Co-Creation of Trust for Healthcare: The Cryptocitizen Framework for Interoperability with Blockchain

Research Proposal · July 2016

DOI: 10.13140/RG.2.1.1545.4963

2 authors:

Peter B. Nichol

Quinnipiac University

2 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Jeff Brandt

BlackStar Lab

1 PUBLICATION **0** CITATIONS

SEE PROFILE

Co-Creation of Trust for Healthcare: The Cryptocitizen Framework for Interoperability with Blockchain

Full Paper

Peter B. Nichol, PMP, CSSMBB, CMPI, CQM, CSM, SA, SP
Digital and Innovation Expert
Managing Director
Oroca Innovations
peter.nichol@orocainnovations.com

Jeff Brandt, BSCS
Post Graduate Biomedical Informatics
Chief Architect BlackStar Lab
mHealth Security Expert
OHSU School of Medicine
jeffrey.l.brandt2013@alumni.ohsu.edu

***Abstract* — The aim of this paper is to integrate the concept of co-creation of trust for healthcare and propose applications of blockchain to positively impact aspects of healthcare interoperability. The focus of the paper is on blockchain health ecosystems and the patient-centric interactions that underpin the co-creation of trust, balancing the pluralistic morality of identity. The co-creation of trust for healthcare framework is divided into four concepts applied to healthcare based on the underlying theoretical foundation – blockchain is a database and technology that facilitates an exchange of value within a trustless network, without intermediaries. These conceptualized propositions suggest that co-creation of trust ecosystems have a direct positive impact on patient satisfaction, fraud, healthcare outcomes, and reduce the security risks associated with interoperability. This paper contributes to the literature on co-creation of trust within healthcare ecosystems leveraging blockchain.**

***Keywords*—** *Co-Creation of Trust, Healthcare, Interoperability, Blockchain, Trust, Digital Ledger, Digital Ecosystems, Platforms, Non-Reputation Systems, and Self-Sovereignty.*

I. INTRODUCTION

Individualized care is what we mean when we speak of "patient" or "health." The world is suspicious of individualism, magnified in healthcare. Prevention, telemedicine, and wellness each address healthcare at an arm's length. The future of healthcare will be person-centric care and will leverage patient identities to be portable as a passport.

Person-centric and patient-centric care touches you, the individual. The symmetric democratization balances the knowledge-driven power of medicine as power shifts from the doctor to the patient. Personal health is about more than reporting and the analytics of care variability. Person-centric care stems from destructing the vision of the masses and creating concrete cures that change individual lives today. Erecting power from family, friends, and communities to find solutions for our healthcare problems. Communities are support groups for comforting the sick. What if tomorrow they were enablers for the cures? How society views personal health, must change. There is no such thing as a common disease. Rethinking N-of-1 and M2M (machine-to-machine), might offer insights into new analytical topologies that will be the new platforms for tomorrow's cures. We must move from philosophical discussions to making impacts – together we can find cures.

Blockchain can unlock barriers to identifying schemes for personal health and chronic illness management, driven by the conditional access provided by the patient. The symmetric democratization of healthcare will give patients back control. Health is personal and must be individualized. Forming communities to leverage the demand-side economies of scale increases the value as more patients are impacted and become absorbed into a community to find a cure. How can society extend trust to find cures? The Internet is a trustless medium and every day we need to rely on trust in a trustless world. We currently use many platforms in attempt to facilitate trust. However, the frequency of healthcare breaches continues to rise and organizations do not have the skilled manpower to guarantee a secure system. As a result, reputations are tarnished, and trust continues to dwindle. Blockchain is not necessarily a "trustless architecture," but it does offer "risk-minimized" solutions.

User facing applications, purchase decisions, and infrastructure never have aligned for healthcare. The patient is still waiting and the experience of care is disjointed. Ultimately, the seamless integration of health has yet to be fully discovered. Interoperability, security, audibility, cost-efficiency, real-time, and agile enrollments, public transparency, and guaranteed continuity (removal of the central operator) are areas where blockchain can advance the ecosystem of health.[1]

II. HOW DOES BLOCKCHAIN HAVE THE POTENTIAL TO CHANGE THE WORLD OF HEALTHCARE

In this paper, we examine the co-creation of trust for healthcare to build value; an ecosystem of interoperable components built on top of a trust layered platform to create

[1] Nichol, P. B. Person-centric healthcare amplified by blockchain. (2016). Retrieved from http://www.cio.com/article/3041641/health/person-centric-healthcare-amplified-by-blockchain.html

entirely new opportunities for patient participation. Next, we provide four propositions on co-created trust systems for healthcare utilizing blockchain technologies, which are followed by the research propositions, implications, limitations, and our conclusion.

Six foundational characteristics make up blockchain technology:

1. Distributed – across all the peers participating in the network.
2. Decentralized – every full node has a copy of the block chain.
3. Public – the actors in blockchain transactions are hidden, but everyone can see all transactions.
4. Time-stamped – the date and time of all transactions are recorded in plain view.
5. Persistent – because of consensus and the digital record, blockchain transactions can't catch fire, be misplaced, or become damaged by water.
6. Non-reputation – confirms that the data sent by a specific sender is sent in a manner that the sender is unable to deny having sent the data (authenticity of data creation and integrity of data unmanipulated in transit).

Blockchain records will last over the long haul.[2]

III. ONC 10-YEAR VISION TO OBTAIN INTEROPERABILITY

The Office of the National Coordinator for Health Information Technology (ONC) devised a ten-year plan to develop and adopt a healthcare interoperability infrastructure. Blockchain ecosystems can both provide the envisioned infrastructure through open source frameworks to further reduce cost and facilitate improved access to interoperability.

1. Build upon the Existing Health Information Technology (IT) Infrastructure
2. One Size Does Not Fit All
3. Empowering Individuals
4. Leverage the Market
5. Simplicity
6. Maintain Modularity
7. Support Multiple Levels of Advancement
8. Focus on Value
9. Protect Privacy and Security Interoperability

IV. CO-CREATION OF TRUST

Blockchain is much more than cryptocurrency and the benefits of blockchain will extend well beyond the financial markets into healthcare.

What is a blockchain? Blockchain is a series of connected machines for creating trust.[3]

While we know Bitcoin and Ethereum are popular blockchains there are alternatives such as Billon (regulated "cryptocash" blockchain solution as digital cash for governmental fiat currencies), Hasq (blockchain based on hash functions without public key cryptography implemented in TokenSwap), LaZooz (decentralized real-time ride sharing), Mastercoin (metaprotocol with the ability to process various transactions and sub-currencies), Namecoin (Digital currency that can store data within a chain), Nxt (cryptocurrency financial platform that uses proof of stake to reach consensus for transactions), Peercoin (cryptocurrency-based token incorporating proof of stake in its consensus model, Swarm and Koinify (decentralized crowdfunding), and Synereo (synchronous and asynchronous communications), among others.[4] Each blockchain technology presents advantages depending on fitness-for-use.

Blockchain technologies address the previous legitimate concerns of security, scalability, and privacy of electronic health records. Below is a simple example of how blockchain can be applied to healthcare work in practice.

1. Patient: The patient is provided a code (private key, cryptographic or distributed hash) and an address that provides the codes to unlock their patient data. While the patient data is not stored in the blockchain, the blockchain provides the authentication or required hashes (multi-signatures, also referred to as multi-sigs) used to enable access (identification and authentication) to the requested data.
2. Provider: Contributors to patients' medical records (e.g., providers) are provided a separate universal signature (codes, hashes, or multi-sigs). The provider's hash(s) when combined with the patient's hash establishes the required authentication to unlock the patient's data.
3. Profile: The patient defines in their profile, the access rules required to unlock their medical records.
4. Access: If the patient defines 2-of-2 codes, then two separate computer machines (the distributed hash tables (DHT) would have to be compromised to gain unauthorized access to the data. In this case, establishing unauthorized privileged access becomes very difficult when the machine types differ, operating systems differ, and they are hosted on independent hosting providers.
5. Audit: A non-reputable audit trail is inherently provided by blockchain. Hash codes of the data are provided and backward referencing "links" illustrate a "chain-of-custody."
6. Non-repudiation: Hash algorithms and public key infrastructure (PKI) guarantees the records' validity, and that a document was authentically signed and certified.

Why is this approach more secure than how medical records are stored today? In the cases of the Office of Personnel

[2] Nichol, P. B. How CIOs explain blockchain to their CFO. (2016). Retrieved July 11, 2016, from http://www.cio.com/article/3072470/healthcare/how-cios-explain-blockchain-to-their-cfo.html

[3] Economist. The promise of the blockchain: The trust machine. (2015). Retrieved from http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

[4] Mougayar, W. Understanding the blockchain - O'Reilly Radar. (2015). Retrieved from http://radar.oreilly.com/2015/01/understanding-the-blockchain.html

Management (21.5 million initially and another 4.2 million, loss of personnel data), Anthem (80 million patient and employee records), and the Army National Guard (850,000 SSN and home addresses of current and former National Guard members) only one computer was compromised for each of these large-scale breaches. Would these data breaches have occurred if two separate computers needed to be compromised to gain access? How about five computers or 100 computers each in different places across the world?[5]

Today blockchain has what is called, M-of-N multi-signatures (multi-sigs), meaning multi-signatures are required to establish the authentication required to unlock data (likely stored in the cloud). The M-of-N multi-sig means that 'N' computers would all be required (multiple computers hashes combined) to decrypt the code, e.g., providing the authentication to access that patient's medical records. Elaborating on the concept of multi-sigs, an M-of-5 means that five machines would have to be compromised, each with a separately controlled code or hash. There are also other variants, for example, 2-of-3 multi-sig, which means not only would two separate codes be required, but also the patient data could still be unlocked even if only two of the three keys were available. For example, if the three keys were held by a patient's physician, spouse, and a neighbor, then two of the three keys would be needed to unlock the data (typically used for emergencies involving life and death situations).[6]

V. CONDITIONAL PRIVACY AND ELECTRONIC MEDICAL RECORDS

Privacy is a major concern – until it isn't. For example, if you ask a patient if they would like to share their full personal health history including blood type, all previous procedures, and life habits with providers they likely will be quick to say no. If you asked the patient a similar question if their heart rate went below 40 beats per minute (say in an ambulance), then would they share it? They will be quick to exclaim, 'of course!' Access and consent to medical information is a conditional decision and determined based on environmental context. Today electronic health record (EHR) systems have a difficult time, factoring in conditional consent. Often a patient authorizes either full access to their medical records (all in) or no access. This model doesn't meet patient needs and will evolve with time.

The beauty of blockchain technology, applied to healthcare, is a centralized platform that decentralizes health data (medical records) increasing security of sensitive information. A patient can now use their own signature, combined with that of a hospital signature to unlock data to provide more secure access to medical information for use in treatment. The patient by using their profile has full control of their medical information and can select the information to be shared and viewed by providers or doctors. This model lifts the costly burden of maintaining patients' medical histories away from the hospitals: eventually, cost savings will make it full cycle back to the patient receiving care.

Applying blockchain technology to healthcare will solve the challenge of electronic health records interoperability. Not solved at a county, state, or national level but addressing global electronic health record interoperability. Saying global electronic health records aloud almost sounds crazy; a foreign concept, which should be founded by the Defense Advanced Research Projects Agency (DARPA) of healthcare. That's because global electronic health records, until today, were a dream we only hoped our children's children could solve.

Exploring a practical example makes this experience more real. I'd like to introduce you to Diane. Diane is married, in her mid-50s, works hard and enjoys life when she can break away from work. While on the way to work, Diane felt a bit lightheaded, but after her workout that was often the case. She didn't think any more about it. After she had arrived at the office, she collapsed. Co-workers scrambled to call 911, EMTs arrived and scanned her PatientChainID, Diane, similar to most patients had a profile setup previously. The profile Diane had set up, with the help from her primary care doctor, included rules and identified family members that could approve access to her health records in the case of an emergency. Diane had three family members listed, including her husband, Jake.

The EMT announced and requested access to Diane's medical records on the PatientChain Network. Within minutes, Jake had verified access, and the EMT was able to access Diane's medical records. The EMTChainID, the HospitalChainID, when combined with Diane's PatientChainID (authorized by Jake), unlocked Diane's medical record, which enabled the EMTs to provide more specific care, considering her pre-existing conditions. Diane was diagnosed with syncope (pronounced SIN-ko-pee), which is defined as a sudden, brief loss of consciousness and posture caused by decreased blood flow to the brain. She fainted due to low blood sugar. According to WebMD, fainting is a common problem, accounting for 3% of emergency room visits and 6% of hospital admissions. Diane was held for the day and released that evening. A month later, Diane reviewed her profile and she removed the hospital and the EMT as that access was no longer required. Diane had an electronic health record that was accessible on a cloud-based network, globally, by any payer and any provider after authorization was provided. (Diane, of course, is imaginary and now safe).[7]

VI. BLOCKCHAIN TRUST FRAMEWORK FOR HEALTHCARE

To conceptualize the different types of trust ecosystems, we draw on two theoretical foundations: consensus and cryptocitizen.

Discovered by the Portuguese in 1527 and lying about nine degrees north of the equator the 39 square mile island of Yap, is the most western of the Caroline Islands part of the Federated States of Micronesia located in the Pacific Ocean. William Henry Furness visited the island in 1903 and wrote about the island's stone money in his book titled, *The Island of Stone Money UAP of The Carolines*, published in 1910. The Yapese did not use the money; their medium of exchange was called fei. These large 'coins' were stone wheels ranging from one foot to twelve feet, with a hole in the center, where a pole could be inserted for transportation. The rai stones could weigh up to 8,800 lbs. As a

[5] Nichol, P. B. Blockchain Technology: The Solution for Healthcare Interoperability. (2015). Retrieved from https://www.linkedin.com/pulse/blockchain-technology-solution-healthcare-peter-b-nichol

[6] Nichol, P. B. Blockchain Technology: The Solution for Healthcare Interoperability. (2015). Retrieved from https://www.linkedin.com/pulse/blockchain-technology-solution-healthcare-peter-b-nichol

[7] Ibid.

result, it was not always practical to transfer the stone physically from the seller to the buyer for payment. Therefore, the community would communicate at the council square in the center of the village where all the chiefs met when discussing the affairs of the tribe. Here it would be agreed that a transfer was being made from family A to family B. Additionally, because of the weight of the rai stones, typically eight strong men were needed to move the stones, in a sense, building community consensus for the ownership transfer.

This form of community consensus ensured that ownership was effectively administered. To our mutual dismay, the modern and official currency of Micronesia is the US dollar, and rai stones have evolved into a national symbol. This example demonstrates trust through consensus, a similar model embedded within blockchain technologies.

The cryptocitizen a concept of societal shared trust, where citizens have a new relationship with authority reducing government involvement in decentralization – availability of government services versus citizens being directly governed. These foundations of health are mapped to the Office of the National Coordinator for Health Information Technology's vision for interoperability described in the publication, *Connecting Health and Care for the Nation a Shared Nationwide Interoperability Roadmap*.

Today	**Cryptocitizen with blockchain**	**ONC Achieving Interoperability Roadmap**
Fragmented Ecosystem	Modular Architecture	Built Upon the Existing Health IT Infrastructure
Good for One Patient, Good for All	Patient-Centricity and Patient Controlled	One Size Doesn't Fit All
Central Ownership	Consumptive collaboration	Empowering Individuals
Legacy Technology Layers	Leverage Foundational Technology Enabling Better Care	Leverage the Market
Complex Data Orchestration	Immediately Verifiable Data	Simplicity
Payer and Provider Controlled Access	Conditional Access to Healthcare data	Maintain Modularity
Strained Integration Points, Little Device Interop.	Interoperability for Devices, Records, Labs, Billing – Any Transaction	Consider the Current Environment and Support Multiple Levels of Advancement
Aggregate, disparate systems	Verifiable, Immutable authenticity, open source	Focus on value
Central Authority	Distributed Immutability	Protect privacy and security in all aspects of interoperability

Table 1. ONC Interoperability Alignment and Cryptocitizen with Blockchain Versus Without

Health IT ecosystems must combine individual access and shared health information, health information technology, safety in care delivery, population health management, regional health information exchange (RHIO), and leverage elasticity of big data analytics. Table 1. Highlights the ONC principles of interoperability, rested against the cryptocitizen that blockchain has the potential to enable, in comparison to the current state of interoperability progress without the future intervention of blockchain technologies.[8]

Blockchain enabled transactions, on the other hand, are managed by disintermediated central authorities controlling identity, data access, and permissions which promote trust between the producers and the consumers. Disintermediation is often accomplished by changing the perception of delivery and in this case, will change the perception of healthcare. Disintermediation fractures the role of the middlemen between producers or avoids traditional distribution channels with intermediates such as distributors, brokers or agents. In the case of healthcare disintermediation, co-creation trust leverages blockchain to improve authenticity.[9]

VII. BLOCKCHAIN TRANSACTIONAL PROCESSING FOR HEALTH

Blockchain allows organizations to operate and conduct commerce in a trustless and permissionless ecosystem to discover provenance of the product, service, or interaction. Provenance proves authenticity or origin creating an auditable record in addition to a historic record of the full supply chain of food products (allergies), prescriptions, and even your medical records to ensure traceability. Articulating the value of blockchain becomes even more challenging when applying the blockchain technology to healthcare. Welcome to the modern and fashionable electronic health record.

Allow me to expand; the doctor would confirm the diagnosis and confirm treatment was performed, and the payer would establish that insurance coverage was valid. The transaction verification is also where consensus of the diagnosis occurs. It could be as simple as requiring the public keys from a patient's doctor and provider to create consensus or agreement. This agreement is based on a threshold cryptosystem (mainly for the military prior to 2012, subsequent versions include: RSA, Paillier cryptosystem, Damgard–Jurik cryptosystem, ElGamal) or ring signatures (a message signed with a ring signature is endorsed by someone, in a particular group of people, e.g., your family doctor's health practice), or even other cryptographic techniques

[8] Office of the National Coordinator for Health Information Technology (ONC). Connecting Health and Care for the Nation: A 10-Year Vision to Achieve an Interoperable Health IT Infrastructure. (2015). Retrieved from https://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf

[9] Nichol, P. B. Disintermediation and intermediation beyond theory. (2016). Retrieved July 12, 2016, from http://www.cio.com/article/3058882/innovation/disintermediation-and-intermediation-beyond-theory.html

that could be implemented.[10]

The next explanatory steps updating an EHR from the perspective of the blockchain, illuminating the roles between the patients, payers, and the providers.

1. Receive Token – a healthcare transaction is received by the blockchain as a set of actions grouped in the form of tokens.
2. Pull Base Block – a historical block will be pulled (the last block confirmed) including an identifier for the block, which is used to create the new block.
3. Verify the Transaction – the token is validated (the set of healthcare actions, enrollment information, proof-of-insurance, diagnosis, and procedure codes for treatment) and broadcasted to named peers for review.
4. Validation of Block – at this point the digital signature of the validators is added to the block (hashed).
5. Token Extended – the initial health token (the set of actions) is extended to include the validity token from the confirmed health actions.
6. Block Creation – the block creation contingent on the validity token, historical block identifier, digital signatures, peer reviews, and the set of healthcare tokens. Through the consensus process, miners calculate, validate, and then generate the new block.
7. Block Broadcast – using the blockchain health record and the peer-reviewed token(s) these combined blocks (sets of healthcare actions) are then broadcast to peers.

To summarize: a token is received containing healthcare transactions (medical, dental, pharmacy, labs, messages, or ancillary services) and a historical block identifier is used as the start of the base new block. The token, a set of healthcare transactions, is peer reviewed and validated once the peer review is completed. Digital signatures are added to the block, extending the token. The healthcare token, historical identifiers (previous block), peer reviewed validated tokens, and with the digital signatures complete, the miners create a new block reflecting the recently received healthcare transactions. Miners then broadcast to peers on the blockchain.

Instead of medical data sitting across silos with limited interoperability, with blockchain we now have the ability to move the information in a secure, auditable, and shared data layer. Transparency isn't only about the supply of goods; it also involves services – healthcare services.[11]

VIII. MEDICAID AND MEDICARE FRAUD PREVENTION

Blockchain will have enormous impacts on global business and the world economy. This tectonic shift will disrupt citizens and change their behavior. This change is transformational and will affect everything from the clothes you wear, the food you eat, and even the products you buy. Blockchain technology will be injected into everything.

According to the Centers for Medicare and Medicaid Services (CMS), in Fiscal Year 2014, the government recovered $3.3 billion because of healthcare fraud judgments. Since 1997 with the inception the Healthcare Fraud and Abuse Control (HCFAC) Program, $27.8 billion have been recovered to the Medicare Trust Funds. Open Ledger technology such as blockchain can reduce this waste by providing a complete audit trail of transactions. In healthcare this will provide increased transparency to reduce and eliminate fraud in prescriptions, billing, and security breaches that drive patient identity fraud.

Patient identification and authentication is a huge problem increasing fraud and affecting interoperability. It costs CMS and health organizations millions of dollars a year in uncollectible fees. A primary issue is that the U.S. does not utilize a singular form of national patient identifier. As an alternative, the U.S. uses other forms of identification for patient identification that can be repudiated, such as social security numbers and driver's licenses. A recent report from the House Committee on Appropriations contains language on the use of national patient identifiers (patient registries). This subject has been talked about for many years. However, there has been political opposition to the adoption of a national patient identifier despite many healthcare experts believing this adoption is necessary to protect patient identity rights and for national healthcare interoperability.[12,13]

The blockchain framework inherently has the ability to solve our patient identity problem. There are several companies currently exploring applications of blockchain technologies to solve the global identity problem supported by digital passcards. The recent problem in Syria has highlighted the national concern with unidentified refugees. It is estimated that there are over 232 million undocumented migrants worldwide. Solving the challenge of a portable identity will move us closer to expanded healthcare for American citizens and those we protect.

Non-reputable digital passcards could replace our current IDs, e.g., driver's licenses, SS# and health insurance numbers. Traditional financial auditing as we once knew it has ended. Financial auditing will experience the most extreme business model change since the passage of the Sarbanes-Oxley Act (SOX) in 2002. New financial auditing with blockchain technologies ensures that businesses are fiscally responsible. This business model change will save lives.

At the 2016 Shanghai Blockchain Hackathon, a new team launched a new solution called PermaRec (permanent record), during this two-day event. Jennifer Qin Yi, an audit partner of a consultancy out of Beijing and lead partner responsible for coordination of the firm's investment management industry in Asia Pacific, led the team. This solution allows companies to record transactions in a globally distributed ledger residing on the blockchain. The PermaRec solution connects SAP, Oracle, and other financial reporting systems, enabling the consultancy to review transactions from both parties to ensure legitimacy and appease regulators. While the product is not mature, the thinking

[10] Nichol, P. B. Blockchain health record bank replaces EHRs and EMRs. (2016). Retrieved from http://www.cio.com/article/3051735/healthcare/blockchain-health-record-bank-replaces-ehrs-and-emrs.html

[11] Nichol, P. B. Blockchain health record bank replaces EHRs and EMRs. (2016). Retrieved from http://www.cio.com/article/3051735/healthcare/blockchain-health-record-bank-replaces-ehrs-and-emrs.html

[12] House of Representatives, Committee on Appropriations. DEPARTMENTS OF LABOR, HEALTH AND HUMAN SERVICES, AND EDUCATION, AND RELATED AGENCIES APPROPRIATIONS BILL, 2017, 1–269. (2016).

[13] Murphy, PhD, K. Why Optimism Is Building for National Patient Identifier. (2016). Retrieved July 17, 2016, from http://healthitinteroperability.com/news/why-optimism-is-building-for-national-patient-identifier

is visionary.

What if this PermaRec solution was in place for the Red Cross in 2010? It's more than likely that Haitian lives would have been saved, and the location of $488 million in donations would be fully accounted. The business of donations to support disaster relief will dramatically change. When consumers have the option of donating to an organization where every transaction is publicly transparently displayed on a blockchain or donate to an organization that doesn't share donation disbursement details – the citizen decision will be quick. The business of charity has just changed.

The Office of the National Coordinator for Health Information Technology (ONC) is able to leverage this example and apply this to prevent Medicaid and Medicare payment fraud. The Association of Certified Fraud Examiners (ACFE) estimates that fraud costs organizations worldwide $3.7 trillion a year or 5 percent of the Gross World Product (GWP). Extending this application of blockchain we can apply these principles to tackle fraud. Medicaid, Medicare, and Social Security fraud could be impacted by conducting transactions to beneficiaries and providers serviced from the blockchain. Blockchains can be used in any situation when a verifiable public record is required, and blockchain ecosystems benefit from not being under the control of any one entity. Blockchain technology, when applied to healthcare, has the potential to decrease corruption and fraud – creating entirely new business models enabling transparency and tightening down on waste and abuse.[14]

IX. RESEARCH PROPOSITIONS

The purpose of these propositions is not to extend information-theoretic results but to scope practical research domains to examine the role co-creation of trust plays in healthcare.

We developed these propositions based on healthcare challenges concentrating on improving the trust associated with treatment, improving access to personal medical information, and improving accuracy of patient information (medical and billing) to advance patient outcomes. We offer three general propositions (P1, P2, and P3) that link the role of patient-centric healthcare. Expanding on the dimensions to ubiquitous monitoring of medical devices through an immutable digital ledger, patient self-sovereignty of identity, improved trust for electronic health information exchanges and all payers' claims databases, we expect to influence each through improved patient trust and public transparency on the blockchain.

Consistent with the shift toward the co-creation of trust, conditional privacy, trust framework for healthcare, and the blockchain health ecosystems discussed earlier in this paper, the remainder of this paper introduces research propositions that examine co-creation of trust ecosystems.

A. Proposition 1: Healthcare Device Maintenance Ranging from Medical Devices to Nanomachines Will Autonomously Communicate Device-To-Device.

Robotics health threatens to challenge how patient care and treatment is performed while redefining the word "preventative." As devices continue to proliferate the patient clinical environment, device maintenance will transform into the Blockchain-Internet-of-Things (BIoT).

Device-to-device distributed sharing will create a new market for semi-autonomous devices. These devices - such as delivery robots providing medical goods throughout a hospital autonomously or disinfection robots that interact with people with known infectious diseases such as healthcare-associated infections or HAIs - will be reporting information not to a central authority but to other devices. Medical nanotechnology is expected to employ nanorobots that will be injected into the patient to perform work at a cellular level. Ingestibles and internables bring forward the introduction of broadband-enabled digital tools that are eaten and "smart" pills that use wireless technology to help monitor internal reactions to medications. Medical nanotechnology is just the beginning.[15]

One problem to consider is the onslaught of devices entering the medical market, e.g., in-patient (implanted, in-room), prescribed home health devices, and patient provided wearables. The management and provenance of all these devices is an issue that has not been addressed. Blockchain and smart contracts have the ability to provide information on devices, maintain their security, and provide the provenance, which will allow providers to place more trust in patient generated health data (PGHD).

Blockchain frameworks and smart contracts have the facilities to match devices to patients over the lifetime of a device: similar to the way drug manufacturers are fighting fraudulent drugs around the world.

The following is an example of how blockchain technologies could manage medical devices. A patient named John, with atrial fibrillation, is having an atrial defibrillation device implanted: commonly known as an Afib device. This implantable defibrillator allows quick restoration of the sinus rhythm by administering a low-energy shock. The Afib device was manufactured by company "X" with a serial number "Y." During manufacturing, a blockchain was created to track this device. The US Food and Drug Administration (FDA) mandated that a hash of the unique device identifier (UDI) be stored in the blockchain along with other pertinent information. The hash of the device information is stored and verifiable in an immutable digital ledger. The implanted Afib device is assigned to John (patient), and the device's blockchain is updated with information such as hospital, doctor, emergency contacts, and advance directives around care for patient John. The Afib device is supported by a series of smart contracts that can autonomously notify John (patient) and providers when the device needs service, e.g., battery expiration, or when health irregularities are detected.

Today, device preventive maintenance is rudimentary at best. For example, when an Afib device requires maintenance, the device starts to audibly alarm Jon (patient), which can be disturbing. A smart contract could also send preventative maintenance information to the patient and provider, reducing the chance of a catastrophic failure.

In January 2016, the Population Reference Bureau report, *Aging in the United States*, showed that Americans 65-and-older will more than double – growing from 46 million today to 98

[14] Nichol, P. B. How CIOs explain blockchain to their CFO. (2016). Retrieved July 11, 2016, from http://www.cio.com/article/3072470/healthcare/how-cios-explain-blockchain-to-their-cfo.html

[15] Nichol, Peter B. How medical robots will change healthcare. (2016). Retrieved from http://www.cio.com/article/3043172/innovation/how-medical-robots-will-change-healthcarerhealth-get-familiar-with-it.html

million by 2060. The growth of the total population 65-and-older population is projected to grow from 15 percent to nearly 24 percent. Who will take care of the influx of aging individuals, when timely healthcare today is already questionable? Medical robots will change healthcare. They have to.

Co-creation of trust for healthcare can provide a healthcare device management system that interoperates with any healthcare system.

B. Proposition 2: Personal and Public Self-sovereign Will Place Identity Ownership in the Hands of the Patient.

Self-ownership (or sovereignty of the individual, individual sovereignty or individual autonomy) is the concept of property in one's own person, expressed as the moral or natural right of a person to have bodily integrity, and be the exclusive controller of her or his own body and life. Tilting this definition, we can apply self-ownership to healthcare and ownership of patient information. Self-sovereign identity is guided by the principle that every patient is the source and therefore owner of their own identity. This is not an administrative control that can be rented, leased, or sold. The immutability of blockchain hardens the data over time, to offer a canonical record of health data. Patient ownership of the data, accelerates patient data transparency to observe what data is being accessed, who can access the data, and for what period of time. Self-sovereign identity provides sovereignty, security, and privacy to promote benefits for the patient and the organization or agency by reducing risk, strengthening security, improving accuracy, deepening permission control, and decreasing the time required for regulatory oversight. Several distributed consensus technologies, including NameCoin, DNSChain, and BlockChainID provide components of identity system registries.

LinkedIn and Amazon have low levels of sovereignty that can be disabled at the discretion of the identity provider. Patient identity ownership, on the blockchain, prevents the disadvantages of person data stores (where the user is their own identity provider) or the disadvantages of identity as a service or IAAS (contracted service under the control of the patient).[16]

Self-sovereignty distributed consensus empowers the patient with ownership of their medical identity. Shared identities expanded to include meta-data can be combined with public access control rules, which a network ecosystem can leverage to moderate access-control.[17]

C. Proposition 3: Electronic Health Information Exchanges (HIE) and All-Payer Claims Databases (APCD) Will Establish Trust Using Blockchain Technologies.

The co-creation of trust can improve the speed, quality, safety, and cost of patient care by applying blockchain technology to the three key forms of HIEs:

1. Directed Exchange (ability to send and receive secure information electronically between care providers to support coordinated care)
2. Query-based Exchange (ability for providers to find and/or request information on a patient from other providers, often used for unplanned care).
3. Consumer Mediated Exchange (ability for patients to aggregate and control the use of their health information among providers).[18]

Directed Exchanges can use blockchain's immutable and chronological time stamped ledger to improve verification of authenticity. Query-based Exchanges can leverage API addressable indexing to verify authenticity of patient information to improve accuracy of decisions on clinical diagnoses, medications, labs, removing much of the need for duplicative testing. Consumer Mediated Exchanges could unify patient confidence empowering patients to be the "CEO of their personal health."

Patients could actively participate to validate the accuracy of their health information, offer conditional access to providers and payers, and correct billing information from a unified access record leveraging blockchain distributed consensus.[19]

X. PRACTICAL APPROACHES FOR INTEGRATING BLOCKCHAIN TECHNOLOGIES INTO HEALTHCARE SYSTEMS

Healthcare organizations, patients, and providers want a frictionless process when accessing medical records systems. Electronic health record implementations over the past several years have been disruptive to workforce productivity; future healthcare innovations need to be seamless, not disruptive to existing health operations. Adding blockchain technologies into the healthcare ecosystem must be straightforward. Integrating blockchain technologies into healthcare is as simple as adding an additional database and authentication schema to a legacy system. Extending databases to support expanded customers, providers, or billing requirements is performed daily in multiple domains outside of healthcare.

A RESTful (architectural style of interactions between data elements rather than implementation details) solution such as Fast Healthcare Interoperability Resources (FHIR, pronounced "fire") could be used to access and share records. EHRs could store records using blockchain technology without interrupting existing healthcare services. Enhancing the authentication, authorization, and data locations are the only business system design changes required.

The pinnacle of medical records' interoperability is patient controlled medical records. With blockchain technologies patients can own and control their identity, access their data, and conditionally authorize the sharing of medical records with providers. The remaining challenge to solving healthcare interoperability is not seamless connection to providers, but rather normalizing the semantics and convincing EHR vendors to participate in sharing of patient records. Interoperability will start once ownership of health records has shifted from provider-controlled patient information to patient-controlled health information. Please note, that while important, the technical orchestration of authentication and authorization will not be covered in this article.

[16] Smith Ph.D., S. M., & Khovratovich Ph.D., D. Identity System Essentials. (2016). Retrieved from http://evernym.com/assets/doc/Identity-System-Essentials.pdf

[17] Zyskind, G., Nathan, O., & Pentland, A. Enigma: De-centralizaed Computation Platform with Guaranteed Privacy, 9. (2015).

[18] Office of the National Coordinator for Health Information Technology (ONC). What is HIE (Health Information Exchange)? (2014). Retrieved from https://www.healthit.gov/providers-professionals/health-information-exchange/what-hie

[19] Nichol, P. B. Blockchain collaboration defines the fabric for healthcare 2.0. (2016). Retrieved from http://www.cio.com/article/3050664/healthcare/blockchain-collaboration-defines-the-fabric-for-healthcare-20.html

XI. THEORETICAL AND REGULATORY IMPLICATIONS

Firstly, this paper contributes to the literature on co-creation of trust for healthcare. Previous work has focused on the application of blockchain in financial services; this paper sets the foundation for future work to explore the implications of patient-centric empowerment underpinned by blockchain.

Secondly, it adds to the body of research on healthcare applications with blockchain by addressing the benefit to healthcare ecosystems and differentiating these benefits from the current state landscape aligned to the ONC vision to achieve an interoperable health IT infrastructure. A fundamental aspect of the co-creation of trust for healthcare requires changes to the healthcare culture impacting the complex dynamics of healthcare delivery. Healthcare entities will not need to change their technology backbone, but will need to change how prevention, treatment, and outcomes are recorded.

Thirdly, there are several implications for practice. The next frontier is the convergence of the physical, digital, and biological. The inexorable shift will have a profound effect on the patient experience. Citizens will increasingly engage with governments. This increased engagement will place pressure on public authorities to embrace disruptive changes, increase transparency, and improve efficiency. The evolution of privacy will not become an exogenous force, over which the private and government entities will have limited control. The ability to shape the future is here and we as citizens are empowered to lead the change.

Lastly, regulators must consider that when regulations are put in place firms generally reallocate financial resources away from innovation activities and towards regulatory compliance activities. Regulations should be inevitably concentrated on flexibility (incentives-based, performance aligned), information based (accounting for substantive compliance value adds), and stringency (the degree of change required for innovation within a compliance landscape). The government must maximize regulations that incentivize innovation, not disincentivize.[20]

XII. LIMITATIONS AND DIRECTIONS FOR FUTURE WORK

There are some limitations to this conceptual analysis. Firstly, this is an explanatory paper that presents a set of propositions but does not explicitly propose implementation approaches. Secondly, the conceptual analysis supports its propositions with the assembling of concepts. It does not follow any single fit-for-use application as such subjecting it to multiple hypotheses. Future research is needed to develop practical approaches to implementation to expand on a single theory that could encompass the realization of the co-creation of trust for healthcare presented in this paper. The above propositions need to be tested with proof-of-concept trials.

The independent variable could be the degree of trust co-creation while the dependent variable could be a set of varied performance measures such as patient satisfaction, security, data access, data authenticity, and data permissions accuracy and the method selected to test. An example would be a mixed methods design, which would combine surveys, proof-of-concept results, and patient information. Another direction for further work could be to test the impact of co-created trust systems within a healthcare micro-community on patient satisfaction through a longitudinal study.

The fact is, in 2015, large investors pumped over USD $1.21 trillion (as of July 23, 2016) into blockchain technology companies. Yet some industries remained tied to the methods of the past. Remember the hype over the telegraph in the nineteenth century? The telephone has matured but hype? We all know how overstated the telephone was by the end of the nineteenth and start of the twentieth centuries. How about the buzz and over promises of canals and railroads in the 1700s and 1800s? Hype probably isn't the best word to describe the development of railroads that were one of the most important phenomena of the Industrial Revolution. The list doesn't seem to end and continues with the likes of automobiles, radios and then the jet engine, rockets, and atomic energy into the 1950s and 1960s with biotechnology, nanotechnology, and genomics. Do we consider the canals, railroads, telegraphs, automobiles, and cell phones hype? If these hyped technologies landed us here, imagine how blockchain can change society in the future.[21]

XIII. CONCLUSION

This paper developed a concept for the co-creation of trust for healthcare. Three main propositions were conceptualized.

Interoperability, security, and payment reform are the three toughest obstacles in the quest towards improving healthcare. Bitcoin is only one example in a sea of blockchain potential applications: we must not forget the application to healthcare. Blockchain may well be a game changer. Whether the digital currency industry takes off or not, blockchain technologies will revolutionize every industry and the ways in which consumers and patients interact. These propositions suggest that blockchain can be applied to healthcare ecosystems to create trust, enable conditional patient privacy, and securely protect electronic health records. Blockchain technology can rebuild trust in healthcare.[22]

XIV. REFERENCES

[1] Nichol, P. B. Person-centric healthcare amplified by blockchain. (2016). Retrieved from http://www.cio.com/article/3041641/health/person-centric-healthcare-amplified-by-blockchain.html

[2] Nichol, P. B. How CIOs explain blockchain to their CFO. (2016). Retrieved July 11, 2016, from http://www.cio.com/article/3072470/healthcare/how-cios-explain-blockchain-to-their-cfo.html

[3] Economist. The promise of the blockchain: The trust machine. (2015). Retrieved from http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

[4] Mougayar, W. Understanding the blockchain - O'Reilly Radar. (2015). Retrieved from http://radar.oreilly.com/2015/01/understanding-the-blockchain.html

[5] Nichol, P. B. Blockchain Technology: The Solution for Healthcare Interoperability. (2015). Retrieved from https://www.linkedin.com/pulse/blockchain-technology-solution-healthcare-peter-b-nichol

[20] Stewart, L. A. The Impact of Regulation on Innovation in the United States: A Cross-Industry Literature Review. Institute of Medicine Committee on Patient Safety and Health IT. (2010). Retrieved from http://www.itif.org/files/2011-impact-regulation-innovation.pdf

[21] Bitcoin: Why unfamiliarity is slowing healthcare adoption. (2016). Retrieved from http://www.cio.com/article/3052264/innovation/blockchain-is-not-bitcoin-why-unfamiliarity-is-slowing-healthcare-adoption.html

[22] Ibid.

[6] Nichol, P. B. Blockchain Technology: The Solution for Healthcare Interoperability. (2015). Retrieved from https://www.linkedin.com/pulse/blockchain-technology-solution-healthcare-peter-b-nichol

[7] Ibid.

[8] Office of the National Coordinator for Health Information Technology (ONC). Connecting Health and Care for the Nation: A 10-Year Vision to Achieve an Interoperable Health IT Infrastructure. (2015). Retrieved from https://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf

[9] Nichol, P. B. Disintermediation and intermediation beyond theory. (2016). Retrieved July 12, 2016, from http://www.cio.com/article/3058882/innovation/disintermediation-and-intermediation-beyond-theory.html

[10] Nichol, P. B. Blockchain health record bank replaces EHRs and EMRs. (2016). Retrieved from http://www.cio.com/article/3051735/healthcare/blockchain-health-record-bank-replaces-ehrs-and-emrs.html

[11] Ibid.

[12] House of Representatives, Committee on Appropriations. DEPARTMENTS OF LABOR, HEALTH AND HUMAN SERVICES, AND EDUCATION, AND RELATED AGENCIES APPROPRIATIONS BILL, 2017, 1–269. (2016).

[13] Murphy, PhD, K. Why Optimism Is Building for National Patient Identifier. (2016). Retrieved July 17, 2016, from http://healthitinteroperability.com/news/why-optimism-is-building-for-national-patient-identifier

[14] Nichol, P. B. How CIOs explain blockchain to their CFO. (2016). Retrieved July 11, 2016, from http://www.cio.com/article/3072470/healthcare/how-cios-explain-blockchain-to-their-cfo.html

[15] Nichol, Peter B. How medical robots will change healthcare. (2016). Retrieved from http://www.cio.com/article/3043172/innovation/how-medical-robots-will-change-healthcarerhealth-get-familiar-with-it.html

[16] Smith Ph.D., S. M., & Khovratovich Ph.D., D. Identity System Essentials. (2016). Retrieved from http://evernym.com/assets/doc/Identity-System-Essentials.pdf

[17] Zyskind, G., Nathan, O., & Pentland, A. Enigma: De-centralizaed Computation Platform with Guaranteed Privacy, 9. (2015).

[18] Office of the National Coordinator for Health Information Technology (ONC). What is HIE (Health Information Exchange)? (2014). Retrieved from https://www.healthit.gov/providers-professionals/health-information-exchange/what-hie

[19] Nichol, P. B. Blockchain collaboration defines the fabric for healthcare 2.0. (2016). Retrieved from http://www.cio.com/article/3050664/healthcare/blockchain-collaboration-defines-the-fabric-for-healthcare-20.html

[20] Stewart, L. A. The Impact of Regulation on Innovation in the United States: A Cross-Industry Literature Review. Institute of Medicine Committee on Patient Safety and Health IT. (2010). Retrieved from http://www.itif.org/files/2011-impact-regulation-innovation.pdf

[21] Bitcoin: Why unfamiliarity is slowing healthcare adoption. (2016). Retrieved from http://www.cio.com/article/3052264/innovation/blockchain-is-not-bitcoin-why-unfamiliarity-is-slowing-healthcare-adoption.html

[22] Ibid.

[23] Charles, MHP, D., Gabriel, Ph.D., M., & Searcy, MPA, MA, T. Adoption of Electronic Health Record Systems Among U.S. NonFederal Acute Care Hospitals: 2008-2014 (pp. 1–10). Office of the National Coordinator for Health Information Technology. (2015). Retrieved from https://www.healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf

[24] Lilley, K. Current, former Guard members warned of data breach. (2015). Retrieved from http://www.armytimes.com/story/military/guard-reserve/2015/07/14/national-guard-data-breach-opm-ssn/30150319/

[25] Mathews, A. W. Anthem: Hacked Database Included 78.8 Million People. (2015). Retrieved from http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364

[26] Nakashima, E. Hacks of OPM databases compromised 22.1 million people, federal authorities say -. (2015). Retrieved from https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

[27] NEWSBTC. Healthcare on a Blockchain. (2015). Retrieved from http://www.newsbtc.com/2015/05/18/healthcare-on-a-blockchain/

[28] Nichol, P. B. Personalization of Big Data Analytics: Personal Genome Sequencing. (2015). Retrieved July 12, 2016, from https://www.linkedin.com/pulse/personalization-big-data-analytics-personal-genome-peter-b-nichol

[29] Nichol, P. B. Blockchain applications for healthcare. (2016). Retrieved from http://www.cio.com/article/3042603/innovation/blockchain-applications-for-healthcare.html

[30] Nichol, P. B. Healthcare tailored with precision medicine. (2016). Retrieved from http://www.cio.com/article/3041938/healthcare/healthcare-tailored-with-precision-medicine.html

[31] Nichol, P. B. How to monetize healthcare using blockchain. (2016). Retrieved from http://www.cio.com/article/3042158/health/how-to-monetize-healthcare-using-blockchain.html

[32] Snyder, M., Du, J., & Gerstein, M. Personal genome sequencing: current approaches and challenges. (2010). Retrieved from http://genesdev.cshlp.org/content/24/5/423.full

[33] Weiss, M. How Bitcoin's Technology Could Reshape Medical Experiences. (2015). Retrieved from http://www.coindesk.com/bitcoin-technology-could-reshape-medical-experiences/