HIMSS
transforming health through information and technology™

June 2018 Audience Q&A
Blockchain Reset: Seeing through the Hype and Starting down the Path, Part 2

Below is a list of panelist responses to questions that could not be answered within the time allotted the recent presentation "Blockchain Reset: Seeing through the Hype and Starting down the Path, Part 2".

Responses from the following panelists included below:

David Houlding, Principal Healthcare Program Manager, Cloud + Enterprise, Industry Experiences, Microsoft
Mike Jacobs, Senior Distinguished Engineer - Blockchain Evangelist, Optum
Ted Tanner, Co-Founder & CTO, PokitDok
Corey Todaro, Chief Product Officer and Director of Hashed Labs, Hashed Health
Emily Vaughn, Blockchain Product Director, Change Healthcare

Q: How do you overcome the increasing CPU demand where any Blockchain system actually in high use will require CPU and Power that outpaces Moore's Law? Bitcoin is already dramatically impacting the environment with power demand.

David: Large CPU demand from Bitcoin is a consequence of the associated consensus algorithm using PoW (Proof of Work) which requires Bitcoin mining. All of the healthcare use cases we discussed in the webinar panel, and almost all of the healthcare use cases for blockchain that I am aware of, are private consortium blockchains and not public blockchains. Private consortium blockchains have very different consensus algorithms that do not require mining and do not use large amounts of CPU or power.
Ted: Permissioned chains are not using mining. Period. DokChain uses POET (Proof of Elapsed Time).

Q: On a private blockchain, with fewer nodes, what is the risk of a 51% hack? Any concerns?

Emily: On a private network, where we control all the nodes, we can prevent a 51% attack using Kafka consensus mechanism. However, when we scale it to more nodes with trusted partners, Kafka breaks down.
Ted: As stated, the control and access mechanics on a permissioned chain invalidate collusion. Please study the concept of enterprise permissioned chains.

Q: Were there other blockchain frameworks that were assessed for use by Change? It seems like there are so many initiatives - how did Change decide which one to use?

Emily: [Change Healthcare] did evaluate other platforms but chose Hyperledger for this solution due to its modularity and the community behind it - it was the right solution for an enterprise-grade private-to-permissioned roadmap.

Q: Are you worried that using a private blockchain like Hyperledger removes the ability to tokenize a patient's data as well as have a worldwide scalable network from day one?

Emily: [Change Healthcare is] not worried that Fabric doesn't use tokens for network consensus -- we could still build a token-based application on top of Fabric. As we scale the network beyond a private environment, we will likely need a new network model for node operators
Ted: PokitDok has provided a means to create crypto-assets that are ERC20 compliant so you can tokenize any transaction.

Q: What consensus model is being used?

> **Emily:** [Change Healthcare uses] Kafka for the private network - [we] will likely choose another when migrating to permissioned network.
> **Ted:** For DokChain, we are currently using Intel Sawtooth Proof of Elapsed Time (POET) as it is the most efficient. However, that doesn't mean we can't use future methods of Proof Of Stake, Proof Of Existence, etc. as we have already studied and modelled these in our system.

Q: Reduction of dispute resolution processes seems an obvious benefit

> **Ted:** Not sure if this is a question, but, yes, computational governance with provable consensus with autonomous agents obviates the need for dispute resolution.

Q: What data system is actually being used to store data? I often hear Blockchain but none of the ledger systems can store significant data per transaction. In most cases ledger stores a hash and other traditional data systems (SQL, UDB2, Oracle) are there.

> **Ted:** We have found the most flexible and resilient data store for our use in a truly distributed processing system is IPFS (Interplanetary File System). I'm not really sure how SQL or Oracle aids in this process although it can be used as a data source.

Q: Ted Tanner addressed an interesting part "How to make participant wants join" would love to hear more on his view of how to reward those that participate.

> **Ted:** I'm not sure I understand the question. If I understand correctly, it reads as a literal incentive. I get this question all the time. What is the incentive? If you mean a literal subsidized incentive, which appears to be how most of the Health IT industry operates, there is not one. What did Meaningful Use really get us other than several hundred companies that do not want to interact nor have listened to the provider or consumer? The reward to participate is reduced friction between the provider and consumer. The reward is creating an ecosystem that will deliver and be more invisible between the provider and consumer such that generations will prosper. As far as a literal reward, we have an incentive model for entities and consumers to share high quality data within the system thereby creating a much more accurate delivery mechanism. This reward is tokenized - ergo can be monetized.

Q: How will Blockchain technology integrate with wellness and population health?

> **Ted:** We have several hundreds of companies built on top of our Platform as a Service (PaaS), and there is no concept of integration. If you want to build an application on top of us for population health, you get all of the backend mechanics as the service permits. Blockchain allows for a distributed trusted network, which is implicit in Population Health.

Q: Does your infrastructure network support multiple EHR platforms vs. 1 network = 1 EHR application?

> **Emily:** The Intelligent Healthcare Network - Change Healthcare's clearinghouse network today - connects to multiple EHR systems. We cover about 1 in 5 patient records and 2 out of 3 insurance claims.
> **Ted:** We have an API that operates across 55 EMRs. Therefore, once again, the silo of an EMR is one of the reasons Health IT is in its current situation. There will be many chains, and the EMRs will be outside nodes.

HIMSS
transforming health through information and technology™

Q: Can pre-authorizations be near instant with blockchain?

> **Ted:** Yes, it is one of the main use cases that we are working on with DokChain and PokitDok.

Q: How can I receive the white paper for the provider directory pilot when it is published?

> **Mike:** The white paper is planned to be part of a press release, which will have information about getting the white paper.

Q: Is anyone working on or aware of using blockchain-based QR code for patient identification?

> **Ted:** If you saw the PokitDok SDK demo at Distributed Health, then you saw us scan a QR code for the asset with respect to the identity and perform an autonomous auto adjudication with payment in real time. It's already part of the DokChain SDK. Actually, there is a much more frictionless step: use near field communications of the mobile device and check in the patient at the time of service instead of an asset scan.

Q: Are there mechanisms or patterns for revoking access, for example if a participant is determined to be a bad actor, or a patient revokes a consent to share with some provider?

> **Mike:** Revoking access for bad actors is a node-based revocation that varies by tech stack (think white listing). Revoking access to application data like consent of sharing patient data must be managed at the application level.

Q: Blockchain is known to have slower transactions than normal databases. How is this issue addressed, if used in healthcare?

> **Ted:** The health industry predominantly operates on faxes and phone calls with an accounts receivable window of 90-180 days - most systems are well within that throughput and consensus time window.

Q: [There are] many new projects that have hit the coin market that utilizes private blockchains (likely due to HIPPA requirements). How is tokenization, which is generally public (especially in allowing outsiders to invest) reconciled with the use of a private blockchains?

> **Ted:** We address this in detail in our whitepaper that has been published openly for quite some time, and we have made namespace changes to Hyperledger to support tokenization with ERC20 compliance.

Q: Where is a good resource to learn more about consensus algorithms for private identifiable data?

> **Ted:** *Distributed Algorithms* by Wan Fokkink is a good book. Also Jim Gray and Leslie Lamport, "Consensus on Transaction Commit", ACM Transactions on Database Systems (TODS), Volume 31 Issue 1, March 2006, pp. 133-160. The methods that we use for Contextual Relevant Identity Management are explained in our whitepaper.

Q: How do you get to an immutable ledger with multiple blockchain vendors?

> **Ted:** We see promise in the Interledger protocol and Hyperledger Quilt project. The more open the protocol and open source the systems, the better.

Q: Is the concept of cyptoeconomics needed in blockchain in healthcare industry?

> **Ted:** The healthcare industry, at least in the United States of America, is a business as such by definition. So, it's a given that tokenized economies allow for frictionless economics.

Q: I am more of a public blockchain developer and the projects I have worked on cannot store data on the (Ethereum network) we encrypt data with a user's private key and then store it on a decentralized database, [such as the Interplanetary File System] (IPFS). Can private chains store data? If not, how are you storing and encrypting the data on private chains? Is IPFS being used?

> **Ted:** We use IPFS in our system for off chain data. You are not going to store a volumetric 3D Magenetic Resonance Image set on chain.

Q: Is hacking possible in blockchain hyperledger and thus compromising patient data in EHRs?

> **Ted:** We use the Hyperledger Sawtooth architecture utilizing a trusted execution enclave, and the smart contracts are encrypted as well. Of note, in 2016 HIMSS published a report stating that 35-40% of all data in transit and at rest is un-encrypted. Therefore, if anything, building systems that are hashed with each block and providing a secure key mechanism with computationally secure smart contracts is better than what we have with EMRs. Are EMRs actually secure?

Q: How is immutability affected when we say that data does not necessarily need to reside on the blockchain and that the data can be on legacy systems and the blockchain can reference that data?

> **Ted:** We provide smart contracts that synchronize all off and on chain distributed data as a function of consensus.

Q: If the data in the legacy system is changed and all that is on the blockchain is pointers then would immutability of data still be a characteristic?

> **Ted:** No. We provide smart contracts that synchronize all off and on chain distributed data as a function of consensus. The data pointers then are updated as a function of the DLT.

Q: Is blockchain 100% data leak proof?

> **Ted:** If I understand the question correctly, you are speaking of metadata leakage with respect to consensus of identity. Thus, I would say technically "no." However, in a permissioned enterprise chain, we would know what leaked - how, when, and where. That being said, in 2016 HIMSS published a report stating that 35-40% of all data in transit and at rest is un-encrypted. So, if anything, building systems that are hashed with each block and providing a secure key mechanism with computationally secure smart contracts is better than what we currently have.

Q: Where is the patient data saved? Blockchain is not that good on saving great amount of information, or am I wrong?

> **Ted:** We use IPFS that is triple encrypted with the in-transit data encrypted for off-chain data and smart contracts to synchronize the data.

Q: We are facilitating care coordination among patients, caregivers and providers. Can we reasonably deploy blockchain as a method of creating reliable patient-entered data, rectify source discrepancies in that data, and improve patient ID & workflow issues?

> **Ted:** Yes, that is one of the salient aspects.

Q: How [can we] change the mentality for Healthcare organizations to give up the control over their information for [the] better good?

> **Ted:** Great question. This entire process is behavioral not technical. "Their information" is actually the consumers' information. In the future, we hope the consumer is incentivized to provide tokenized data that is completely distributed. A cursory check of any social network will tell you that consumers share health information. However, yes, this is a behavioral issue as there will be disintermediation. There will be several companies that will be disintermediated that operate on a float mechanism or middleware concept.

Q: Could blockchain technology be adapted to carry a payload such as a [Consolidated Clinical Document Architecture] CCDA for healthcare records? Would it be suitably secure?

> **Ted:** The CCDA / PHR would be stored off-chain. Yes, it would be secure.

Q: Is there any benefit of using Hyperledger when there is only one node in whole network?

> **Ted:** If what you are saying that you are using Hyperledger as a master data management deployment model with one node across your internal network, then the answer is "yes."

Q: Do you think using Hyperledger or any other blockchain networks is a good idea for a B2C business model in healthcare industry?

> **Ted:** Yes. Creating a distributed trusted network that allows access to data from a provider-consumer interaction would be good for the industry.

Q: If a patient forgets their password or otherwise loses access to their personal patient information, how would they be able to regain access to their information?

> **Ted:** We have worked on a very novel set of algorithms for identity management called contextually relevant identity management protocol, which allows the access of your data independent of the password or device. If the device is destroyed, we can recover the "key" and/or password relative to that key.

Q: How does a permissioned blockchain eventually become public as it scales?

> **David:** Permissioned blockchains are typically private consortium blockchains where all participating organizations are well known and highly trusted. This type of blockchain could grow in terms of the number of organizations that join the private consortium, integrate with the associated blockchain, and transact data on it. These kinds of blockchains would not automatically transition to a public blockchain. An explicit decision would first have to be taken by the consortium to go public and then there would have to be a technical transition to realize this. Similarly, two blockchain "islands" could merge or join together if a consortium decision was taken to do so. However, transitioning from a private to a public

blockchain, which is wide open for access by any anonymous participant, would be very unlikely for the vast majority of healthcare use cases I have seen for blockchain.

Q: Will patients end up owning and managing their own patient data and provide access to the providers via permission over the blockchain?

David: These could be longer term benefits of blockchain. Improved transparency and patients ability to review and amend data, and manage consent and access to their data are great privacy benefits that blockchain can enhance.