Blockchain Technology Innovations

Tareq Ahram[1], Arman Sargolzaei[2], Saman Sargolzaei[3,4], Jeff Daniels[5], and Ben Amaba[6]

[1]Institute for Advanced Systems Engineering, University of Central Florida, Orlando, FL, USA
[2]Department of Electrical Engineering, Florida Polytechnic University, Lakeland, FL, USA
[3]Rancs Group LLC, Wilmington, DE, USA
[4]Department of Neurosurgery, University of California at Los Angeles, Los Angeles, CA, USA
[5]Lockheed Martin, Dallas, TX, USA
[6]IBM Corporation, Miami, FL, USA

***Abstract*— Digital world has produced efficiencies, new innovative products, and close customer relationships globally by the effective use of mobile, IoT (Internet of Things), social media, analytics and cloud technology to generate models for better decisions. Blockchain is recently introduced and revolutionizing the digital world bringing a new perspective to security, resiliency and efficiency of systems. While initially popularized by Bitcoin, Blockchain is much more than a foundation for crypto currency. It offers a secure way to exchange any kind of good, service, or transaction. Industrial growth increasingly depends on trusted partnerships; but increasing regulation, cybercrime and fraud are inhibiting expansion. To address these challenges, Blockchain will enable more agile value chains, faster product innovations, closer customer relationships, and quicker integration with the IoT and cloud technology. Further Blockchain provides a lower cost of trade with a trusted contract monitored without intervention from third parties who may not add direct value. It facilitates smart contracts, engagements, and agreements with inherent, robust cyber security features. This paper is an effort to break the ground for presenting and demonstrating the use of Blockchain technology in multiple industrial applications. A healthcare industry application, *Healthchain*, is formalized and developed on the foundation of Blockchain using IBM Blockchain initiative. The concepts are transferable to a wide range of industries as finance, government and manufacturing where security, scalability and efficiency must meet.**

Keywords—Blockchain; Business; Cloud computing; Cloud services; Control Systems; Cybersecurity; DevOps; Finance; Government; Healthcare; IoT; Industry 4.0.

I. INTRODUCTION

Blockchain is a distributed ledger technology, commonly used in the crypto currency Bitcoin. The Financial Times (2016) defines Blockchain as a "network of computers, all of which must approve a transaction has taken place before it is recorded, in a 'chain' of computer code. The details of the transfer are recorded on a public ledger that anyone on the network can see."

In 2008, Satoshi Nakamoto introduced the world to Bitcoin by releasing the paper, "Bitcoin: A Peer-to-Peer Electronic Cash System."[1] The proposal was to distribute electronic transactions rather than maintain dependency on centralized institutions for the exchange. When looking at Bitcoin the new concept is the Blockchain framework based on research for time stamping packages and protecting the chain of custody. Blockchain is essentially a simplified payment verification system. Bitcoin and by extension, Blockchain, are realizing steady growth. At the time of this paper, statistics from Blockhain.info indicate a $15.3B market cap and $314.7M in transactions per day. Despite the growth, many questions surround widespread adoption of Bitcoin. However, the underlying framework has gained attention with application outside of the financial world.

Blockchain will mature in a number of areas as the body of research grows. Researchers are working to apply a number of use cases included smart contracts, supply chain, and healthcare [2] (PHI) as this paper demonstrates. Associate Professor of Computer Science at Cornell Emin Gün Sirer, has observed, "The Internet of Things could be an enormous application area where people want to communicate with devices, but not through intermediaries. There is no killer app yet, but it is likely to feature the transparency of Blockchain [3]." Today, researchers are focused on security, privacy, and scalability of Blockchain. In his April, 2016 piece, "Might Blockchain Outlive Bitcoin?" Hurlburt addresses the need for ethics and operational guidance observing before Blockchains become commonplace replacement for traditional transaction databases, strict standards, including acceptable behavioral guidelines, must be lay out[1].

We started with a financial application for transactions in Bitcoin. The ceiling is high and expectations are boundless for Blockchain. Applications vary and many technologists are bullish on the future. For example, digital entrepreneur Blythe Masters indicates "you should be taking this technology [Blockchain] as seriously as you should have been taking

978-1-5090-1114-8/17/$31.00 ©2017 IEEE

the development of the Internet in the early 1990's. It's analogous to email for money [4]." Michael Harte, CTO at Barclays suggests the transformative nature of Blockchain, "we could go the way that file transfer technology changed music, allowing new businesses like iTunes to emerge [5]."

Cognitive computing, IoT, supply chain, and healthcare applications hold promise for integration with Blockchain. The paper surveys the promises of Blockchain technology from the cybersecurity perspective. Next is a discussion on professional responsibility of Blockchain technology. *HealthChain* is then introduced where Blockchain technology powers security, scalability and efficiency in the healthcare industry application. The paper concludes with a summary of how Blockchain is changing the world.

II. CYBER SECURITY

As part of the discussions at the 2013 VSAE Annual Conference (www.vsae.org), data and currency have similar challenges [6]. Data may be a more important asset than money in certain scenarios. Money and other valuables such as jewelry can be kept under your mattress – a premises solution – or in a bank – a cloud solution. Which has the better security? The bank can afford stronger security in terms of vaults with foot thick hardened steel walls, and can have a security team made up of security professionals and one or more people on payroll who stay abreast of new burglary strategies and determine and implement counterstrategies. The platforms and components were chosen to ensure a robust framework on the prevention, isolation and remediation of cyber-security breaches. For example, the IBM Bluemix platform leverages the security API (application programming interface) to secure workloads against the latest threats and comply with regulatory requirements efficiently.

The platform is used to simplify the management of who can sign in to cloud applications, and scan those applications for vulnerabilities, embed security controls into data management and big data services. Protect access to apps and workloads, scan apps for vulnerabilities, and protect the data are very important as part of the security control and vulnerability analysis. With the platform, we can easily add user authentication and single sign-on capabilities into web and mobile apps, deploy policy-based authentication interfaces to allow quick creation of multi-factor authentication, assess web and mobile applications for vulnerabilities, strengthening both security and regulatory compliance efforts by scanning apps before deployment, you can identify issues, generate reports, and make recommended fixes.

To protect the data, the platform approach will utilize built-in security and privacy controls within big data and data management services, including data masking, discovery, and audit. Taking the API approach, we can then combine the security API with other APIs including IoT (Internet of Things), DevOps, Cloud Integration, Mobile and Business Analytics. Another aspect that we had to consider was we had to place the API platform on a secure infrastructure, which supports deployment of regulated workloads through extensive compliance and clear delineation of roles and responsibilities. The project was able to reuse important best practices and patterns to insure success of the information system and the life cycle from end to end for the project.

III. PROFESSIONAL RESPONSIBILITY

With the conversion from analog to digital devices, goals and approaches have changed overnight in the products, processes and services enabled with software. Public infrastructures are becoming more advanced through sensors, computing chips, actuators and better power sources. Software, hardware, and networks are transforming all the digitalization of transportation, air quality, water purity, buildings, materials, and environment. Although the technologies will continue to change; the technical, ethical and moral responsibility for professionals only increase. Post-accident root-cause analyses often point to operator error: a human mistake is almost always involved somewhere in the chain of events. When one delves into the big engineering disasters (Chernobyl, Fukushima, Deep Water Horizon, and Bhopal), one finds that failures of social and professional engineering surface. Usually, behind the human mistake, one finds a series of organizational and management actions that make that mistake more and more likely [7].

Professionals must protect the public's safety, security, health and welfare as their top priority. Due to pressure on many teams, quality and outcome was not the primary goal while time and resource conservation detracted from the public's well-being. Recent misconduct in emissions standards of vehicles to the EPA (Environmental Protection Agency) signifies the importance of continual education of ethical and moral standards in conjunction with technical competence. Civil, mechanical, electrical, chemical, and sanitation professional engineers have been in place to insure the public's well-being. Until recently, system and software engineers were not compelled to conform to the minimum standards.

Today, software engineers can obtain their software professional engineering license through the National Society of Professional Engineers like their peers**.** Licensure is the process by which a federal, state or local governmental agency grants an individual permission to practice in a particular occupation or profession that is subject to regulation under the government's authority and to refer to oneself as "licensed" or authorized to practice. Within the practice acts are mandates for practitioners to become licensed, usually based upon requirements such as education, examination, experience and moral character. Obtaining a license in order to practice a profession is *mandatory*, and state laws may provide for criminal or administrative penalties for unlicensed practice. Also, systems engineering has become integrated into the other engineering disciplines

as part of the National Society of Professional Engineers' Engineering Body of Knowledge as one of the key technical capabilities. Therefore, for the new complex digital devices, there is responsibility and a path to professional licensure that not only incorporates minimum technical competency, but ethical and moral principles to protect the public. Misconduct, negligence and incompetence are aspects too risky for digital construction and infrastructure projects. Therefore, as licensing continues to span the profession with the minimum standard of care, it becomes vitally important to understand the process in the context of the type of project, risk, environment and skills. The American Society of Mechanical Engineers (ASME) has been proactive regarding computer programs too, as digital controls and analysis become more the norm. In 2011, Westinghouse failed to appropriately dedicate commercially procured software in accordance with the law. Specifically, Westinghouse did not conduct a technical evaluation to identify safety function, critical characteristics, and acceptance methods for a commercially procured version of the ANSYS finite-element analysis software**.** In 2013, the Nuclear Regulatory Commission (NRC) inspection team determined that Ultra Electronics did not appropriately control Lab View, a 3rd Party Software, in accordance with released procedures and instructions or demonstrate by another means of verification (i.e. dedication or conducting tests not relying on the same software used for design) that the software was capable of performing its safety function as related to the testing of safety related components.

These events and others have raised the professional accountability of not only the control systems software, the analysis and support software that could affect the performance of the nuclear system. Even the emerging Blockchain technology looks to professional engineers to help govern and manage its maturation. Major power industry transformations are likely to emerge as Blockchain matures. While initially popularized by Bitcoin, Blockchain is much more than the foundation for crypto currency. It offers a secure way to exchange any kind of good, service, transaction or information with the potential to build new global networks and drive new business models for manufacturers and power companies. The continued similarities between the goals of Blockchain protocol and the professional engineering protocol are remarkable thus demonstrating that, individually, Blockchain ideas are not new and may in fact be more compatible to existing institutions than previously considered. Professional licensure now plays a major role in new engineering disciplines such as software engineering or Blockchain because of the impact it is now playing in all of our traditional engineering disciplines and infrastructure that is digitally transforming.

Blockchain as a software technology would naturally fit into the professional software engineering licensure minimum standard of care. With public health, wealth, safety, security and environmental protection as a priority, licensing bestows accountability and liability to those developing and operating digital systems and privacy records. There is a tremendous responsibility to persons, institutions and our environment when new technology is introduced. There are several risks that should be considered. By offering a minimum standard of care or benchmark of not only technical, but ethical and moral responsibility, we will be able to mitigate risks with the customers' best interest as top of mind.

IV. BLOCKCHAIN POWERED HEALTHCHAIN

Following HIPAA (Health Insurance Portability and Accountability Act of 1996) privacy rule, individually identifiable health information including demographic and genetic information, that is transmitted or maintained in any form or medium, is categorized as Protected Health Information (PHI) [8], [9]. HIPAA privacy rule sets standards on keeping the privacy of the individuals' PHI under control and gives patient's rights over the information. Although the rapid growth of cloud utilization for creation of HIPAA-compliant database boosted the physical safeguarding of information and reduced HIPAA violations, however this mitigation to distributed databases on the cloud would not alone solve the health care payee and provider's dilemma of privacy breaches. The situation worsens when facing different infrastructure deployed by different health care providers or even further when the statistics show a significant rise of mobile device uses, including smart phones and tablet computers, among physician and patients to communicate with each other, or access to PHI [10]. Much has been achieved by introducing mobile apps and software for clinical practices, yet despite the traditional encryption and password settings applied by HIPAA for a covered entity, breaches may still occur and PHI may be compromised[11]. Necessity of proper use and integration of new devices, which have access to PHI, is an utmost priority in an efficient health care era. The current work considers Blockchain technology use case to tackle the above-mentioned barrier of accommodating novel technologies into the existing HIPAA compliant network facilitating excellent care and patient comfort.

Fig. 1 describes how Blockchain technology can improve the system efficiency while optimizing security and scalability. A sample lifecycle of an individuals' PHI where each of the networks (Urgent Care Network, Primary Care Physician (PCP), and Referral Network) create and update their own versions of PHI. In this scenario, each network may/may not have access to the full updated version of the PHI (Original updated version hypothetically kept with the patient) and therefore may not be providing the individual with proper diagnosis and treatment. The other disadvantage of the currently utilized scenario its requirement for the patient to fill out the questionnaires based on which a new copy of the PHI is created for each individual network and is kept locally. Prior explanation on the exponential growth of the use of mobile devices technologies in each of the involved networks could potentially increase security concerns

due to the fragmented supporting information system. Considering individuals' PHI as a digital *asset*, Blockchain technology offers a robust solution where every *authorized* provider, including patient, can access, analyze and update an agreed record (shared *ledger*) of the PHI, irrespective of the network they belong to. A proposed Blockchain implementation of the lifecycle of PHI, which we refer to it as *HealthChain,* targets multiple facets of the optimized design simultaneously. The patient creates the first version of the PHI record during initial visit to one of the provider networks. Initial version of the PHI (our digital asset in the chain) is then loaded on to the Blockchain. Utilization of the *Smart Contracts* [12],[13] insures that the patient can only create the initial version of PHI and load it onto the Blockchain.

Invoking a transaction by the patient can lead into transferring the *asset (PHI Record)* to the provider. The *transaction* is not finalized until *Consensus* is achieved. All updates to the PHI are visible to the members of the chain with right permissions. Retaining robustness, security, privacy and validity of the PHI are continuously insured with the use of proven decentralized cryptocurrencies joined with Blockchain technology (www.ibm.com/blockchain). The utilized 3 tier architecture of *HealthChain* is implemented as a private Blockchain network on IBM Blockchain and deployed on Bluemix (https://www.ibm.com/cloud-computing/bluemix/). Top layer of the architecture is populated with a web page interface where user interacts with the *HealthChain*. Web page is hosted on the middle layer where a NodeJs (www.nodejs.org) server is responsible to communicate with the HyperLedger fabric and chain code. User interface of the implemented system is shown in Fig. 2 along with background node construction.

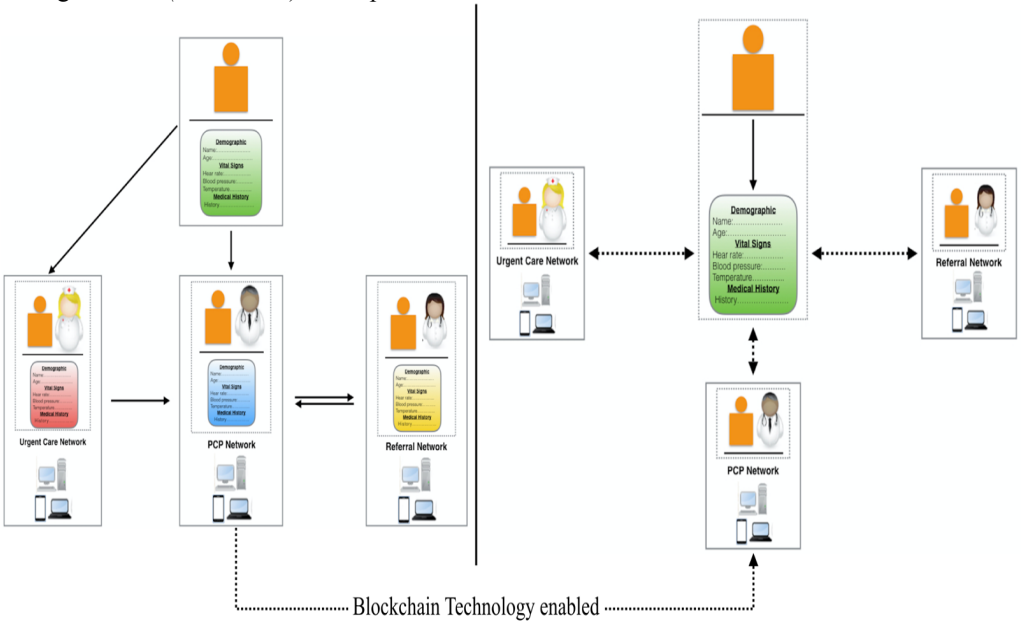

Fig. 1. **(above)** Current lifecycle of Protected Health Information (PHI) on the healthcare provider networks. Each of the involved networks, "urgent care network", "primary care physician (PCP) network", "Referral network", creates and updates its own version of an actual correct PHI; **(right)** HealthChain, a proposed implementation of Blockchain technology architecture. This design facilitates the access to a most up-to-dated and complete version of the patients' PHI while setting a higher standards for security and robustness.

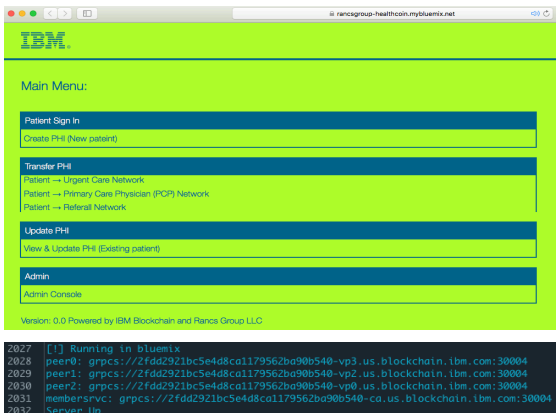

Fig. 2. HealthChain system User Interface (UI) with the backgorund blockchain network construction data highlighting the creation of blockchain peers on IBM cloud.

HealthChain powered by Blockchain largely benefits from the modular architecture of Hyperledger fabric which enables confidentiality, scalability and security in health informatics. Its implementation of smart contracts ensures the proper authorization and set privileges on its permissioned network. HealthChain is equipped with PBFT consensus[14] algorithm which provides a

continuous reliable service delivery in asynchronous environment (populated with software bugs, operator mistakes and malicious attacks) and yet minimizing the computational complexity burden required by conventional solutions to encrypt PHI transfers between healthcare network providers and/or mobile devices within the networks.

V. CONCLUSION

Information technology has become a critical innovation in almost every industry. Those institutions or teams that can use technology correctly and effectively play a major role in disrupting the status quo in a leadership position. Those that don't keep up with technology generally do not survive. The authors of this paper have identified the Blockchain technology as a catalyst for emerging use cases in the financial and non-financial industries such as industrial manufacturing, supply chain, and healthcare. The research indicates Blockchain can play a pivotal role in transforming the digitization of industries and applications by enabling secure trust frameworks, creating agile value chain production, and tighter integration with technologies such as cloud computing, and IoT. In producing a cloud-based application called HealthChain, the researchers have demonstrated the capability to apply professional engineering principles, combined with a DevOps approach to iterative development and management, and integration of cyber security, distributed computing, and Block-chain technologies. We feel HealthChain is one of many examples that demonstrate the transformative capability of Blockchain.

Industry is looking to produce efficiencies, create new innovative products, and strengthen customer relationships globally by the effective use of mobile, IoT (Internet of Things), social media, analytics and cloud technology to generate models for better decisions. Blockchain offers a secure way to exchange any kind of good, service, or transaction. Establishing the initial technology in the financial sector as given us insight and recommendations to be applied to other industries including health care where security, transformation and regulation plays a major role in advancing. Blockchain will enable more agile value chains, faster product innovations, closer customer relationships, and faster integration with the Internet of Things (IoT) and cloud technology. Blockchain allows immediate contracts, engagements, and agreements with inherent, robust cyber security features. This paper presented how Blockchain is changing the world.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Www.Bitcoin.Org*, p. 9, 2008.

[2] S. Sargolzaei, B. Amaba, M. Abdelghani, and A. Sargolzaei, "Cloud-based Smart Health-care Platform to tackle Chronic Disease," vol. 4863, no. August, pp. 30–32, 2016.

[3] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[4] G. Hurlburt, "Might the Blockchain," no. April, pp. 12–16, 2016.

[5] B. Libert, M. Beck, and J. Wind, "How blockchain technology will disrupt financial services firms," *Knowledge@Wharton*, pp. 2–7, 2016.

[6] G. Engaged, J. Tobe, G. Your, C. Computing, C. Dellorso, E. Apps, E. Reggie, R. Coughlan, and M. S. Fernandes, "Annual Conference – May 6-7 , 2013 – Kingsmill Resort ' The Value of Values : Linking Strategy and Decision Making ' – 2013 Annual Conference Educational Sessions," 2013.

[7] W. E. Summary and S. Plants, "Power and the Industrial Internet of Things (IIoT)," no. January, pp. 1–14, 2015.

[8] U. S. D. of H. and H. Services, "Standards for privacy of individually identifiable health information; proposed rule.," *Fed. Regist.*, vol. 64, no. 212, p. 59917, 1999.

[9] Centers for Medicare and Medicaid Services, "Security Standards: Technical Safeguards," *HIPAA Secur. Ser.*, vol. 2, pp. 1–17, 2007.

[10] M. Modahl, "Tablets set to change medical practice," *Quantia MD*, 2011.

[11] C. L. Ventola, "Mobile devices and apps for health care professionals: uses and benefits," *Pharm. Ther.*, vol. 39, no. 5, p. 356, 2014.

[12] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 254–269.

[13] K. Delmolino, M. Arnett, A. E. Kosba, A. Miller, and E. Shi, "Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab.," *IACR Cryptol. ePrint Arch.*, vol. 2015, p. 460, 2015.

[14] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *OSDI*, 1999, vol. 99, pp. 173–186.