Commodifying Trust

Trusted Commerce Policy Intersecting Blockchain and IoT

Lee W. McKnight
Syracuse University iSchool

Richie Etwaru
Syracuse University iSchool & QuintilesIMS

Yihan Yu
Syracuse University Newhouse School & Syracuse University WiTec

Paper prepared for presentation at: 45th TPRC Research Conference on Communications, Information and Internet Policy, George Mason University School of Law, Arlington, Virginia, September 8-9, 2017

AUGUST 12, 2017

SYRACUSE UNIVERSITY SCHOOL OF INFORMATION STUDIES

Contents

Suggested Citation:

McKnight, Lee W. and Etwaru, Richie and Yu, Yihan, Commodifying Trust: Policy Implications of Blockchaining the Internet of Things (August 15, 2017). 45th TPRC Internet, Information and Communication Policy Conference, September 8-9, 2017, George Mason University Law School, Arlington, VA,

List of Figures

Abstract

Blockchain or distributed ledger technology is the key innovation inside Bitcoin, the virtual currency, or distributed database commodity. Distributed ledger applications are presently in experimental and early commercial use in applications and for industry sectors now extending far beyond Bitcoin, and far beyond Fintech (financial technology.)

This paper evaluates blockchain technology and suggests there is a significant opportunity for regulators and policymakers to shape the evolution and commercialization of this disruptive trust innovation, particularly for the Internet of Things, in a direction that contributes to human well-being. Designing for privacy and security are just two of the policy issues that must be rethought as blockchain technology gains widespread use.

As blockchain is increasingly used to establish secure trust relationships and permanent records in a wide array of markets and institutions, will the diverse regulatory treatments of – essentially the same – innovation create new policy barriers to its wide application? Are there information policy measures, which can help policymakers, industry, and users avoid the inevitable pitfalls of a novel technology? If so, is there a new alignment of distribution of authority also among regulators, which these innovations may spark, or public welfare and public sector effectiveness might benefit from?

This paper summarizes original research by the co-authors, and is among the first to deconstruct blockchain for a wide array of industrial sectors and Internet of Things markets. Preliminary results and insights on three policy challenges are shared. Suggestions for further cross-sector blockchain and Internet of Things policy research conclude the paper.

Introduction

Technology paradigms and models that are significantly influencing industry and society in parallel may virtually intersect. Two technologies that are both accelerating, and are now converging, will create an overlap and generate uncertainty that requires further research. These two technologies are blockchain and the internet of things. The path dependency from which we may anticipate this impending collision of technologies and business models can create opportunities for firms, and challenges for government and civil society.

Blockchain is a distributed trust protocol that builds on encryption and distributed immutable ledgers to drive information sharing between unfamiliar parties in an intimate way without having to manufacture trust with intermediaries or complex infrastructure. This can accelerate the sharing of new types of data between new categories of parties in new ways, like never before in the history of our species.[1]

The internet of things includes the sensor instrumentation of non-digital assets that create digital endpoints in an electronic network enabling the capture of new types of information, about new things that we never captured information on, at low cost and high speed; ready to be shared. This can accelerate our ability to see and learn about the world from de-materialize view. More broadly, the internet of things includes all the sensors and digital assets already in, on and around us, such as the wearables, drones, cameras, microphones, GPS and radios already embedded in our environment. Now in the internet of things their data might be more readily aggregated and analyzed, which has both positive and negative externalities.

Together, these two paradigms create the potential for new data sets collected by sensors on items of the world that were never sensored, and to store said data on blockchains which facilitate easy and trusted exchange of information between unfamiliar parties in an intimate way. This form of co-operation between humans to create and capture value is termed *trusted commerce*.[2] While there are already emergent policies and regulatory approaches to aspects of blockchain and the internet of things individually, there is a policy gap at the intersection that requires immediate and focused research and policy consideration. [3]

---

[1] For more on the role of technology in the history of human well-being providing an empirical basis for this observation, see Audrey N. Selian, Lee McKnight, (2017) *The Role of Technology in the History of Well-Being: Transformative Market Phenomena Over Time*, in Richard J. Estes, M. Joseph Sirgy, Eds., (2017) *The Pursuit of Human Well-Being. The Untold Global History*, Springer International Publishing, pp 639-687.

[2] For more on the emergence of trusted commerce, see Richie Etwaru, (2017) *Blockchain: Trust Companies. Every Company Is at Risk of Being Disrupted by a Digital Version of Itself*, Dog Ear Press.

[3] The New York State Department of Financial Services BitLicense Regulatory Framework from 2015 is an example of early regulation a virtual currency application of blockchain. This provides a model for regulators elsewhere to follow for virtual currency. For more information see: New York State Department of Financial Services, Bitlicense Regulatory Framework: http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm See also: New York State Department of Financial Services, New York Codes, Rules and Regulations Title 23. Department of Financial Services Chapter I. Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf

What is blockchain?

Blockchain is the combination of asymmetric cryptography and distributed databases arranged in a manner to ensure that data can be stored presented in a form where it is simple and inexpensive to tell if the data was tampered with, by whom, when, and in some cases for what reason. Famously, the blockchain protocol of cryptography and distributed databases is the underlying fabric for Bitcoin and other digital crypto currencies. Bitcoin is blockchain instantiated for currency, a single use case.[4]

The blockchain protocol stands to be more powerful than its first instantiation Bitcoin. To help frame the magnitude of the blockchain protocol versus Bitcoin, some suggest the metaphor suggesting Bitcoin is to blockchain what AOL Chat was to the Internet. A small example of how the TCP/IP protocol can be used for a simple use case such as Chat. The fundamental promise is that data that can be presented by itself, with the ability to be check for tampering is data that is more trusted than a data set that cannot be easily checked for tampering. As a result, data on a blockchain is more trusted than data not on a blockchain, and hence the need for intermediaries that manufacture trust in data sets such as banks for financial data, department of motor vehicles for identity data, title companies for ownership land and property data are less needed.

Where is blockchain going next?

Early applications of the blockchain protocol have gone beyond representing currency or financial data, the industry has started to add identity data, and in some cases inventory data to the blockchain protocol. The maturity model below illustrates a potential adoption journey for blockchain on data sets, starting with trusted data expanding to other data sets beyond financial data, and eventually the implications when consensus can be found easier on truths represented in data sets, and finally the ability to have human or software agents act on data sets autonomously with smart contracts.

Figure 1: Blockchain Institutional Revolution Maturity Model

	Finance Data	Identity Data	Reputation Data	Inventory Data	Market Data	Agreement Data	Cooperate Data
TRUST	1A	2A	3A	4A	5A	6A	7A
CONSENSUS	2A	3B	3B	4B	5B	6B	7B
AUTONOMY	3A	4C	3C	4C	5C	6C	7C

(Source: R. Etwaru, 2017)

[4] For the original work describing Bitcoin, and the Blockchain, see Satoshi Nakomoto, 2009, *Bitcoin: A Peer-to-Peer Electronic Cash System,* https://bitcoin.org/bitcoin.pdf

Bitcoin is in cell 1A above, an instantiation of the ease at which financial data can be shared between unfamiliar parties in an intimate way without the high dependence on an intermediary such as a bank. Other trust use cases extended from cell 2a to 7A and will be discussed later in the paper. Cell 7C represents a use case where corporate data representing how a corporation organizes, governs, make decisions and distributes value are trusted by design without the need for corporate auditors, corporate lawyers, and accounting governance bodies. This trusted corporate data when share with unfamiliar parties in an intimate way is currently being referred to as a Decentralized Autonomous Organization (DAO).

At the core of blockchain is the notion that data can be presented in a manner where it can be trusted as a standalone without the need for an intermediary to verify the fidelity of the data. This notion of Blockchain, first drives sharing of new types of data sets never imagined as shareable before because of the high cost of standing up an intermediary to verify the fidelity of said data set between familiar parties. Secondly, the notion drives sharing between unfamiliar parties in intimate ways, which could not have been attempted before because of the high cost of standing up said familiarity.

What is the internet of things?

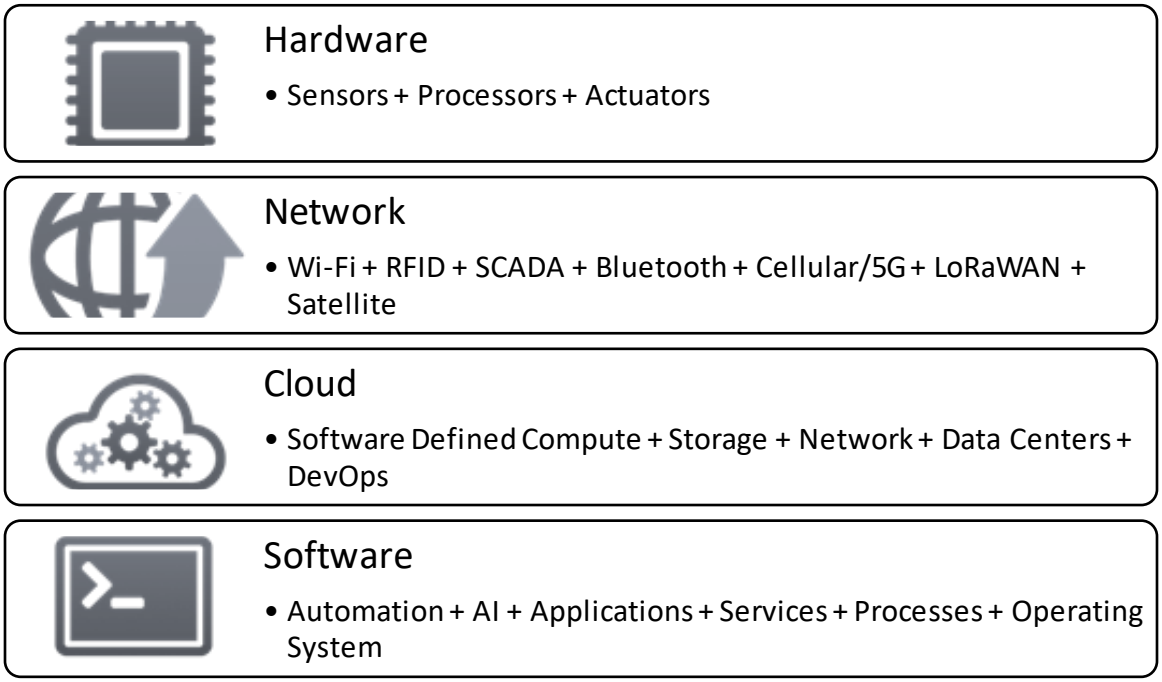
The internet of things, often referred to as IoT or IoE (the internet of everything) is a paradigm that encapsulates hardware, software, and networking enabling our species to instrument animate or inanimate objects with "sensors" that are connected to the internet enabling these sensors to collect data streams about the animate or inanimate or the environment around the animate or inanimate objects, and report said data streams back to a centralized location via the internet.[5] Examples of the internet of things instantiated are thermostats that are connected to the internet remotely reporting to a user's mobile phone the temperature of the user's home, or sensors on oil rigs that are remotely reporting as a constant stream of data the speed and direction of the movement of the water/ocean around the oil rig back to a central location on land via the intent to a computer screen.

This ability to manufacture sensors that can measure specific attributes of animate or inanimate objects or the environment around animate or inanimate objects, connect these sensors to the internet so that they can remotely report single points in time measures or constant streams of data back to other animate or inanimate objects, databases, computers, or mobile devices describes the "instrumenting" of the world with sensors. With enough instrumentation, once heavily analog and material intensive sectors or industries can be de-materialize and/or digitized create conditions where commerce can run faster on real time

[5] For a recent technology assessment of the Internet of Things, see United States Government Accountability Office, Center for Science, Technology, and Engineering Report to Congressional Requesters, (May 2017) GAO-17-75, *TECHNOLOGY ASSESSMENT Internet of Things Status and implications of an increasingly connected world* http://www.gao.gov/assets/690/684590.pdf (Note: co-author Lee W McKnight served as a contributor to the National Research Council workshop and as a reviewer and commenter on the draft report.

higher fidelity demand and supply signals garnered from the internet of things. To visualize the elements of Internet of Things Devices, Systems, and Services, see Figure 2 below.

Figure 2: The Internet of Things Deconstructed



(Source: Lee W McKnight, adapted from USGAO 17-75)

As Figure 2 above illustrates, depending upon whether one is focusing on the Industrial Internet of Things, or taking a consumer, device, network, cloud or software focus to the Internet of Things, a number of different elements can be emphasized. Similarly, in modern systems the traditional hardware process of 'compute' can be defined in software, as can the network and storage as well as the data. What remains constant is some form of physical sensors must be present.

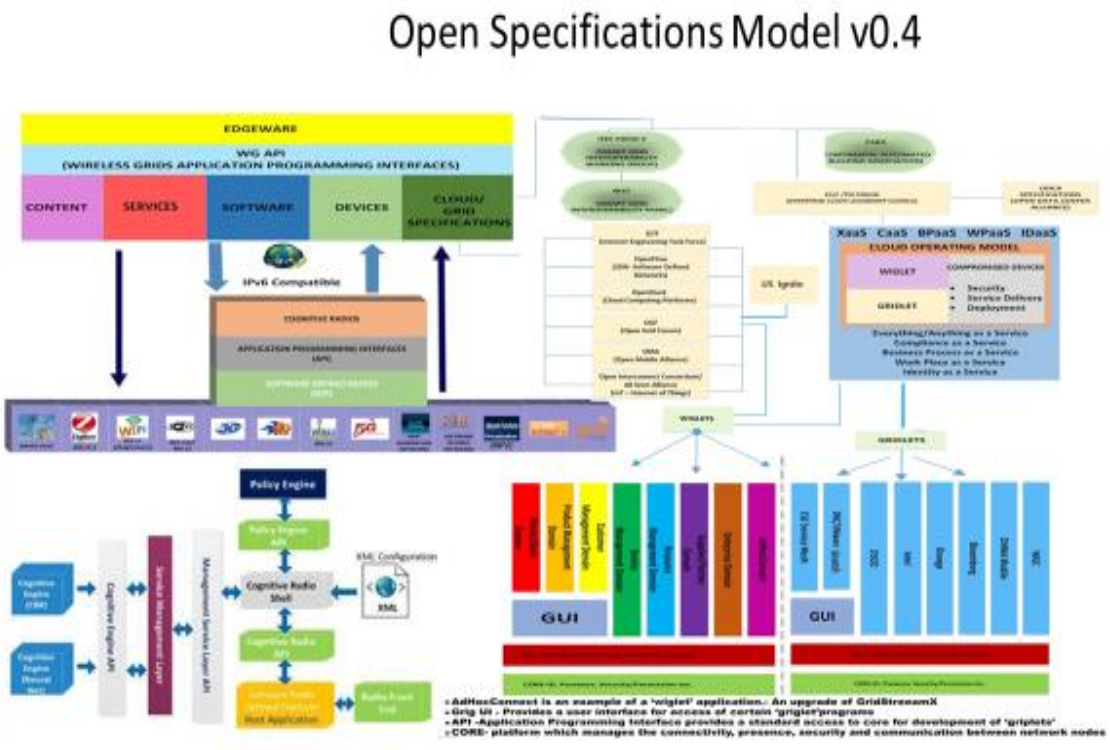
Where is the internet of things going next?

Currently, the internet of things is helping commerce collect new datasets that may not have been collected at scale before, and putting those data sets to use. The fidelity of the new datasets, the usefulness of the data, and the ability of once non-connected and non-smart things to become connected and smart is an evolution. Adding a sensor to a thermostat into a home to be able to report back the temperature of the home to a user's mobile phone

remotely via an internet connect does not make the thermostat a smart thermostat, or the home a smart home.

Human and cyber-physical systems are always vulnerable to a variety of threats, with the Internet of Things expanding the threat surface enormously and creating an unknown number of new risk factors. When coupled with the human failures and lack of security awareness and training, Zero Day Exploits and other embedded system vulnerabilities, a new approach is needed. An Open Specifications Model has been developed around a 2-part cyber-physical kernel by researchers and students from many nations in part through several National Science Foundation Partnership for Innovation projects. The work began in 2002 as exploratory research on what we now call the Internet of Things, cloud services, Edgeware, and soon will call 5G+ advanced wireless networks. Nine doctoral theses have been authored and thousands of academic and industry researchers, school teachers and schoolchildren, as well as Enterprise CIOs, government and civil society members, have contributed to date in various ways including to academic and professional conferences, publications and journal articles, and standards, reference architecture, and framework specification organizations.

Figure 3: Open Specifications Model v0.4 for the Internet of Things



Source: WiTec, Syracuse University, 2016

As the Open Specifications Model illustrates (and suggests edgeware architecture to protect people, devices, networks, applications. data, content and services, and non-person entities,

including edge networks and edge computing devices, and edge cloud services are being instrumented with sensors that are moving through a maturity model. The smartness of the object instrumented with sensors is on a scale. We believe that the internet of things will mature in a direction where data sets that are more new will be collected/streamed remotely over the internet, the fidelity of the new data sets will increase and sensors become more sensitive and scalable, and the smartness of the devices instrumented with sensors will increase over time to an internet of smart things.

The Open Specifications Model v0.5 now in development has many technical mechanisms, as well as law, policy and economic elements and features; and is far from complete, and must continually evolve as for example blockchain and Internet of Things were added to v0.4. The virtual market questions stimulating the research originally reviews the insights from the 'cloud to edge' focus of the current phase and suggests directions for future Edgeware research and development. Innovation Zones in Democratic Republic of Congo and testbeds in the United States permitting evaluation of Edgeware and the Internet Backpack for emergency and education use are described in other work also prepared for presentation at TPRC 45.[6]

Figure 4: Internet of things maturity model

	Internet of dumb things	Internet of chatty things	Internet of obedient things	Internet of useful things	Internet of smart things
WHAT CAN THEY DO	Things that are connected digitally	Things that can have conversations	Things that can execute instructions	Things that can report or trigger events	Things that can engage and add value
WHAT DOES IT FEEL LIKE	Light sensor can only report back absence or presence of light	Camera connected to a tall building	Controller that can change the temperature in a house	Sensor in trunk of car that hears from your calendar that you are driving to your golf game, nut notices the golf clubs are not in the trunk	Sensor on mattress or bedroom to know that a person did not have enough rest at night
WHAT IS AN EXAMPLE	Sensor to see if a light is on or off	Lens that can report back remotely what it sees	Thermostat that can be told to change the temperature in a house	Network of sensors verifies that golf clubs are still in the garage, and orders and pickup service to bring your golf clubs to the course	Sensor communicates with person's admin and calendar, moves an early 7AM meeting to 8AM, and informs alarm clock to allow human one more hour of much needed sleep

[6] See www.iatag.org and Lee W McKnight, Katcho Karume, and Yihan Yu, '*Getting There from Here; The 30 in 2020 Broadband Vision for the Democratic Republic of Congo*, Paper prepared for TPRC 45, September 8-9, 2017, www.tprc.org

What does the intersection of the two paradigms look like?

New sensors that instrument animate objects range from thermostats at bottom of the ocean, to accelerometers in the body of a human being to track motion and balance. These sensors are increasingly being "connected" to digital networks such as the Internet via increasingly faster and cheaper connectivity protocols creating a tsunami of new data being captured and stored. These new data streams stored into data sets are being used by a small number of guardians of said data, for a small number of evolutionary reasons.

New data sets in addition to financial data are being loaded onto blockchain distribute ledgers for intimate data sharing between new networks of participants who are historically unfamiliar with each other's. A data set such as the motion and balance of the human body collected by an accelerometer instrumented in a patient is currently stored in an IoT database, and only accessible by permitted and visible/known guardians of said data set. When this human motion and balance data set is loaded on a blockchain where sharing between unfamiliar parties is the status quo, new research and implications are needed around how sensitive data once "guarded" by a trusted guardian is now in a world where trust is commoditized and sharing is democratized.

At the intersection of blockchain and the internet of things - or as the title of the paper suggests blockchaining the internet of things – are use cases where new datasets being collected from new sensors lack a clear policy on how guardians can use them.

The complexity of the use cases increases when said new datasets are loaded on a blockchain where there is limited policy around how sharing can be done beyond the initial guardians of the datasets to unfamiliar parties in intimate ways. Currently, while intermediaries such as banks for financial data stand in the way as they verify the sanctity of a data set, they also serve as the mechanism that throttles access to data sets. On a Blockchain where permission is designed for, the mere ease of sharing without a need for an intermediary to verify data because the fidelity of a data set is inherently built into the data set creates conditions where the temptation to share at scale with parties who lack the appropriate permission needs policy guidance.

Finally, the uses cases saturate with complexity where once guarded datasets are now shared at scale with unfamiliar parties in intimate ways to generate new insights with little or no policy considerations around how, when, where, for what and by whom said insights can be leveraged.

Figure 5: Blockchain/IoT Opportunities and Policy Issues

	Status of current policies	Difficulty of constructing policy	Impact of lack of policy
New datasets captured in the internet of things.	Some	Easy	Low
New datasets captured in the internet of things + loaded on a blockchain so unfamiliar parties can access in intimate ways	Little	Medium	High
New datasets captured in the internet of things + loaded on a blockchain so unfamiliar parties can access in intimate ways + new insights can be derived by combining non-adjacent datasets	None	High	High

Healthcare use case

Fitness tracker is a part of the internet of things, specifically; they contribute to the emergent digital health aspect of healthcare. The information captured by fitness trackers is currently not regulated by the FDA and the devices are considered a DTC lifestyle category device. Most of the data captured from fitness trackers belong to the guardian who is the person being tracked. While there are some guidelines on what the corporations that manufacture the fitness trackers can do with the data sets, the policies fail to address how parts of the fitness tracking datasets can be stored on blockchains where sharing is democratized.

Once fitness tracker datasets are loaded on a blockchain where the datasets can be shared with other adjacent participants on the blockchain such as gyms, health insurance companies, and sporting goods apparel stores; the low cost of access and sharing of the high fidelity data in the absence of clear policy can potentially encourage a behavior where the data is shared beyond the realms of consideration of current policy sets. A sporting apparel store, for example, may now be able to target specific customers who have purchased fitness tracker devices with advertisement for fitness apparel, or a health insurance company may potentially consider into the actuarial process the evidence that one insured is running and hence a lower health risk over another insured who is not running and hence a higher health risk.

Lastly, on a blockchain where other permitted parties such as border control agencies are sharing on the same distributed ledger, information on where a traveler has been running or travelling captured from the GPS sensor on a fitness tracker can create conditions where border agents can evaluate the threat of a person entering a country or a region in real time based on the prior travels or visits to countries or cities infected with threats. While this example creates opportunity in keeping the world safe, there are policy considerations in privacy and human rights, that are currently not in the focus of the debate around blockchain and the internet of things as they intersect on this simple data set.

Automotive use case

The automobile is the poster child of once inanimate objects now being dematerialized with sensors into the internet of things. Cars can now see, hear, respond, and recommend increasingly faster and more precisely. A network of loosely defined policies governs the ownership and attribution or returned value from the data collected and generated from cars. The movement of a car for example, when pooled with the movement of other cars can create live traffic data streams that optimized GPS routing. The cameras that modern cars are equipped with can/should be able to spot potholes and report them to local authorities, and the voice commands asked/told to cars by drivers can/should be used to drive the improvement of natural language processing or at a minimum capture demand signals of what drivers want from cars, i.e. early demand signals of what humans expect cars to understand.

As the internet of things accelerates the ability for new and improved data streams to be collected from and by automobiles, the policy around the ownership and attribution of returned value from said data sets are falling behind. Once on a blockchain, these data sets will continue to be leveraged by first the sharing to unfamiliar parties and eventually merged with other datasets on blockchains to driven new and interesting insights of value. For example, the number of potholes discovered and reported by a car may qualify that car for access to preferred HOV lanes when there is congestion.

What is visibly clear, and requires the focus to fashion policy around is the ownership of these new data sets, and the ability to attribute derived value back to the systems or individuals that create the data sets initially. Here we see data sets that are loosely owned by the originators used in an evolutionary way creating little-returned value that has to be attributed back to the originator. As these data sets begin to evolve and be shared at scale on blockchains, the derived value resulting from the datasets will likely increase exponentially and as a result the need for focus on policy that governs the ownership and attribution of returned value back to the originators of data sets derived from cars owned by a human, or a human herself needs to be studied further.

An Oil and Gas use case

The oil and gas industry has shifted from surveying the planet at single points in time to sensoring the planet as a continuous stream of information. Data sets on air pressure, temperature, wind, the density of land or water, the sounds of the ocean, and the shifts of the tectonic plates underpinning volcanoes are increasingly being captured by sensors that are a part of the internet of things.

Some of these datasets represent a significant commercial opportunity to identify and sequence the harvesting of the planted natural resources. As these data sets begin to be added onto Blockchains, and as a result, they are shared beyond the traditional intended parties and

countries whose mal intent are unfamiliar to those installing these innocent sensors. We are moving into new territory in the relationship between mankind and the planet. For some, new data sets of the planet stemming from the increased sensoring installed by the oil and gas industry represent commercial opportunity, for others, it represents implications of national security.

In such use cases, it is not only important to consider policy in how data sets may be used as in the healthcare use case above, or how may the ownership and attribution of value derived from new shared data sets as in the automotive use case above; here we see the debate around who should have access to certain data sets where those with mal intent can affect national security, or which data sets should be accessible to all in an effort to level the playing field.

The lack of trust driven by limited policy governing how these new data sets described in this use cases are shared with unfamiliar parties in an intimate way stands in the way of similar use cases being realized to form the next generation human co-operation termed trusted commerce.

Three Blockchain + IoT Policy Challenges

The core of the need for policy consideration stems from the exponential sharing of new information to unusual parties in an intimate way that is prompted at the intersection of blockchain and the internet of things.

Figure 6: Three challenges at the intersection of blockchain and the internet of things

	Time before the policy gap has material implications	Implications of risks to industry	Implications of risks to government
How is permission to share data determined and governed	Immediately	low	high
Who owns the data and how is derived value attributed back to owners	Five years	Medium	High
Who has access to which data sets, and which data sets should always be accessible to all	Ten years	High	High

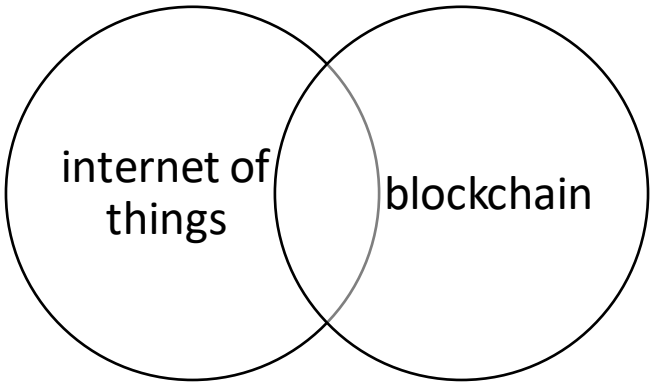
Studies to improve trusted commerce policy efficacy

Studying both paradigms concurrently

Both blockchain and the internet of things have an increasing number of specialists and experts in each of the fields. However, there are few specialists and experts that presently studying the implications and implementations at the intersection of both paradigms. The policy gap discussed is emerging at the intersection where new data sets are collected by sensors in the internet of things and shared in an unprecedented manner to unfamiliar parties in intimate ways on a blockchain.

Our initial research suggests that experts attempting to examine the policy gap should be specialized in both the internet of things and blockchain. Good candidates for policy introspection at the intersection of the two paradigms should understand cryptography, distributed databases, byzantine fault tolerance, sensor hardware, data transfer protocols, and the landscape of current policies in the area of data privacy, open data, and emergent data ownership self-regulatory bodies.

Figure 7. Individuals with skills in both paradigms



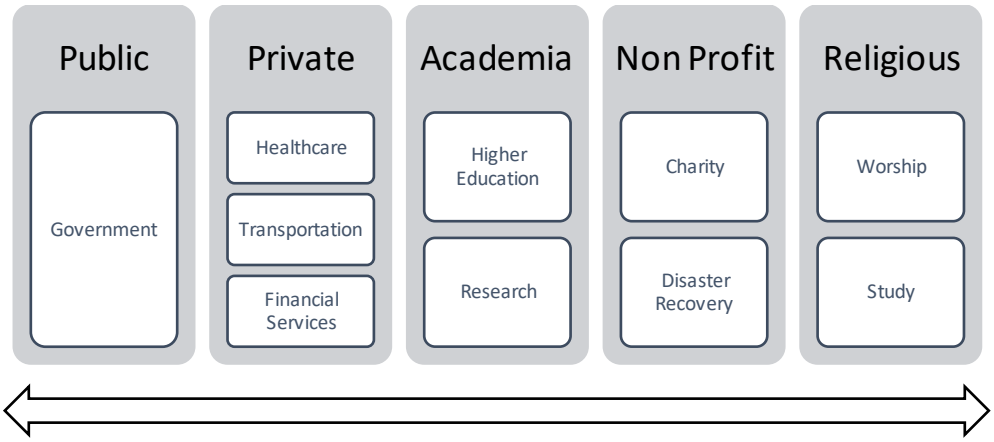
Studying the use cases in multiple sectors and industries

The use cases where the internet of things and blockchain intersect span multiple sectors and industries. In most use cases where the two paradigms intersect multiple industries of the private sector are involved, and in some cases, various parts of the public sector and governments can be involved, and lastly in some rare cases academia and religious organizations can be affected or stand to benefit.

Because of the wide reaching horizontal nature of both of these paradigms ranging from the internet of things enabling the collection of new data sets such as GPS data or the pitch of the

sound of whales at the bottom of the ocean, and the reach of democratized sharing on blockchains from sharing with unknown parties that are trusted by unknown parties with unknown trust profiles; the impact of the intersection of the paradigms can span the public and private sectors a multiple industries with a simple use case.

Figure 8. Use cases span sectors and industries



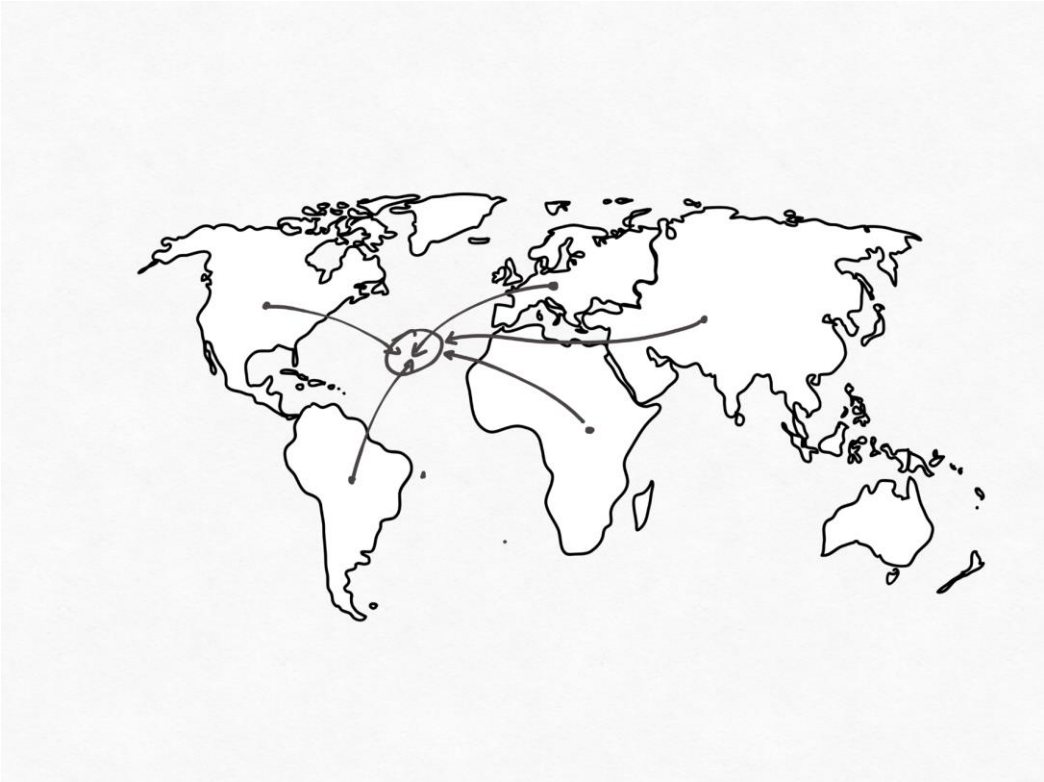
Studying beyond the sovereign boundaries

The internet fueled the blurring of policy lines across sovereign boundaries in the area of data and technology. Sensors in the internet of things instrumented on the human body, or on airplanes, submarines, cruise ships, or have long range visibility or scanning technologies can collect new data sets far beyond the sovereign boundaries of the owner or guardian of the sensor.

When the new data sets that are collected across sovereign boundaries are stored on Blockchains where participants on a Blockchain can be domiciled within different sovereign boundaries, we arrive at a matrix or confluence of different sovereign policies that may need to be arbitrated.

This intersection of two paradigms that show exponential growth and adoption potential across sovereign boundaries at unprecedented rates create an expanding policy gap that continues to overlap into a matrix potential conflicting prior policies and warrants particular considering for new policies.

Figure 9. Blockchain/IoT Policies cross boundaries



Trusted Commerce Recommendations

The intersection of the internet of things and blockchain stand to represent opportunity or challenge for any nation to take advantage of the byproduct of both paradigms converging. The results of the converging paradigms is a state of commerce that is driven by digital demand and supply signals shared at the global scale on industrial strength trusted blockchains. This state of commerce is described as Trusted Commerce, consisting of trust companies and/or organizations.

The United States of America should take a leadership role, design the approach, and facilitate the consideration and focus needed to close this emergent policy gap and accelerate the emergence of the next generation of creation and coordination by humans who co-operate in a network called trusted commerce.

The recommendation is to work through the XYZ office, and the ABC office of the Government of the United States of America, in partnership with the XYZ existing world organization, and the ABC existing self-regulatory body to pull together individuals that (1) understand both the internet of things and blockchain paradigm, (2) scholars and practitioners from multiple sectors and industries, and (3) internet, data, privacy, and national security policy experts from the G20

into a "Trusted Commerce Working Group" (TCWG). The TCWG would be tasked with publishing a framework and roadmap for a policy campaign to pave the way for trusted commerce to become a reality.

Our three policy recommendations for developing policy for blockchaining the Internet of Things are:

1) a Blockchain IoT Trusted Commerce Commission or Working Group, perhaps organized by the National Research Council of the National Academies of Science, Engineering, and Mathematics, and including both academic and industry experts, Congressional staff (GAO), and Executive Branch Agency and Regulatory staff, should be convened as soon as practicable;

2) A Symposium or Workshop should be convened as soon as is practicable to gather broader input following a preliminary review of obstacles and opportunities for enhanced public sector efficiency and public safety, and reduced regulatory uncertainty; at the intersection of Blockchain and IoT. Among the key outputs of the Working Group and the Event would be:

3) Recommendations for implementation of regulatory convergence and policy process automation with information assurance through Blockchain for the Internet of Things.

Conclusion

Our research indicates that both the internet of things and blockchain continues to mature to a state of adoption which will impact the state of commerce and the human experience. Additionally, early indicators in adoption and cross paradigms use cases suggest that the paradigms are reflectively accelerating each other. Throughout our initial research, what is becoming clear is that the amount of cross-paradigm use cases at the intersection of blockchain and the internet of things will potentially grow exponentially at a scale of 10 to 100 times single paradigm use cases.

The use cases at the core of the intersection of the of the two paradigms demonstrate a dominant trait around trust. Because of the immutability of distributed ledgers facilitated by key management and cryptography trust is increasing in the activity to share data, and the dependency on intermediaries to broker the sharing of data is declining. We are beginning to agree with the conclusion of others that this increase in transaction trust will give rise to a new generation of supply chains and value exchange markets as humans co-operate to create and capture value referred to as Trusted Commerce.

As the three uses cases illustrated in this paper suggest, Trusted Commerce creates new experiences and services for humanity that spans across the internet of things and blockchain, sectors and industries, and in some cases sovereignties. As prior research has demonstrated, consumers value trust in transactions, and as a result we believe that consumers will migrate to

organizations that run on Trusted Commerce platforms will and away from current commerce platforms where transparency is low, distrust is high, and inefficiencies in time, cost, and experience created by the need for intermediaries are abundant.

Because of the velocity and volume of the cross-paradigm use cases that are emerging, we have concluded that considering policies at this time is of paramount importance.

References

Aitzhan, N., Svetinovic, D., (2016) Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams –IEEE Transactions on Dependable and Secure Computing, IEEE Xplore Document. (n.d.). Retrieved August 15, 2017, from http://ieeexplore.ieee.org/abstract/document/7589035/

Christidis, K., Devetsikiotis, M., (2016) Blockchains and Smart Contracts for the Internet of Things, - IEEE Xplore Document, pp. 2292-2303, (n.d.). ISSN: 2169-3536 DOI: 10.1109/ACCESS.2016.2566339 Retrieved August 15, 2017, from http://ieeexplore.ieee.org/abstract/document/7467408/ IEEE Access

Clozel, L., Macheel, T., J (August 3, 2016), Did Regulatory Meddling Cause Bitfinex Hack? Retrieved August 15, 2017, from https://www.americanbanker.com/news/did-regulatory-meddling-cause-bitfinex-hack

Collomb, Alexis; Sok, Klara. Blockchain / Distributed Ledger Technology (DLT): What Impact on the Financial Sector? Communications & Strategies; Montpellier 103 (Third Quarter 2016): 93-111,212,214. - ProQuest. (n.d.). Retrieved August 15, 2017, from https://search.proquest.com/openview/b5b5fa49be78d9d574a4c20bc94fc42f/1?pq-origsite=gscholar&cbl=616298

Etwaru, R., (2017) Blockchain: Trust Companies. Every Company Is at Risk of Being Disrupted by a Digital Version of Itself, Dog Ear Press, ISBN-10: 1457556626; ISBN-13: 978-1457556623

Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of Things, Blockchain and Shared Economy Applications. *Procedia Computer Science*, *98*, 461–466. https://doi.org/10.1016/j.procs.2016.09.074

Lehrman, N., (2017) Open Specifications v0.4 – Ethereum: A Platform for Decentralized Applications, in: Lee W. McKnight, Ed., (2017) Open Specifications Model v.04 for Wireless Grids in the Internet of Things, Syracuse University WiTec

McKnight, L. W. (2018) Blockchained Markets and Wireless Grids in the Internet of Things, World Scientific Press, in press

McKnight, L. W. Ed., (2017) Open Specifications Model v.04 for Wireless Grids in the Internet of Things, Syracuse University WiTec

Nakamoto, S., (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. (n.d.). Retrieved August 15, 2017, from https://bitcoin.org/en/bitcoin-paper

New York State Department of Financial Services (2015) New York Codes, Rules and Regulations Title 23. Department of Financial Services Chapter I. Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf

NYSDFS: Final BitLicense Regulatory Framework. (n.d.). Retrieved August 15, 2017, from http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm

Parker, L., (2017, April 1). Bitcoin regulation overhaul in Japan » Brave New Coin. Retrieved August 15, 2017, from https://bravenewcoin.com/news/bitcoin-regulation-overhaul-in-japan/

Selian, A. N., & McKnight, L. (2017). The Role of Technology in the History of Well-Being: Transformative Market Phenomena Over Time. In *The Pursuit of Human Well-Being* (pp. 639–687). Springer, Cham. https://doi.org/10.1007/978-3-319-39101-4_19

Underwood, S. (2016). Blockchain Beyond Bitcoin. *Commun. ACM*, *59*(11), 15–17. https://doi.org/10.1145/2994581

United States Government Accountability Office, (May 2017) Center for Science, Technology, and Engineering Report to Congressional Requesters, GAO-17-75, TECHNOLOGY ASSESSMENT Internet of Things Status and implications of an increasingly connected world. http://www.gao.gov/assets/690/684590.pdf

Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., Kishigami, J. (Oct. 2015) Blockchain contract: A complete consensus using blockchain – 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE) IEEE Xplore Document. (n.d.). Retrieved August 15, 2017, from http://ieeexplore.ieee.org/abstract/document/7398721/

Zurcher, B., et.al. Device management with Azure IoT Hub. Retrieved August 15, 2017, from https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-device-management-overview

Werbach, K. D., Trustless Trust (August 8, 2016). TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016. Available at SSRN: https://ssrn.com/abstract=2757380

About the Authors

Lee W. McKnight is an Associate Professor in the Syracuse University iSchool (School of Information Studies), an Affiliate of Syracuse University's Institute for National Security and Counterterrorism (INSTC), and lectures annually at MIT since 1998. Lee was Principal Investigator of the National Science Foundation Partnerships for Innovation Wireless Grids Innovation Testbed (WiGiT) project 2009-2014, which was recipient of the 2011 TACNY Award for Technology Project of Year. Lee is inventor of edgeware, a new class of software for creating secure ad hoc overlay cloud to edge applications. Lee's research focuses on cloud management of dynamic edge services, virtual markets and wireless grids, and Internet governance. McKnight teaches graduate and undergraduate courses such as Blockchain Management, Cloud Architecture, Cloud Management, Information Security Policy (joint with Syracuse Law School/INSCT), and Information Policy at Syracuse University, and lectures annually in the MIT Professional Education short course, 'Technology, Organizations, and Innovation: Putting Ideas to Work.' In addition to many peer reviewed journal articles in technical and policy journals; his academic work includes several path-breaking books. McKnight received a Ph.D. in 1989 from MIT; an M.A. from the School of Advanced International Studies, Johns Hopkins University in 1981; and a B.A. magna cum laude from Tufts University in 1978.

Richie Etwaru is an Adjunct Professor with the Syracuse University iSchool; and is Chief Digital Officer of QuintilesIMS www.quintilesims.com, and author of *Blockchain Trust Companies*. (Dog Ear Press, 2017) Previously, Richie was with the Office of the CIO, UBS.

Yihan Yu is a graduate student in the Syracuse University Newhouse School, is affiliated with Syracuse University WiTec (Worldwide Innovation Technology and Entrepreneurship Club), and a 2016 M.S. in Information Management graduate of the Syracuse University School of Information Studies.