ali.pdf

16. HIE of One UMA Authorization Server

17. http://oauth.net/

18. http://openid.net/wg/heart/

19. http://www.healthit.gov/facas/sites/faca/files/HITJC_APITF_Recommendations.pdf

20. https://developers.google.com/identity/protocols/OpenIDConnect

21. http://openid.net/certification/

22. https://www.dlapiper.com/en/us/insights/publications/2015/08/new-eu-regulation-for-electronic-signatures/

23. https://fidoalliance.org/

24. http://www.coindesk.com/vermont-blockchain-timestamps-approval/

25. http://bit.ly/10SovTech

26. http://openid.net/wg/heart/charter/