# Blockchain for Healthcare Proposal

Leidos: August 8, 2016

## Introduction

Leidos cybersecurity experts have been observing the use of Blockchain for some time, including its utilization in the highly successful cyber currency BitCoin. We understand this technology thoroughly, and are intrigued by its potential for establishing a measure of peer-to-peer authoritative integrity among an unregulated peer community. In this white paper, we consider how this technology could be used for healthcare applications.

Leidos envisions a flexible blockchain approach that can be applied to many types of healthcare records, integrated through a flexible interface that allows health organizations to take advantage of the security features provided by Blockchain while also supporting the privacy requirements faced in the healthcare industry. Our concept incorporates an innovative approach to mining that mitigates many of the concerns related to the adaptation of Blockchain technology to new domains.

In our consideration, we observe that the true power of Blockchain is for establishing a public, peer-moderated, "ledger" that is resistant to integrity and availability attacks. As such, this technology is *not* directly useful for applications that require confidentiality, although it may be used in support of those applications. Rather, its power is in applications that require *integrity* and to achieve *availability* by avoiding single points of failure. There are two general scenarios that require these properties: the establishment of "trusted" identities, and the protection of "trusted" transactions, such as financial transactions. The key here also is that Blockchain is most useful where "trusted" identities and "trusted" transactions need to be established without requiring a "trusted" central authority acting as the central regulator or broker. Therefore, our proposal will focus on these scenarios.

## Understanding Blockchain in General

Nakomoto provides a solid description of the Blockchain model, and how it solves a number of challenges related to distributed cryptocurrencies. The heart of Blockchain is a shared, distributed "ledger" that is replicated among multiple nodes and broken down into a "chain" of blocks containing transactions between the participants. The architecture of this system is as follows:

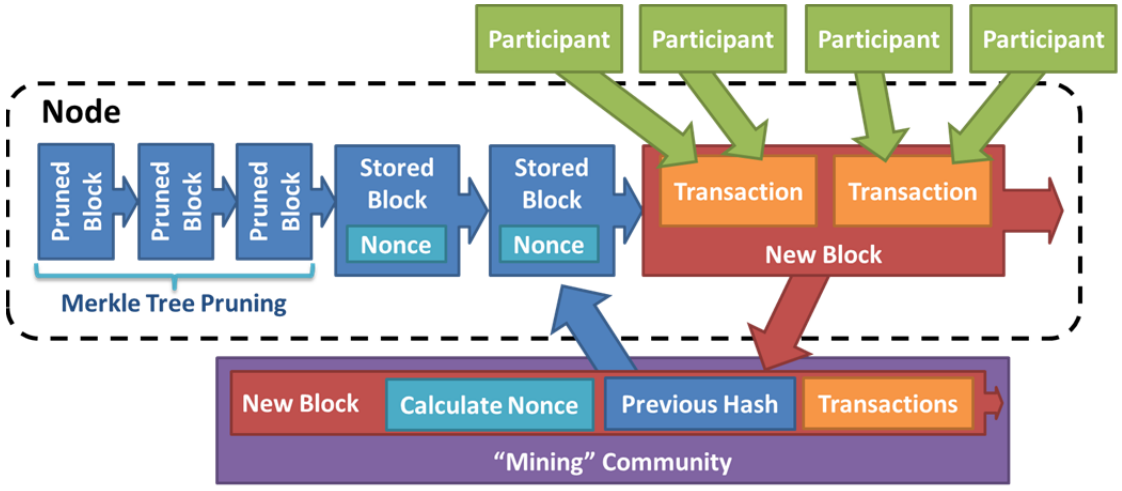


***Figure 1:*** *The Blockchain architecture includes Participants, Nodes, and Miners.*

- **Participants** possess keys that they use to sign transactions between one another. In the case of Bitcoin, these are financial transactions, but any transaction that can be digitally signed can be stored.

- **Nodes** store the distributed "ledger" that contains all transactions. Old transactions that have been superseded are pruned using Merkle Tree Pruning to save space without disturbing the hashes that ensure the integrity of the ledger.
- **Miners** take blocks from the Nodes and attempt to calculate a "Nonce"- (a random piece of information) that creates a hash in the proper, acceptable format. The "winning" hash is then used to cryptographically seal each block. The use of a nonce is designed so it takes a long time and significant computing power to calculate. In the case of Bitcoin, this is approximately 10 minutes using a large-scale distributed computing infrastructure.
- **Participant Keys** are public key cryptography key pairs used to digitally sign transactions. Each participant possesses a private key associated with a digital "wallet," and the corresponding public key is entered into transactions they participate in. Anonymity can be accomplished by sharing no other meta data about the participant beyond their public key, and if the participant operates their own node then their transactions can be very difficult to trace. Conversely, if anonymity is not needed, additional meta data about the participants can be captured and digitally signed in transactions to provide strong identities.
- **Transactions** contain interactions between the participants in the Blockchain. In the case of Bitcoin, transactions represent exchanges of currency, but any type of cryptographically signed activity can be captured, including single-party, dual-party, and multi-party interactions. Transactions are secured using the Participant public keys, providing non-repudiation for the participants while also enabling anonymity if it is desired.
- **Blocks** store transactions in the Blockchain itself. Each block contains one or more transactions between participants in the system. When all of the blocks in the chain are combined, what results is a distributed, public ledger providing high availability and non-repudiation of the transactions contained within. Blocks are linked together cryptographically using two components. First, each block in the chain is "locked" using a hash of the data in the block, along with a "Nonce" calculated by the miners. Second, each block in the chain contains a link to the preceding block and its hash, ensuring the chain cannot be re-ordered to insert or replace blocks.

This architecture creates a chain of blocks constituting a public transaction "ledger." The cryptographic strength of the ledger grows over time, so older transactions become more difficult to modify as additional blocks are added to the chain. This is because any change to an older block requires that all blocks after the changed block be re-calculated as well.

## The Capabilities of Blockchain

Blockchain provides a number of security capabilities that Leidos will extend to the health care community.

- The "mining" process means that for an attacker to introduce fraudulent transactions, the attacker must obtain a huge amount of computing capacity.
- The cryptographic strength of the chain increases over time, making older transactions more difficult to modify as additional blocks are added to the chain.
- The public ledger in the Blockchain provides public disclosure of transactions, as well as non-repudiation of transaction activities.
- Because the ledger is stored on all nodes of the system, there is good resistance to denial of service attacks.
- Because public keys alone are used to identify participants, participants can achieve a level of anonymity in the public ledger, if privacy is desired.
- In the case of BitCoin, the financial model ensures that the exchanges operating nodes and the miners operating computing resources are compensated for the infrastructure they operate.

All of these capabilities are very powerful, but they also bring to light some potential issues. In particular, users must be cautious of the following limitations inherent to the Blockchain approach:

- The public nature of the Blockchain ledger means transaction details that are meant to be kept confidential should not be stored in the Blockchain unencrypted.
- When used for non-financial applications, it is unclear how miners and node operators can be compensated for their efforts and computing power.
- If used within a closed community, it may be easy for a single large participant to bring to bear a plurality of computing capacity that enables them to control the authoritative Blockchain and corresponding ledger.

To be successful, healthcare applications for Blockchain must ensure these limitations are considered and compensated for as necessary.

## Value of Blockchain for Healthcare

Leidos envisions that use of Blockchain's "public ledger" framework to support many diverse purposes across the healthcare industry. Our concept of applying Blockchain to healthcare is especially useful for use cases that require the following characteristics:

- Public disclosure is needed so all participants in the Blockchain are aware of the contents of the Blockchain ledger.
- Privacy is needed so participants in some or all of the transactions in the ledger are anonymized, while other data is publicly disclosed
- High availability and non-repudiation are needed for the public ledger.

At a high level, applications with these characteristics include the following:

1. Delivering "trusted digital identities" that are useful for medical operations and compatible with existing technologies.
2. Establishing a public registry for storing personal and organizational data while protecting privacy.
3. Establishing a public ledger for tracking medical transactions and making the information available to multiple parties.

## Potential Gaps in Blockchain for Healthcare

Leidos has identified three major challenges to unlocking the value of Blockchain within the healthcare industry:

- In a public Blockchain, all transaction data is visible to the public. Healthcare regulations and applications require varying levels of privacy protection, depending on the nature of the data to be protected (PII, PHI, etc.). Therefore, a completely public Blockchain for Healthcare does not make sense and Leidos proposes the creation of a private Blockchain implementation.
- In a public Blockchain, providers of the mining and node infrastructure must be compensated for their efforts. In Bitcoin, this compensation is provided using charges embedded in the Transaction ledger and stored in the Blocks. Since Healthcare is about more than money, levying such fees will be difficult. Therefore, a Healthcare Blockchain may need to be structured as a private community, with participants providing the required infrastructure.
- In a public Blockchain, insertion of fraudulent transactions is guarded against through the voting power of the computing capacity devoted to mining. For an attacker to permanently alter the ledger, they must achieve a plurality of computing power across the Internet. With Bitcoin, this is particularly difficult because a large number of individuals and organizations are compensated for mining. In a closed Healthcare Blockchain, this safeguard may not exist, and it might be easy for a large organization to

achieve a plurality of computing power and control the ledger. Leidos' proposal addresses a partial mitigation to this issue however we realize ongoing research is still required.

## The Healthcare Community of Interest

Potential Blockchain use cases for Healthcare will revolve around the interactions between five major sets of parties: Individuals, Providers, Payers, Regulators, and Vendors:

- **Individuals** include patients, family members, caregivers, and their advocating organizations, such as corporations, advocates, mediators, and attorneys.
- **Providers** include hospitals, clinics, doctors, specialists, therapists, pharmacists, other healthcare professionals, and the organizations they operate under.
- **Payers** include governments, insurance companies, and individuals involved in paying for healthcare services.
- **Regulators** include Local, State, and Federal government regulators charged with overseeing medical service delivery, quality, and billing.
- **Vendors** provide supporting technology and services to the other parties, to enable effective delivery of medical services, billing, and other related capabilities.


***Figure 2:*** *Individuals, Providers, Payers, Regulators, and Vendors are the primary potential participants in a Healthcare Blockchain.*

## Proposed Blockchain for Healthcare Architecture

To overcome the abovementioned challenges, we propose establishing one or more "Blockchain for Healthcare" community implementations. These implementations would be "closed Blockchain communities," and would have the following characteristics.

1. These would be private Blockchains, with Nodes operated by participants in the community. To take advantage of the decentralized nature of Blockchain, individuals and regulators would not operate nodes. All business entities with a financial stake would operate nodes, including Providers, Payers, and Vendors. Each community would have the following properties:
    a. All nodes in the community are aware of all other nodes in the community. New nodes may request to be added to the community by communicating with an existing node, but are not enabled until all existing nodes have acknowledged the new node and added it to their copy of the community database.
    b. The process for adding and removing nodes would be configurable on a per-community basis, with all nodes in the community adhering to a common policy. We envision the policy may be one of the following methods:

i. One node may act as a "gatekeeper" and be responsible for authorizing the addition and removal of nodes. This may be appropriate when the Blockchain is operated on behalf of an industry association with central governance.
ii. Node operators may be required to "vote" to accept additions or removals, with changes requiring approval by a majority of nodes before they are committed.
iii. A single node may "sponsor" an addition or removal, with "approval" from one or more other nodes required to mitigate unilateral action.
iv. Nodes may add or remove themselves at will, and operate as an open community.

The key to this implementation would be that the community management process in the Blockchain system align with how the corresponding community of people and organizations operates.

c. The community database is itself stored as a Blockchain database. New nodes are not permitted to participate in the Blockchain until they have been added to the community Blockchain and the block containing their addition has been sealed and accepted by the existing nodes.
d. The community database is published to the operators of each node, and is subject to periodic manual audit. This to protect against organizations attempting to control the community by adding enough nodes to assume a plurality.

2. For simplicity, Blockchain communities would be limited to one or more applications. We would not try to establish a single community to meet all possible needs. We envision these communities might include the following:
    a. **Providers** and **Payers** might establish a community to track billing information, with **Individuals** able to read transactions that pertain to them, and **Regulators** able to read transactions for oversight purposes.
    b. **Providers** and **Vendors** might establish a community to allow **Vendors** to track and authenticate to their technologies connected to **Provider** facility networks.
    c. **Regulators** might establish a community to allow them to interoperate securely with regulated entities, including **Providers**, **Payers**, and **Vendors**.
    d. **Individuals**, **Providers**, and **Payers** might establish a community to allow **Individuals** to maintain their personal information and make it available to **Providers** and **Payers**.
    e. **Providers** and **Regulators** might establish a community to track drug prescriptions and to prevent overprescribing and to track dangerous regulated drugs like narcotics.
    f. **All Parties** might establish a community for issuing and maintaining secure digital identities, similar to digital certificates, that might be usable for identifying parties over untrusted networks and authenticating between digital systems.
3. To track transactions within these communities, we would establish a generalized and extensible transaction schema. This schema would include the following properties:
    a. The schema would be defined using XML, so attributes and tags are defined using an intuitive format familiar to many computer scientists.
    b. The schema would be extensible. Transactions and transaction blocks would include references to the schema used to create them, so readers of the blocks would be able to properly decode the blocks and the transactions contained within them.
    c. The schema would include built-in compression of transaction blocks after to the cryptographic signing of the blocks, to conserve space. This compression would be performed after the signing, to enable later Merkle Tree pruning within the blocks.
    d. The schema would include an option for transaction parameters to be stored encrypted. Encrypted transactions and transaction parameters would be encrypted using the public keys of one or more participants, so those participants could read the data stored therein.

    e. The schema would allow for transaction parameters to include references to data stored at one or more of the transaction participants, further enabling the handling of transactions containing private, regulated, or access-controlled data.
    f. The schema would identify participants in transactions using only their public keys. To protect patient privacy, additional parameters identifying participants would be optional.
4. As mentioned above, transactions containing confidential data can be stored in the Blockchain encrypted. This encryption would be performed using the public keys of the transaction participants, along with the public keys of any desired third parties, such as patients or payers. Therefore, any of the participants can decrypt the transaction details, without necessarily compromising their privacy.
5. To solve the miner compensation problem, each node in the network would also be a mining node. Since nodes are operated by participants in the community – Providers, Payers, and Vendors – these participants would also be the ones doing the mining. Rather than using a plurality of computing power to determine the authoritative sources of new blocks, we propose new blocks be calculated as follows:
    a. All nodes would keep track of a database containing all nodes in the community, as referenced by their DNS names and accompanying organization description string. This database would be disclosed to all participants, and subject to peer audit. This ensures that participants who attempt to add unnecessary nodes are disclosed.
    b. Each node would transmit all transactions it receives to all other nodes, so each connected and online node would have a copy of all transactions.
    c. At the end of a preset period – we propose once an hour, although it could be longer or shorter – all nodes would wait a preset time for transactions to synchronize across the network, and each node would begin working on all of the transactions that occurred within the previous period.
    d. Each node would then calculate the Nonce for its block independently, and create its own copy of the "sealed" block and disseminate that block to the rest of the network.
    e. To protect against tampering, each node would have a public-private key pair it uses to digitally sign all blocks it calculates. This protects its blocks from tampering, as they are disseminated across the community. Each node that receives blocks from the other nodes would verify the blocks' signatures before accepting them.
    f. As each node receives copies of the block from the rest of the community, it would compare those copies with each other and to its own block. For a block to be considered "official" the following properties must be satisfied:
        i. Blocks must have a valid digital signature representing the node that calculated the block, and only one block will be accepted from each node. If multiple different copies of a block are received from a given node, the latest received block is considered.
        ii. Blocks must be received from at least 80% of the community, as calculated against the community database.
        iii. Blocks from at least 60% of the community must be identical. This "majority rule" block would then be accepted as the "official" version of the block for archive.
    g. Nodes will not commit a new block until the above properties are satisfied. If a block is overdue, the node will generate an error calling for human intervention.
6. As described above, the block generation process is designed to fail and require human intervention, rather than commit fraudulent transactions. The two safeguards are as follows:
    a. The community database is maintained transparently, and operators are required to periodically audit the database to ensure each participant only operates a single node.
    b. When calculating new blocks, the community will generate an error and stop calculating if 60% of the community cannot agree on the content of a new block.
7. To integrate with existing IT infrastructure, the reference implementation would include two functions for integration into existing applications:

a. A QUERY function would connect with a node and permit queries of the node's copy of the transaction database, using the accompanying schema.
b. A TRANSACTION function would connect with a node and permit the generation of new transactions using the public keys of the participating parties.

We believe this architecture provides a method for operating a community Blockchain that provides the power of Blockchain, while also addressing its limitations when used in a community application.

## Healthcare Use Cases for Blockchain

Some of the possible scenarios where the proposed community Blockchain might be useful include the following:

1. Collecting patient personal information (name, address, health insurance) and making it available to providers while protecting against fraud.
2. Tracking patient medical transactions for the purpose of financial reimbursement.
3. Establishing digital identities for patients for online transactions.
4. Tracking treatments to prevent double treatments.
5. Tracking drug prescription issuances to prevent double prescription.
6. Establishing digital identities for medical devices.

These possible scenarios include a large number of possible types of transactions and use cases, all of which could be stored in private community Blockchains used by the healthcare community. Some of these possible interactions are as follows:

- **Individuals**, **Providers**, and **Payers** all need secure online identities that are resistant to fraud, abuse, and counterfeiting, and which provide confidentiality and non-repudiation online.
- **Individuals** obtain medical services from **Providers**, which are then billed to **Payers**. This is the simplest transaction, although few medical transactions are actually this simple.
- **Individuals** receive prescriptions from a **Providing Doctor**, which must then be handed off to a **Providing Pharmacy**, and then billed to a **Payer**.
- **Individual** medical treatments must then be divided up and billed to multiple **Payers**, including back to the **Individual** themselves. The total amount of the bill must be tracked against payments, to ensure payment is received in full from all involved parties. This gets particularly interesting when portions of the bill are contested by one or more **Payers**.
- **Individuals** receive complex medical care—such as in the case of a surgery—that involves a multitude of **Providers** all tracking services that must be correlated for payment according to an equal multitude of **Payer** payment and billing policies.
- **Individuals** must update their personal information with all of the interested **Providers** and **Payers**, such as when they move, change phone numbers, or change payment methods.
- **Individuals** must update payment methods and **Payer** prioritization in response to changes of job, change of status (marriage, divorce, birth, death), retirement, or other life events.
- **Payers** change their business status, such as entering or departing a government-operated healthcare exchange, or in relation to company-sponsored healthcare coverage.
- **Payers** wish to challenge portions of a bill, which must then be tracked back to the underlying **Provider** services and further explained or justified, often with input from the **Individual** involved.
- **Individuals** wish to have transparent traceability from their medical procedures back to the bills they receive from **Providers**, and which are partially paid by **Payers**.
- **Payers** and **Regulators** wish to avoid fraud caused by double-billing.
- **Regulators** and law enforcement are concerned about inappropriate prescription of dangerous drugs, such as narcotics.

- **Regulators** which to observe, track, and audit the activities of regulated **Providers** and **Payers**.
- **Vendors** wish to monitor their technologies within **Provider** environments.

In all of these use cases, there is a need for transactions to be stored among multiple parties with non-repudiation of the activities, along with various needs for privacy and high availability.

## Blockchain Effectiveness in the "Real World"

We believe the proposed approach is implementable and will address many of the "Real World" concerns with practical use of Blockchain technology outside of Bitcoin. Specifically, our approach includes the following properties:

- Privacy can be ensured by only identifying individuals using their public keys, and by protecting other sensitive data in the Blockchain using a combination of encrypted parameters and links to data stored elsewhere.
- Individual identities can be managed using key pairs issued by Payers and Providers, and stored on smart cards or similar devices. Individual key pairs can be used within an application community, and can also be ported from one community to another. This aligns well with real-world implementations, such as where a patient might use a Medicate ID card for their treatments.
- Security is based on the Nodes all working together as a community. To compromise the security of the community, an attacker would have to take control of at least 20% of the nodes to cause a quorum failure, 40% of the nodes to cause a consensus failure, 60% of nodes to create fraudulent transactions, and 80% of nodes to control the quorum. Since the community would fail at the 20% mark and stop committing new transactions, we believe this provides significant safeguards against malicious activity and ensures the system fails before it can be manipulated for fraud.
- Because of the modified voting mechanism for committing transactions, this approach would not have the performance problems associated with performing "mining" in a traditional Blockchain. Also, it would address the challenge of compensating miners.
- Since each participant in a given community operates a node, and the computing requirements of a node are relatively modest, the cost of this approach should be relatively low. With that said, there are many unknowns to this factor, including the size of the collective database and the number of possible nodes.

We believe the risk of the proposed approach is relatively low. With that said, more research will be necessary. Areas where we would like to continue researching include the following:

1. Cryptographically analyze the proposed approach to ensure that all activities are cryptographically protected as planned, as well as to analyze how it might fail in case the cryptography is defeated or shows serious vulnerabilities.
2. Establish a "reference implementation" that implements the proposed design in a production environment, allows for integration with existing health care applications, and allows for further testing.
3. Verify the performance of the reference implementation, with regard to the following scaling factors:
    a. How performance changes as nodes are added to the community
    b. How performance changes as the database grows and blocks are pruned
    c. How performance changes as the number of transactions in a block grows
4. Perform threat modeling and "Red Team" the reference implementation to investigate what an attacker could do from the following positions:
    a. When in possession of compromised user credentials
    b. When in possession of a community node running the reference software
    c. When in possession of a community node running customized software
    d. When in possession of multiple nodes in the community.

e. When trying to add a fraudulent node to the community.

Our design should fail before it accepts fraudulent transactions, but that behavior should be verified.

By performing this follow-on research, we will be able to verify the merits of this approach, and validate the concept of a Private Blockchain for the Healthcare community.

## Linkage to the Nationwide Interoperability Roadmap

The Nationwide Interoperability Roadmap describes the challenge of interoperability between three parties, Payers, Providers, and Individuals, with regard to ten Principles of Interoperability. Looking at these principles in sequence with regard to the proposed approach, we can see the following:

1. **Build upon existing health IT infrastructure:** The proposed approach should integrate easily with existing IT infrastructure. Existing applications could be easily modified to use the TRANSACTION and QUERY functions to generate and validate transactions against the community Blockchain.
2. **Maintain modularity:** The proposed approach includes several levels of modularity. Different Blockchain communities can be used to support different applications, including overlapping communities where a given organization might participate in multiple Blockchains simultaneously to support different applications. The extensible schema means the same reference code can support multiple applications, including multiple applications within a single Blockchain. Finally, the application code can be a single library that connects to different schemas, different nodes, and different Blockchains to support separate applications.
3. **One size does not fit all:** The proposed approach can support a variety of applications and communities of interest, without requiring a single monolithic "one size" solution. Organizations can operate multiple nodes to support multiple applications, and can operate different versions of the software and different schemas as needed.
4. **Consider the current environment and support multiple levels of advancement:** Our strategy is to develop a flexible software platform that can then evolve quickly to support operational needs. By operating private communities, we provide modularity and enable integration to be done on a case-by-case basis while allowing multiple implementations, at different levels of advancement, to coexist and evolve separately side-by-side.
5. **Empower individuals:** Our model should be application-driven, so that individuals and organizations participate in the community Blockchains that enable the applications they desire. This in turn supports the empowerment of individuals to utilize the technology they desire to achieve their healthcare goals, whether it is online access to their information or conducting healthcare transactions online.
6. **Simplify:** We believe that an advantage of our proposed approach is to embed the cryptography, non-repudiation, and high availability of secure transactions within the Blockchain, rather than requiring such functions to be performed by the applications themselves. By giving applications access to such a highly-available and cryptographically secure solution, we believe it solves many problems of collective collaboration, without increasing complexity of the applications.
7. **Protect privacy and security in all aspects of interoperability:** The proposed approach provides significant privacy and security by using a private community, but then increases privacy and security through the use of encrypted transactions and embedded reference data permitting transactions to include data that is separated, encrypted, and access controlled. These features provide additional privacy and security than the Blockchain implementation used in Bitcoin, and we believe will be sufficient to utilize Blockchain capabilities within the framework of existing privacy and security regulations.
8. **Leverage the market:** Our objective with this paper is to establish a Blockchain capability that can be used by private innovators to enable desired applications. Our intent is to let these applications, implemented by technology vendors and solution providers, drive the adoption of this technology, just as web standards and technologies have enabled the market to deliver revolutionary new IT and

communication services. We have also sought to reduce the amount of cross-vendor collaboration required to implement this proposed approach, further enabling market adoption and promotion.

9. **Focus on value:** Our approach as described in this paper is to present a flexible Blockchain architecture that can enable multiple applications both separately on separate infrastructures, and side-by-side on shared infrastructures. By reducing the computing requirements for Blockchain "mining," we dramatically reduce the infrastructure costs compared to those required by Bitcoin, increasing value for Blockchain participants and technology providers.
10. **Scalability and universal access:** Based upon our research, the proposed approach should enable scalability and access through two characteristics. By focusing on smaller communities serving specific applications with correspondingly smaller transactions and databases, we address the issue of a single "monolithic" Blockchain trying to support all applications simultaneously. By establishing an open, extensible schema for community Blockchains, we also enable the extension of the Blockchain to support additional applications and communities over time. By permitting portable and transferrable credentials for individuals, we hope to enable widespread access through existing identity capabilities such as PIV ID badges and EMV credit cards.

## Conclusion and Recommendations

In this paper, we have endeavored to address a key challenge with regard to using Blockchain for healthcare, which is the economic model behind the "mining" process. This is hardly the only challenge in the way of using Blockchain for healthcare, as every component of the architecture must be analyzed with regard to its extended lifecycle:

- What happens when organizations upgrade their technology?
- What happens when organizations merge or divest?
- What happens when individuals lose their identity cards?
- What happens when cryptographic keys are lost?
- What happens when keys are compromised and transactions must be re-keyed?
- What happens when the Blockchain's cryptography is rendered obsolete?
- What about quantum cryptography?

These and many other questions come to mind as one thinks about this possibility. A 'perfect' solution may not actually be possible, but as they say, "Let's not let 'perfect' stand in the way of 'good enough.'" On the basis of our research, we believe that Community Blockchains have sufficient potential to warrant further research, establishment of a reference implementation, and cybersecurity, operational, and performance testing. Using these techniques, we may be able to establish a new tool that IT professionals can use to tackle the challenges of the Nationwide Interoperability Roadmap for Healthcare.

## References


1. Allen, Christopher et al: *Decentralized Public Key Infrastructure: A White Paper from Rebooting the Web of Trust*. Downloaded on 8/5/2016 from www.weboftrust.info/downloads/dpki.pdf.
2. Axon, Louise: *Privacy-awareness in Blockchain-based PKI.* University of Oxford Centre for Doctoral Training in Cyber Security. Downloaded on 8/5/2016.
3. Crosby, Michael, et al: *Blockchain Technology: Beyond Bitcoin.* Sutardja Center for Entrepreneurship & Technology, UC Berkeley. Downloaded on 8/5/2016 from http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.
4. Fromknecht, Conner, et al: *CertCoin: A NameCoin Based Decentralized Authentication System.* MIT, May 14, 2014. Downloaded on 8/5/2016 from https://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf.
5. Fromknecht, Conner, et al: *A Decentralized Public Key Infrastructure with Identity Retention.* November 11, 2014. Downloaded on 8/5/2016 from https://eprint.iacr.org/2014/803.pdf.
6. *Gcoin: Running a Private Blockchain (Web Page).* Downloaded on 8/5/2016 from https://github.com/OpenNetworking/gcoin-community/wiki/Running-a-private-blockchain.
7. Johnson, Amanda: *Why NameCoin Didn't Take Off: A Cautionary Tale (Article).* The Cointelegraph, May 1, 2015. Downloaded on 8/5/2016 from https://cointelegraph.com/news/why-namecoin-didnt-take-off-a-cautionary-tale.
8. Kawachi, Akinori, et al: *Computational Indistinguishability between Quantum States and Its Cryptographic Application.* MIT, Mar 12, 2011. Downloaded on 8/5/2016 from http://arxiv.org/pdf/quant-ph/0403069v6.pdf.
9. Nakomoto, Satoshi: *Bitcoin: A Peer-to-Peer Electronic Cash System*. Downloaded on 8/5/2016 from https://bitcoin.org/bitcoin.pdf.
10. Pearl, Sean: *Distributed Public Key Infrastructure via the Blockchain (Presentation).* Rochester Institute of Technology. Downloaded on 8/5/2016 from https://people.rit.edu/smp1697/CSCI762/BlockchainPKI.pdf.
11. Troy, Sue. *Blockchain Use Cases, Private vs. Public Debate Engross Community (Article).* TechTarget. Downloaded on 8/5/2016 from http://searchcio.techtarget.com/feature/Blockchain-use-cases-private-vs-public-debate-engross-community.