Telecommunications Policy xxx (2017) 1–12

Contents lists available at ScienceDirect

Telecommunications Policy

journal homepage: www.elsevier.com/locate/telpol

Blockchain's roles in strengthening cybersecurity and protecting privacy

Nir Kshetri

Bryan School of Business and Economics, The University of North Carolina at Greensboro, Bryan Building, Room: 368, P. O. Box 26165, Greensboro, NC 27402-6165, USA

ARTICLE INFO

Keywords:
Blockchain
Cloud computing
Cybersecurity
Internet of things
Privacy
Supply chain

ABSTRACT

This paper evaluates blockchain's roles in strengthening cybersecurity and protecting privacy. Since most of the data is currently stored in cloud data centers, it also compares how blockchain performs vis-vis the cloud in various aspects of security and privacy. Key underlying mechanisms related to the blockchain's impacts on the Internet of Things (IoT) security are also covered. From the security and privacy considerations, it highlights how blockchain-based solutions could possibly be, in many aspects, superior to the current IoT ecosystem, which mainly relies on centralized cloud servers through service providers. Using practical applications and real-world examples, the paper argues that blockchain's decentralized feature is likely to result in a low susceptibility to manipulation and forgery by malicious participants. Special consideration is also given to how blockchain-based identity and access management systems can address some of the key challenges associated with IoT security. The paper provides a detailed analysis and description of blockchain's roles in tracking the sources of insecurity in supply chains related to IoT devices. The paper also delves into how blockchain can make it possible to contain an IoT security breach in a targeted way after it is discovered. It discusses and evaluates initiatives of organizations, inter-organizational networks and industries on this front. A number of policy implications are discussed. First, in order to strengthen IoT, regulators can make it obligatory for firms to deploy blockchain in supply chain, especially in systems that are mission critical, and have substantial national security and economic benefits. Second, public policy efforts directed at protecting privacy using blockchain should focus on providing training to key stakeholders and increasing investment in this technology. Third, one way to enrich the blockchain ecosystem would be to turn attention to public–private partnerships. Finally, national governments should provide legal clarity and more information for parties to engage in smart contracts that are enforceable.

1. Introduction

Blockchain is touted as a technology that can possibly provide a robust and strong cybersecurity solution and high level of privacy protection (Schutzer, 2016). Its proponents argue that this technology is secure by design. In a blockchain model, there is no need to store information with third parties. The records are on many interlocked computers that hold identical information. If one computer's blockchain updates are breached, the system rejects it (Kestenbaum, 2017). In addition, multi-signature (multisig) protection or the requirement of more than one key to authorize a transaction processes can further improve security and privacy.

Even if a hacker penetrates a network and tries to steal money from an account, multiple redundant and identical copies of the same

E-mail address: nbkshetr@uncg.edu.

https://doi.org/10.1016/j.telpol.2017.09.003
Received 30 June 2017; Received in revised form 6 September 2017; Accepted 6 September 2017
Available online xxxx

ledger are stored worldwide. If one is breached, there are many others as backups that can provide the funds in the hacked account (Due.com, 2017). That is, data in blockchain is distributed around many computers that are interlocked. For hacking efforts to be successful, more than 50% of the systems in the network need to be hacked.

We illustrate the above arguments with an example. Consider OpenBazaar, which is a bitcoin-based multi-signature-protected decentralized marketplace, which went live in April 2016 (Higgins, 2016). OpenBazaar claims that it does not store user information. Even if a hacker successfully breaches OpenBazaar database, the private keys of bitcoin wallets cannot be accessed. Moreover, if the hacker gets the user's private key for a bitcoin address, the multi-signature requirement prevents from accessing and moving the funds from the owner's account (Young, 2016).

The security features of many of the important systems across many industries rely on what is known as "security through obscurity" approach in security engineering. The idea in this approach is to keep a system's security mechanisms and implementation secret. However, a major drawback of this method is that the entire system may collapse when someone discovers the security mechanism. One such system arguably is the Society for Worldwide Interbank Financial Telecommunications (SWIFT), which is a secure messaging system used by financial institutions. Some rightly argue that the existing international payment systems such as SWIFT are outdated and of questionable security. For instance, in 2016, the Bangladesh Central Bank lost over $81 million due to unauthorized transactions that were routed through the New York Federal Reserve Bank using the SWIFT network (Tech, 2017). Several banks in Southeast Asia were also suspected to be hacked via the SWIFT system. (Baker, 2017).

The use of blockchain-based systems probably help avoid the attacks such as noted above. There is arguably no single point of failure or vulnerability in blockchain. It is also important to point out that while bitcoin, the most well-known blockchain application, has had a bad public perception regarding security, the hacking attacks occurred only to other systems that attempted to hold and store bitcoin private keys. It is reported that a bitcoin transaction sent from one party to another arguably has not ever been compromised (Coward, 2016).

Now let us consider the issue of privacy protection. Many of the causes that lead to privacy violation in a non-blockchain world are not likely to apply to blockchain. For instance, primary data collection led to most privacy violations in the so called paper age. On the other hand, most of such violations in the cyber age have resulted from secondary usage of information, which has been normally legally collected (Etzioni, 2015). Note that businesses store huge volume of personal data so that potential innovative uses can be discovered. Mayer-Schönberger and Cukier (2013, p. 153) emphasize that "most innovative secondary uses haven't been imagined when the data is first collected" (Mayer-Schönberger & Cukier, 2013). Note too that most consumers are against the secondary uses of their personal data. Moreover, these concerns are linked with the collection and storing of data as well as data sharing and accessibility by third parties and various user types. Additionally, firms may need to outsource to cloud services providers (CSPs) which may give rise to privacy and security issues (Kshetri, 2014). Part of the fascinating character of blockchain stems from the fact that personal data can be seen only with the subject's permission and the data cannot be stored. Proof of identity is stored in a cryptographic format, which makes it impossible or very difficult to compromise (Seth, 2017). Blockchain-based systems can thus be designed to provide a high level of privacy protection. In this regard, secure storage and transmission of digitally signed documents are what industry experts think as the most likely killer application of blockchain. Due primarily to "super audit trail", such applications have already been built and tested in trade finance, shipping, and insurance in order to validate the identity of individuals as well as assets (Mainelli, 2017).

In order to illustrate this point, consider the Canadian identity and authentication provider SecureKey, which has received investments from Canada's big banks including CIBC, BMO, Desjardins, TD, and Scotiabank (Galang, 2017). When the service goes live, consumers that have proven their identity with a bank and a credit agency can possibly give permission to share their data with a third party such as a utility or a phone company to create a new account (Hughes, 2017). To provide a higher level of privacy protection, it plans to limit the actual amount of data being transmitted. Consumers can possibly choose the type of identifying information they want to share with an organization to quickly verify their identities (Galang, 2017). The company's plan is to use a blockchain-based "triple blind" privacy protocol to connect individuals to partnering online services using an existing credential. The "triple blind" mechanism means that consumers can use their bank credentials to log in and access their cellular phone services. The bank cannot see the data's destination and the recipient cannot see the bank used or bank account information. SecureKey, as a middleman, is also "blind" and cannot see information about the user of the services (Ho, 2017).

In light of the above observations, this paper evaluates blockchain from security and privacy considerations. Since most of the data is currently stored in cloud data centers, we also compare how blockchain performs vis-vis the cloud in various aspects of security and privacy. It gives special consideration to some of the key underlying mechanisms related to blockchain's impact on Internet of Things (IoT) security.

Before we proceed further, some caveats regarding blockchain's efficacy in strengthening cybersecurity and protecting privacy are in order. At the outset, it is important to make clear that blockchain currently is in its nascent state. There have not been a large number of DLT- and blockchain-based applications in order to sufficiently evaluate whether this technology is superior to the current system in defending against various sources of cyber-threats. A related point is that assertions regarding blockchain's superiority vis-à-vis current measures in protecting architecture, elements and components of IoT have not been sufficiently empirically researched.

2. A comparison of blockchain and cloud computing from security and privacy considerations

According to Cisco, by 2020, data stored in the cloud data centers will account for 88% total data center storage capacity. The proportion was about 65% in 2015 (Cisco Public, 2016). Thus, it makes sense to compare blockchain and cloud computing from the standpoint of security and privacy.

Some view blockchain and cloud computing as "kissing cousins" in terms of the similarities in the way security and privacy issues are

handled (Bertrand, 2017). Table 1 compares these two technologies in terms of the ways these issues are dealt with. Both the cloud and blockchain are designed to provide cost-efficient security solutions. Cloud's options of private, community and public deployment models can be mapped to permissionless and permissioned chains.

Organizations have realized that a one-size-fits-all approach may not work for cloud adoption. For instance, organizations may have to make decisions concerning combinations of public and private clouds. A public cloud is effective for an organization handling high-transaction/low-security or low data value (e.g., sales force automation). Private cloud model, on the other hand, may be appropriate for enterprises and applications that face significant risk from information exposure such as financial institutions and health care provider or federal agency. For instance, for medical-practice companies dealing with sensitive patient data, which are required to comply with the U.S. Health Insurance Portability and Accountability Act (HIPAA) rules, private cloud may be appropriate (Kshetri, 2013).

In order to meet security, privacy, and other requirements, permissionless and permissioned chains exist in the blockchain world. A permissionless blockchain such as bitcoin is an open platform. Anyone can join. Permissioned blockchains, on the other hand, are restrictive. Access must be granted by some authority (Bussmann, 2017). An example is the supply chain blockchain developed by IBM and the Danish shipping company Maersk. This is a closed group of participants that are known and have permission to participate in the transaction (Groenfeldt, 2017). The idea in the permissioned blockchains is that by controlling access to only trusted users on the platform, developers can avoid problems faced by permissionless chains. For instance, Ethereum is being used in a number of private, permissioned chains in individual projects or in larger consortia such as R3 CEV or Hyperledger Project. (Bussmann, 2017). Moreover, blockchain's ability to target specific members in the value delivery chain, including regulators and auditors deserves mention.

Both the cloud and blockchain arguably have security protection “baked into” them. The data is fully encrypted in both cases. Some cloud services providers (CSPs) follow a so-called “zero trust” model for security. Note that a “zero trust” network is based on the premise that trustworthiness needs to be considered for every single device. This means that if a device is hacked, it does not pose threat to the whole network. A user often has access only to certain things. In order to get access to the entire network, the attackers need to attack multiple devices at once (Armasu, 2015). Some refer to this improved model as “security micro-segmentation” (Tausanovitch, 2016). One example of a company following such a model is Google (Pauli, 2016).

Some CSPs have also create a “cyber risk free zone”. They engage in constant monitoring for suspicious activities and provide real time response (Bertrand, 2017).

In order to understand how security and privacy issues are dealt with in blockchain, we look at a definition of this technology. The Chicago-based intellectual property law firm Marshall Gerstein & Borun LLP (2017) suggests that a minimal definition of blockchain should include the following: “a distributed ledger network using public-key cryptography to cryptographically sign transactions that are stored on a distributed ledger, with the ledger consisting of cryptographically linked blocks of transactions”. The cryptographically linked blocks of transactions form a blockchain. Note that doing something cryptographically or in a cryptographic manner means that mathematical techniques are used for encrypting and decrypting data. Doing this ensures that data is kept private when it is being transmitted or stored electronically.

Most companies secure themselves using firewalls that protect the network. The global enterprise firewall market was estimated at $6.14 billion in 2014, which is expected to reach to $8.14 billion in 2019 (Armasu, 2015). They also deploy other network level security tools. Some high-profile breaches such as cyberattacks on Sony Pictures Entertainment in November 2014 indicate that there are drawbacks associated with such models (Gaudiosi, 2014). Malicious actors can hack into the network through poorly protected, non-patched devices. Cybercriminals also exploit weak login credentials, or use social engineering tools.

Blockchain, however, is not without drawbacks and limitations. Due to blockchain's newness, well-developed security mechanisms do not exist for some systems. There have been some hacking attacks against digital currencies (Lohade, 2017). One estimate suggested

Table 1
A comparison of the cloud and blockchain from security and privacy considerations.

	Cloud	Blockchain
Mechanisms related to efficiency, and cost-effectiveness	Cloud's pay as you go model performs better than legacy system, which entails building capacity by buying more computers, more software and hiring more IT people, facilitates Cloud's efficiency: infrastructure-as-a-service.	Blockchain removes the need for third parties in transactions by creating a distributed record which is possessed and verified by other users.
Deployment models	Private, community and public	Permissionless and permissioned chains to meet security, privacy, and other requirements Also possible to target specific members in the chain such as regulators and auditors
Some mechanisms to strengthen cybersecurity	The data is fully encrypted Create a “cyber risk free zone”: constant monitoring for suspicious activities and real time response (Bertrand, 2017). Some companies (e.g., google) employ “Zero Trust” network: fine-grained control.	The data is fully encrypted Cryptographic hash functions are used. Public-private key cryptography makes sure that the data is received only by the intended recipient.
Some key challenges	Many cloud providers rely on the firewall model, which involves monitoring incoming and outgoing network traffic. Based on a defined set of rules, decisions are made whether to allow or block a specific traffic (CISCO, 2017). Criminals exploit new ways to break such system.	Newness: well-developed security mechanisms have not been developed for some systems. It has not been used and adopted widely enough for a serious test.

that in the average, there are between 15 and 50 defects per 1000 lines of software code. For Ethereum, the blockchain-based distributed computing platform, featuring smart contract functionality, this number is estimated to be at least twice as many. This can be attributed to the immaturity of Ethereum. *Economist* quoted a blogger, who said that Ethereum contracts are "candy for hackers" (The Economist, 2016). In June 2016, a high-profile hacking case that breached The DAO was revealed. Note that The DAO is a decentralized autonomous organization (DAO)[1] launched by a group of Ethereum developers on April 30, 2016. The project had a 28-day funding window. By the end of the funding period, the DAO raised more than $150 million from over 11,000 funders (Siegel, 2016). It was arguably the biggest crowdfunding project undertaken until that time. On June 17, 2016, someone exploited vulnerability in the DAO's code and stole 3.6 million ether from the fund. Depending on whether the total value of the stolen fund is calculated before or after the hack, it ranged from $64 million to $101 million (Ore, 2016).

One concern, as noted above, is that blockchain has not been used and adopted widely enough. This means that it has not yet been seriously tested (Lohade, 2017).

An additional problem of blockchain has been the way blockchain systems are currently being designed. A researcher pointed out that the organizations in most networks run the same code (Knight, 2017). In this regard, a process-based model proposed by Brian Finch of Pillsbury Winthrop Shaw Pittman LLP may provide a helpful perspective from which to view this issue. He recommends to use a risk-based strategy, where risk equals "threat plus vulnerability plus consequences" (Finch, 2014). A threat is a danger related to cyber-attack that has the potential to cause harms. Cyber-vulnerability refers to the degree to which an organization is susceptible to harm from cyber-attacks. The fact that not many "mission-critical bugs" bugs have been found that have caused some major problems indicate that blockchain-based systems are characterized by a low degree of vulnerability. Finally, consequences are the results or effects of cyberattacks. As noted above, since most networks run the same code, if a nefarious entity were to find a vulnerability, the entire system may face adverse consequences.

In sum, due to the various reasons listed earlier, issues such as security, privacy and availability are among the topmost concerns in organizations' cloud adoption decisions rather than the total cost of ownership (Brodkin, 2010; McCreary, 2008). Allen (2011, p. 3) notes: "One of the largest disadvantages of cloud computing revolves around security and confidentiality''. Due primarily to concerns related to security, privacy and confidentiality critics have argued that its perceived costs may outweigh the benefits (Tillery, 2010). Organizations worry about hidden costs associated with security breaches or lawsuits tied to data breach. Businesses and consumers are cautious in using it to store high-value or sensitive data and information (Goodburn & Hill, 2011). It is possible that many of the drawbacks of the cloud can be avoided or minimized by using blockchain.

3. Security and privacy in blockchain: an illustration from the healthcare industry and market

We start this section with a brief description of how blockchain-based systems work in order to ensure the security and privacy of identity and other personal data. Mainelli (2017) has identified three parties in a typical identity document exchange: (1) subject of the identity, which could be an individual or an asset, (2) certifier is often a government agency, an accounting firm, or a credit referencing agency, which notarizes the documents, and (3) inquisitor makes an inquiry on the subject in order to investigate requirements for know-your-customer or to monitor compliance with anti-money laundering policies.

Typically, a blockchain transaction has two distinct ledgers (Mainelli, 2017). A content ledger has the individually encrypted documents. A transaction ledger holds encryption key access to the document folders related to identity, health, academic qualifications and other individual attributes on a series of what is referred to as "key rings" (Mainelli, 2017). Digitally certified documents related to various attributes are put on the subject's key rings by the certifier. The certifier often needs the subject's permission to do so. A law firm, for example, may provide the subject's digitally signed copies of documents that it has notarized. A government agency can provide the subject with a digitally signed copy of her/his driving license. After putting on the blockchain certifiers do not have access to the data. Inquisitors often rely on the data that a trusted third party has stamped (Mainelli, 2017).

Inquisitors can inspect the documents when the subject gives controlled key usage based on smart contracts. The network may restrict the number or timing of inquisitions. All the inquisitions are recorded for the subject. Third parties such as banks and financial institutions, insurance providers and government agencies may get permission to access documents based on a smart-contract framework. Commercial certifiers such as city inspectors, accountants, lawyers and notaries possibly provide indemnities (e.g., insurance of validity or home safety inspections) to inquisitors for a fee (Mainelli, 2017). In this way, documents stored in a blockchain are likely to achieve a high degree of authenticity.

The healthcare industry could serve as an example for a possible role of blockchain in strengthening security and protecting privacy of consumer data. This issue is important because in 2015 alone, data breaches in healthcare exceeded 112 million records (Munro, 2015).

According to Halamka, Lippman and Ekblaw (2017), in a non-blockchain world, healthcare organizations typically follow three models to facilitate interoperability of medical data: push, pull and view. In a push model, medical information is sent from one provider to another (e.g., from an emergency room physician to a primary care doctor). In a pull model, a provider asks another provider about information (e.g., a cardiothoracic surgeon asking with a primary care doctor). Finally, in the view model, a provider looks at another provider's record. For instance, a cardiologist examines a patient's X-ray that has been taken at an urgent care center. A major drawback of all these models is that data is not audited in a standardized way. Moreover, in the push model, if a patient is transferred to a different hospital, the new hospital may not be able to access the data that was "pushed" to the first hospital. The lack of audit trail means that

[1] DAOs are run through smart contracts and do not need centralized management and the direct control of self-interested institutions.

there is no guarantee of data integrity from the point of data generation to the point of data use. In the pull model, consents often occur on an informal and ad hoc basis. The regulations and policies governing the above approach vary greatly across jurisdictions based on, inter alia, local practice, and national privacy policy enforcement.

It is argued that blockchain offers a fourth model that can make it possible to share medical records securely across providers during the lifetime of a patient (Halamka et al., 2017). Blockchain in electronic healthcare records (EHR) avoids adding an organization between the patient and the records. Blockchain does not function as a "new clearing house" or "safe deposit box" for data. Blockchain's time-stamped and programmable ledger allows intelligent control of record access and there is no need to create custom functionality for each EHR vendor. The ledger also includes an audit trail (Halamka et al., 2017). In a blockchain model, whenever a consumer makes a change to her/his data, the change is communicated to the public ledger (Silverman, 2017).

Several initiatives in the private and public sectors have been undertaken and public-private partnerships (PPPs) have been explored in order to develop blockchain-based solutions for the healthcare industry and market. Researchers from MIT Media Lab and Beth Israel Deaconess Medical Center proposed MedRec, which is a blockchain-based decentralized record management system to handle EHRs. MedRec is reported to manage "authentication, confidentiality, accountability and data sharing". Patients possibly access to their medical information across different providers and treatment sites. An immutable log of all transactions involving a patient's information is created and provided to the patient (Ekblaw, Azaria, Halamka, & Lippman, 2016). MedRec does not store patients' health records. The system possibly stores the record's signature on a blockchain. The signature may provide an assurance that the record's unaltered copy is obtained. The patient will decide where the records can travel. In this way, the locus of control is possibly shifted from the institution to the patient. For patients that do not want to manage their data, it may be the case that service organizations may evolve and the patients can delegate the task to them (Halamka et al., 2017).

As an example of a PPP, in February 2017, the Food and Drug Administration (FDA) and IBM Watson Health announced a partnership to investigate the potential of blockchain in healthcare. They signed a two-year agreement. Initial efforts will possibly focus on oncology-related data and blockchain framework to improve public health efforts. Blockchain can enable the collection of data from a variety of sources, and keep an audit trail of transactions. In this way, accountability and transparency can be achieved in a data exchange process. The FDA and IBM believe that blockchain can support the exchange of data from several sources on terms and for purposes that the own approves and agrees. They include EHRs, clinical trials, genomic data and information gathered from new sources, such as mobile devices, wearables and IoT devices. (Health Data Management, 2017).

Despite the above opportunities, healthcare providers may encounter various barriers that may prevent them from moving to a blockchain-based system. The psychological challenges that healthcare organizations face must be recognized and dealt with in order to address concerns related to privacy, security, and integrity of healthcare data. John Halamka, who manages the IT system in Boston's Beth Israel Deaconess Medical Center put the issue this way: "We still have the culture where every health care provider thinks of themselves as the single steward of the data that is deposited in that organization" (Silverman, 2017). It might be difficult to change the culture that had developed in the healthcare and other sectors.

4. Blockchain and IoT security

Prior researchers have noted that especially the blockchain-IoT combination is likely to be powerful and this combination will probably transform many industries (Christidis & Devetsikiotis, 2016). For instance, smart IoT devices can possibly carry out autonomous transactions through smart contracts (Cognizant Reports, 2016). It may be that combining blockchain and IoT with artificial intelligence (AI), and big data solutions, more significant impacts can be produced. At the same time, the IoT may create major security headache for organizations.

Before proceeding further, it is important to stress that IoT security has been an issue of pressing concern that has received substantial consideration recently. To demonstrate this point, let us consider the following examples. In 2015, the U.S.-based application security company Veracode tested six IoT devices: the Chamberlain MyQ Garage, the Chamberlain MyQ Internet Gateway, the SmartThings Hub, the Ubi from Unified Computer Intelligence Corporation, the Wink Hub and the Wink Relay (Veracode, 2017). The Veracode team found serious security issues in five of them. The team analyzed the implementation and security of the communication protocols used in the IoT systems. The front-end (between users and the cloud services), as well the back-end (between the devices and the cloud services) connections were examined. Except for the SmartThings Hub, the devices had failed to enforce strong passwords. The front-end connections were thus insecure. In addition, the Ubi lacked encryption for user connections. These deficiencies can make them vulnerable to man-in-the-middle (MitM) attacks. The team found even worse results for back-end connections. The Ubi and MyQ Garage failed to employ encryption. They did not offer adequate protection against MitM attacks. They also lacked protection against replay attacks. Note that in replay attacks, MitM attackers capture traffic and then play it back, which potentially trigger unauthorized actions. Moreover, transport layer security (TLS) encryption was not employed in some cases. In cases, where TLS was implemented, there was a lack of proper certificate validation. The Ubi had also failed to properly secure sensitive data (Constantin, 2015).

As another example, consider the October 2016 cyberattacks on the U.S.-based domain name system (DNS) provider Dyn. Dyn said that the attacks originated from "tens of millions of IP addresses" and was among the largest ever attacks (NBCNewYork, 2016). According to Dyn, at least some of the malicious Internet traffic came from IoT devices which included webcams, baby monitors, home routers and digital video recorders (Perlroth, 2016). The concerned IoT devices that attacked Dyn had been infected with control software called Mirai. Mirai is reportedly an easy-to-use program that even unskilled hackers can exploit. It controls online devices and uses them to launch distributed denial of service (DDoS) attacks. The process involves using phishing emails to infect a computer or home network. Then it spreads to other devices such as DVRs, printers, routers and Internet-connected cameras used by stores and businesses for surveillance (Blumenthal & Weise, 2016).

The above flaws comprise severe privacy and security risks. For instance, based on information gathered from an Ubi device such as presence or absence of *noise or light in the house*, criminals can know whether there is someone at home or not. By exploiting vulnerabilities in the Ubi or Wink Relay devices, it is possible for attackers to turn on their microphones and listen to conversations. Vulnerabilities in the Chamberlain MyQ system allow thieves to know when the garage door is opened or closed (Constantin, 2015).

Severe consequences can occur if an IoT device is hacked. Consider the diffusion of smart water meters and associated cybersecurity risks. As of the early 2017, 20% of residents in the U.S. state of California had smart water meters, which collect data and send alerts on water leakages and usage to consumers' phones (Hackett, 2017). The Washington Suburban Sanitary Commission (WSSC) was also reported to be taking measures to integrate IoT into its water supply system. Water-usage data can tell hackers and criminals when residents are not home. It is possible that the perpetrators can then burglarize homes when their residents are away (Hackett, 2017).

It may be that blockchain is especially appropriate and promising for tackling privacy and security problems associated with the IoT. Some point out that blockchain can possibly provide military-grade security for IoT devices (Coward, 2016). Below we consider the key processes and mechanisms as well as some initiatives that potentially contribute to stronger IoT security.

5. Measures at various levels to integrate blockchain in IoT security

Blockchain's incorporation in IoT is being supported through a wide variety of measures intended to strengthen security. Several companies are leading initiatives to integrate blockchain into the production circle and supply chain. For instance, startups such as Provenance use blockchain to promote trust in the supply chain by providing transparency and visibility when products move from the source to customer (Dickson, 2016b).

IBM is using its huge cloud infrastructure to provide blockchain services for tracking high-value items as they move across supply chains. IBM's Watson IoT Platform has built-in capability that allows users to add selected IoT data to a private blockchain ledgers, which can be included in shared transactions. The Platform translates the data from connected devices into the format that blockchain contract APIs need. It is not necessary for the blockchain contract to know the specifics of the device data. The Platform filters device events and sends only the data that is required for the contract (IBM, 2017). All business partners can access and supply IoT data in a decentralized fashion and can verify each transaction (Kaul, 2016). Data are not collected, stored, and managed centrally. Data are protected and shared among only the parties that are involved in the transaction.

Others are creating new business models that eliminate the need of centralized cloud servers. To take an example, Filament, a blockchain-based solutions provider for the IoT, has launched wireless sensors, called Taps. A Filament Tap is a sensor device which allows IoT devices to communicate with computers, phones or tablets within 10 miles (Rizzo, 2015).

Filament runs over the so called “Telehash” communications protocol, which means a central hub such as the cloud is not needed. Instead, the Filament nodes are deployed in a mesh configuration (Jones, 2017). That is, the Taps create low-power autonomous mesh networks. This means that each node relays data for the network and all mesh nodes cooperate in the distribution of data in the network. Some potential applications include managing physical mining operations or water flows over agricultural fields. Device identification and intercommunication are done by blockchain that holds the unique identity of each participating node (Dickson, 2016b).

One key application of Filament Taps is likely to be in the next generation of industrial network technology. Filament's blockchain-based applications in industrial network pair cutting-edge sensors connected in a decentralized system that use autonomous smart contracts. Devices are likely to communicate securely, exchange value with each other and execute intended actions in an automatic manner. For instance, Filament's “Tap” sensors can be attached to a large drilling rig in a remote location. Based on predefined conditions, the drilling rig may sense that it requires an important piece of machinery. It could then automatically send request messages to an autonomous drone, asking to deliver the replacement part. The contracts do not run in a blockchain (Lewis, 2017). Blockchain's role is just to verify inputs and outputs (Scott, 2017). Such applications are especially useful and valuable with the rapid rise in the number of IoT devices that exchange value among themselves (Pajot-Phipps, 2017).

Measures are also being taken at inter-organizational and industry levels. A group of technology and financial companies announced in January 2017 that they formed a group to set a new standard for securing IoT applications using blockchain. Companies joining the group include Cisco, application maker Bosch, Bank of New York Mellon Corp., Foxconn Technology, CS company Gemalto and blockchain startups Consensus Systems, BitSE and Chronicled (Brown, 2017). The group's aim was to establish a blockchain protocol as a shared platform to build IoT devices, applications and networks (Young, 2017a). In April 2017, the group announced that it created an API that supports technologies offered by major Ethereum-based blockchain systems such as JP Morgan's Quorum and the Linux-led Hyperledger project. Using the protocol, users can register multiple weaker identities such as serial numbers, QR codes, and UPC code and bind them to stronger cryptographic identities. Using blockchain, the newly created cryptographic identities are immutably linked across physical and digital worlds. As of April 2017, the software development kits (SDKs) were in beta phase and were available via the Chronicled and Hyperledger libraries on GitHub (Rizzo, 2017).

To take another example, Berlin, Germany-based startup MyBit utilizes the Ethereum and Bitcoin Blockchain networks to address data manipulation problems. A key feature of MyBit's data storage technology is its non-custodial nature, just like the bitcoin wallet platforms and infrastructures. Note that non-custodial platforms such as bitcoin do not hold passwords or other sensitive information of users. Once recorded to MyBit's infrastructure, data is autonomously transferred into the bitcoin and Ethereum Blockchains. It removes trust and provides immutability to users (Young, 2017b).

6. Blockchain-based identity and access management systems

Blockchain-based identity and access management systems can be leveraged in strengthening IoT security. Such systems have

already been used to securely store information about goods' provenance, identity, credentials, and digital rights. Blockchain's immutability can be achieved by making sure that the original information entered is accurate (Catallini, 2017). In this regard, a key challenge that arises in some applications is that it is difficult to ensure that the properties of physical assets, individuals (credentials), resource use (energy and bandwidth through IoT devices), and other relevant events are stored securely and reliably. This aspect can be relatively easily handled for most IoT devices. For instance, a private blockchain can be used to store cryptographic hashes of individual device firmware (software specifically designed for the device). Such a system is likely to create a permanent record of device configuration and state. This record can be possibly used to verify that a given device is genuine and that its software and settings have not been tampered or breached. Only then the device is allowed to connect to other devices or services.

Returning to the Dyn example above, IP spoofing attacks were launched, especially in the later versions of the Mirai botnet. Blockchain-based identity and access management systems can provide stronger defense against attacks involving IP spoofing or IP address forgery. Since blockchain cannot be altered, it is not possible for devices to connect to a network by disguising themselves by injecting fake signatures into the record (Kumar, 2017). The above example involving Filaments' Taps serves to illustrate this point.

7. Centralized cloud model versus decentralized blockchain model: the case of IoT

A common thread that runs through the above security flaws is that they depend on a centralized cloud model. This model is likely to become even more problematic and potentially risky when the number of network nodes grows bigger. One estimate suggested that applications such as Internet radio, music streaming and information services will generate approximately 6000 PB annually by 2021, which is the equivalent to over 300 billion hours of music streaming (Deans, 2016). Centralized models can be expensive and difficult to manage, especially when applied to a data intensive applications involving IoT. Therefore, a decentralized, blockchain-based approach would be more appropriate and more effective for IoT. (Kaul, 2016).

We return to the above examples and comparison of cloud and blockchain models in the context of the IoT. It is important to discuss some key challenges associated with the current centralized cloud model of IoT security. IoT devices are identified, authenticated and connected through cloud servers, where processing and storage are often carried out. Even if IoT devices are a few feet apart from each other, connections between them need to go through the Internet (Banafa, 2017).

First, IoT networks have rocketed to a new level and high costs are a big concern in the centralized cloud model when the existing IoT solutions grow in scale. Gartner estimated that in 2016, 5.5 million new IoT devices were connected every day (Van der Meulen, 2015). It is estimated that by 2020, a network capacity that is at least 1000 times the level of 2016 will be needed (Waterman, 2016). The amount of communications that need to be handled when IoT devices grow to the tens of billions will increase costs exponentially. Large server farms and networking equipment are needed. Infrastructure and maintenance costs associated with centralized clouds grow rapidly. The future is thus even more challenging with the current cloud-based centralized model.

Second, even if device manufacturers and cybersecurity firms are able to address the economic and manufacturing challenges, each block of the IoT architecture may act as a bottleneck or a point of failure, which can disrupt the entire network (Banafa, 2016). For instance, IoT devices are vulnerable to DDoS attacks, hackings, data thefts, and remote hijackings. Criminals may also hack the system and misuse data. Most IoT devices send data into the cloud and messages can be sent from the cloud to the devices. This aspect is especially important with regard to IoT security. As noted above, if an IoT device connected to a server is hacked, all devices connected to the server may be affected.

Third, the centralized cloud model of IoT is susceptible to manipulation. For instance, collecting real-time data does not ensure that the information is likely to be put to good and appropriate use. Consider the water supply system example discussed above. If state officials or water service companies have reason to believe that the evidence of a problem may result in high costs or lawsuits, they can engage in activities to censor, edit, or delete data and associated analyses. They can also manipulate the findings in a particular direction. For instance, consider the water crisis in the city of Flint, Michigan, which began in 2014. The city's mayor said that Flint was experiencing a "man-made disaster" and state of emergency was declared over high lead levels. Flint authorities had insisted for months that the city's water was safe to drink (Hackett, 2017). Citing official documents and findings of researchers who conducted extensive tests, a *CNN* article asserted that Michigan officials may have altered sample data to lower the city's water lead-level (Debucquoy-Dodley, 2016). It was reported that whereas the Michigan Department of Environmental Quality and the city of Flint were required to collect 100 samples from homes to test lead level, they had collected only 71 samples. Moreover, the final report from the Department only accounted for 69 of the 71 collected samples. A researcher from Virginia Polytechnic Institute and State University said that the two samples that were discarded from the analysis had high levels of lead. Including them in the analysis would have increased the level above 15 parts-per-billion (PPB). According to the Environmental Protection Agency (EPA), water supply companies are required to alert the public and take actions if lead concentrations exceed the "action level" of 15 PPB in drinking water (https://www.epa.gov/dwreginfo/lead-and-copper-rule).

While it is yet to be proven in the long term, it may be that blockchain can eliminate many of the above drawbacks (Table 2). IoT solutions can use blockchain to enable secure messaging between devices in a network. In a blockchain model, message exchanges between devices can be treated in a similar way as financial transactions in a bitcoin network. To exchange messages, devices will leverage smart contracts which model the agreement between two parties (Banafa, 2016). Blockchain cryptographically signs transactions and verifies those cryptographic signatures to ensure that only the originator of the message could have sent it. This can possibly eliminate the Man-In-The-Middle and replay attacks (Coward, 2016).

Blockchain's proponents have forcefully argued that this new technology can save us from "another Flint-like contamination crisis" (Hackett, 2017). Projects such as the WSSC's integration of the IoT in supply system can be probably upgraded with sensors such as near-infrared reflectance spectroscopy (NIRS) to include data on chemical levels. If such a system was installed in Michigan, Flint's water

Table 2
Blockchain's potential to address some of the key challenges associated with cloud-based IoT.

Challenge of cloud-based IoT platforms/ applications	Explanation/example	Possible mechanisms by which blockchain can address the problem
Costs and capacity constraints to handle rapidly growing IoT needs	Challenge to handle exponential growth in IoT devices: by 2020, a network capacity at least 1000 times the level of 2016 will be needed.	No need of a centralized entity: Devices can communicate securely, exchange value with each other and execute actions automatically through smart contracts.
Architectural constraints	Each block of IoT architecture acts as a bottleneck/point of failure, and disrupts the entire network: vulnerability to DDoS attacks, hackings, data thefts, and remote hijackings.	Secure messaging between devices: validity of a device's identity is verified, transactions are signed and verified cryptographically to ensure that only the originator of the message could have sent it.
Challenges associated with downtime and unavailability of services	Sometimes cloud servers are down due to cyberattacks, software bugs, power, cooling or other problems.	No single point of failure, records are on many computers/devices that hold identical information.
Susceptibility to manipulation and inappropriate use	Information is likely to be manipulated and put to inappropriate uses	Decentralized access and immutability: malicious actions can be detected and prevented. The devices are interlocked: If one device's blockchain updates are breached, the system rejects it.

Source: Adopted from Kshetri (2017a).

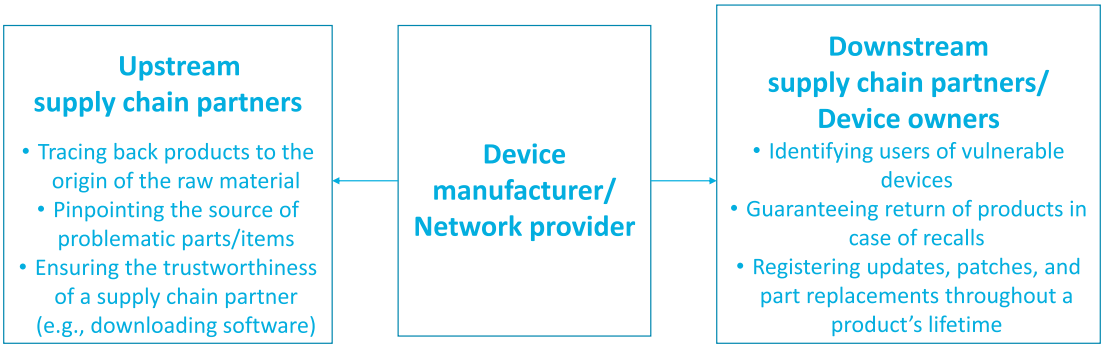

Fig. 1. Blockchain's role in strengthening and improving security in a supply chain network. Source: Adopted from Kshetri (2017a,b).

service company could have found the lead contamination when it exceeded a healthy level. Blockchain-based systems can thus possibly provide the "second layer of crisis prevention" in such cases (Hackett, 2017).

8. Blockchain's roles in ensuring security of supply chain

A key trend that has emerged in the blockchain arena has been the development of sophisticated applications to manage supply chains. Indeed, supply chain has been identified as one of the three areas[2] outside finance with strong fits for blockchain with a potential to deliver real ROI at the early stage of blockchain development (Bünger, 2017). This trend is likely to have a major implication for the security of IoT devices.

It may be that blockchain can improve security of both forward and backward linkages in supply chains. In this way, it can possibly be an effective tool to track the sources of insecurity in supply chains (Fig. 1). If an IoT security breach is discovered, this technology is likely to make it possible to contain the breach in a targeted way. Blockchain can thus possibly facilitate handling and dealing with crisis situations such as product recalls due to security vulnerability.

Blockchain's public availability is likely to make it possible to trace back every product to the origin of the raw materials. Transactions can also be possibly linked to identify users of vulnerable IoT devices. For the reasons explained above, IoT-linked security crises such as the October 2016 cyberattacks on Dyn could have been handled in a better way if the supply chains associated with the concerned devices had adopted blockchain. For instance, China-based Hangzhou Xiongmai Technologies, which makes Internet-connected cameras and accompanying accessories, recalled its products sold in the U.S. that were vulnerable to the Mirai malware. However, in the current non-blockchain environment it is difficult to track down the owners of the devices and contact them if items with security vulnerability are not returned. This could be resolved with blockchain. Blockchain is suitable for complex workflows such as that can be observed in the technology production and supply chain. An application is that blockchain can be used to registers time, location, price, parties involved, and other relevant information when an item changes ownership. The technology can also be used to track raw materials as they move through the supply chain, are transformed into circuit boards and electronic components, are integrated into products, and then sold to customers. Blockchain can also be used to register updates, patches, and part replacements applied to any product or device throughout its lifetime. This would make it easier to track progress in addressing vulnerabilities and security problems

[2] Other two areas are power and food/agriculture.

and send warnings and notifications to product owners (Dickson, 2016a). In this way, blockchain can also provide an effective post-breach resilience plan and implementation.

9. Blockchain and the Fair Information Practices (FIPs)

It would be interesting to consider how blockchain performs in terms of the Fair Information Practices (FIPs), which are an established set of principles for addressing privacy concerns on which modern privacy laws are based (Rubinstein, 2013). Prior research has suggested that big data may challenge the FIPs. Table 3 presents how blockchain is likely outperform the current methods in terms of various provisions and principles of FIPs.

A number of concerns have been raised regarding the handling of data in the current big data environment. First, personal data can be put to new uses to create value in important ways. The commissioner of the U.S. Federal Trade Commission (FTC) pointed out the possibility that firms, "without our knowledge or consent, can amass large amounts of private information about people to use for purposes we don't expect or understand" (Brill, 2013). Prior research has suggested that the proportion of privacy violations associated with secondary usages of personal information compared to those related to primary collection has drastically increased in the big data environment (Etzioni, 2015). Such uses often violate the transparency principle of FIPs (Teufel, 2008). In a blockchain model, there is no custodian or steward of user data. Data are controlled with private and public keys.

Second, many of the innovations involving big data use multiple data sources and involve transferring data to third parties. Many organizations believe that making data anonymous before sharing to third parties would make it impossible to identify. This is often a convenient but possibly false assumption. Researchers have presented a variety of methods and techniques that can be used to de-identify personal data and reassociate with specific consumers (Brill, 2012). Big data processes can generate predictive models that have a high probability of revealing personally identifiable information (Crawford & Schultz, 2013) and thus make anonymization impossible. Failure to protect PII and unintended or inappropriate disclosure violate the security provision of FIPs (Teufel, 2008). In a blockchain model, the owner chooses what information to release to whom and what to withhold.

Third, a large proportion of data in the current big data environment comes from passive data collection without any overt consumer interaction (e.g., related to user preferences and usage behaviors such as location data from mobile devices and the use of cookies to capture Internet browsing history) and most users are not aware and do not notice that data on them is being captured (World Economic Forum, 2013). The lack of individual consent for the collection, use, and dissemination of such information means that such a practice violates the individual participation principle of FIPs (Teufel, 2008). It may be that this problem can be overcome using blockchain.

While it is yet to be proven in the long term, blockchain can possibly be used as an alternative to cookies in order to ensure that users have control over their data. Let us assume that a consumer sees an ad for a book on her smartphone. It may be possible for the book advertiser to ask the consumer to reveal her identity by taking a selfie with her smartphone (Tan & Lim, 2017). In return, the consumer is possibly paid in crypto-currencies such as bitcoin. The consumer may also be asked to allow the advertiser to access her SIM card and verify with the phone company regarding the ownership of the phone. It may be that the advertiser also want to know the consumer's location using s platforms such as Google Maps and Bing Maps. Note that it is possible to perform each of the above activities separately in a non-blockchain world. What blockchain may make possible is connecting all of the concerned parties together with a smart contract. In this example, some of the key parties involved in the smart contract could be the consumer, the book advertiser/publisher, the phone company and Google/Bing. The advertiser will possibly promise a predefined payment in crypto-currency, which may be released to the consumer only if all the concerned parties perform their actions coded in the smart contract (Tan & Lim, 2017). It may thus be possible to verify ad delivery and increase the level of personalization without breaching privacy laws (WARC, 2017). Overall, it may be that blockchain-based smart contracts will be implemented in such a way that consumers can possibly participate in the entire process.

Finally, the accountability principle argues that data controllers should be accountable, that is, they do what is needed and expected – so that the various principles noted above are applied. However, the lack of audit trail means that accountability cannot be assessed in a non-blockchain model. Blockchain ledgers, on the other hand, include an audit trail, which is likely to ensure that accountability has not been neglected or lost.

10. Implications for regulation and policy

The above discussion has important implications for regulation and policy. First, it may be that a strong IoT security can be achieved

Table 3
How blockchain may outperform the current methods in terms of various provisions and principles of FIPs.

FIP principle/provision	Challenge in a non-blockchain world	How a blockchain model can address?
Transparency principle	Without the knowledge or consent of a consumer, intermediaries, such as CSPs may use private information for purposes that the consumer does not expect or understand.	There is no custodian or steward of user data. Data are controlled with private and public keys.
Security provision	Failure to protect PII and unintended or inappropriate disclosure	The owner chooses what information to release to whom and what to withhold.
Individual participation principle	A large proportion of data comes from passive data collection. Most users are not aware and do not notice that data on them is being captured.	Smart contract connects a consumer with all the concerned parties and ensures that the consumer can explicitly participate.
Accountability principle	The lack of audit trail means that accountability cannot be assessed.	Blockchain ledgers includes an audit trail to ensure that accountability has not been neglected

by making a regulatory requirement for companies to deploy blockchain in supply chain. While it may not be entirely achievable in the short run to force all companies to use blockchain-based solutions to track items through complex supply chains, policy makers can start with systems that are mission critical, and associated with substantial national security and economic benefits. For instance, the supply chain of defense systems may fit this description.

Second, the above analysis indicates that blockchain outperforms most other approaches in privacy protection. An effective deployment of blockchain to protect privacy, however, requires the development of a rich ecosystem around this technology. Public policy efforts directed at protecting privacy using blockchain should therefore focus on providing training to key stakeholders and increasing investment in this technology. For instance, it is important to make sure that commercial certifiers such as city inspectors, accountants, lawyers and notaries feel comfortable in using this technology. Policy makers also need to pay attention to developing absorptive capacity of relevant organizations such as banks and financial institutions, insurance providers and government agencies in order to benefit from this technology.

Third, one way to enrich the blockchain ecosystem in order to increase the role of this technology in strengthening cybersecurity and protecting privacy would be to turn attention to public–private partnerships. Prior research has suggested that public–private partnerships are an appropriate means of dealing with underdeveloped institutions, especially in developing countries (Kshetri, 2015, 2017b). Often the motivation and objectives of national governments and the private-sector actors partly overlap in developing new and transformative technologies such as blockchain. National and local governments should provide funding and other support for private sector activities that are directed principally at development of blockchain-based solutions to strengthen cybersecurity and protect privacy. Some specific examples of such policies were discussed earlier in the U.S. context (e.g., collaboration between the FDA and IBM). An analysis of in the U.S. semiconductor industry in the 1950s and the 1960s indicated that procurement from government defense agencies and the government's support for R&D facilitated the entry of new firms in the electronics industry (Boeker, 1989).

In the early stage of the development of the U.S. semiconductor industry, the U.S government and military were the principal market for the products if the country's semiconductor industry (Utterback & Murray, 1979). To put things in context, guaranteed purchase of blcockchain-based solutions by government agencies to apply in diverse areas such as issuing of driving licenses and land registry can stimulate the entry of new firms in the blockchain industry.

Government investment in R&D for the development of privacy-protecting and security-enhancing blockchain-based solutions is also critical. This is due to the public goods nature of knowledge (Geroski, 1995). Private sector firms are often reluctant to invest optimally in R&D related to blockchain-based solutions due to the fact that the inventors often need to make new technologies and knowledge available to the public in order to reap the rewards. However, when firms make new inventions public, at least some of the knowledge contained in the invention also becomes public, which may stimulate additional innovations (Popp, 2010). The spillover may provide benefit to the public, but not to the innovator. Private firms thus often lack incentives to engage in a socially optimal level of research activity in new areas such as blockchain.

Finally, many of the above arguments are based on the assumption of legality of a smart contract framework. The idea here is that software codes can algorithmically enforce agreements among parties. There is, however, considerable disagreement and confusion among legal community members on the subject of smart contract. One view is that “code is law”. The opposite argument is that “No, code isn't law” (del Castillo, 2017). Some attorneys have noted that in order to be legally enforceable, a smart contract must meet all the traditional elements that a binding contract needs to have (Alderman, 2017). National governments thus should provide legal clarity and more information so that parties can engage in smart contracts that are enforceable.

11. Concluding comments

From the above discussion, it is clear that blockchain may prove to be a nightmare for cybercriminals, data manipulators and others who mishandle personal data. Overall based on the above evolving mechanisms and forces, a promising future can be foreseen for the use of blockchain in addressing various aspects of security and privacy. Among the most promising is that individuals are able to control their own personal data. For instance, after certifiers such as a government agency provide the subject with a digitally signed copy of a document (e.g., driving license), and put it on blockchain, they no longer have access to the data (Mainelli, 2017).

Some of the key security challenges associated with the cloud can be addressed by using the decentralized, autonomous, and trustless capabilities of blockchain. Blockchain ensures that each party is held accountable for its individual roles in the overall transaction and thus prevents disputes. Especially blockchain's decentralized, and consensus driven structures are likely to provide more secure approach when the network size increases exponentially. As a blockchain network may include different types of participants, organizations' choice between permissioned and permissionless blockchain is a function of the number of participants, the value of assets being traded or exchanged and the importance of authorizing participants with varying credentials.

When machines become capable of implementing cryptographic security, most of the current hacking activities can be eliminated or at least reduced. This exactly has been the focus of a number of blockchain-related initiatives that are being undertaken at various levels. Blockchain possibly enables a costless verification of a device's attributes. The cryptographic verifiability feature is likely to stop MitM, replay and other types of attacks. Blockchain-based transactions are also easily auditable. Due primarily to this and other features, blockchain can possibly play a key role in tracking the sources of insecurity in supply chain as well as in handling and dealing with crisis situations such as product recalls in case of a security vulnerability. As explained above, it may be that blockchain-based identity and access management systems can address key IoT security challenges such as those associated with IP spoofing.

Acknowledgment

The author is grateful to an anonymous *JTPO* reviewer and the Editor in Chief Erik Bohlin for their detailed, generous and insightful

comments. An earlier version of this paper was presented at the Inaugural Ostrom Workshop Colloquium on Cybersecurity and Internet Governance held in Indiana University, Bloomington, IN on April 27–28, 2017. The author gratefully acknowledges the helpful comments from Scott Shackelford, organizer of the Workshop and other participants.

References

Alderman, P. (2017, August 16). *Smart contracts in Australia: Just how clever are they?*. Retrieved from https://www.lexology.com/library/detail.aspx?g=3747bb11-18ec-4a6a-9182-ac7f84fc7ebe.

Allen, J. M. (2011). Cloud computing: Heavenly solution or pie in the sky? *Pennsylvania CPA Journal, 82*(1), 1–4.

Armasu, L. (2015). *Google adopts zero trust network model for its own cloud, may 13*. Retrieved from http://www.tomsitpro.com/articles/google-zerotrust-network-own-cloud,1–2608.html.

Baker, M. (2017). *Why SWIFT's days are numbered, and What's Next.MSPmentor*. Retrieved from http://mspmentor.net/technologies/why-swift-s-days-are-numbered-and-what-s-next.

Banafa, A. (2016). *A secure model of IoT with blockchain*. OpenMind, Retrieved from https://www.bbvaopenmind.com/en/a-secure-model-of-iot-with-blockchain/?utm_source=views&utm_medium=article06&utm_campaign=MITcompany&utm_content=banafa-jan07.

Banafa, A. (2017). IoT and blockchain Convergence: Benefits and challenges. IEEE. Internet of Things, Retrieved from http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html.

Bertrand, J. (2017). *Blockchain and Cloud kissing cousins*. Finextra, Retrieved from https://www.finextra.com/blogposting/13780/blockchain-and-cloud-kissing-cousins.

Blumenthal, E., & Weise, E. (2016). *Hacked home devices caused massive Internet outage*. USA Today. Retrieved from http://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/.

Boeker, W. (1989). The development and institutionalization of subunit power in organizations. *Administrative Science Quarterly, 34*(3), 388–410.

Brill, J. (2012, March 2). *Big data, big issues*. Fordham University School of Law. Retrieved from http://www.ftc.gov/public-statements/2012/03/big-data-big-issues.

Brill, J. (2013). *Demanding transparency from data brokers*. Washington Post Opinions. Retrieved from http://www.washingtonpost.com/opinions/demanding-transparency-from-data-brokers/2013/08/15/00609680-0382-11e3-9259-e2aafe5a5f84_story.html.

Brodkin, J. (2010). 5 problems with SaaS security. *Network World, 27*(18), 1–27.

Brown, J. (2017). *Companies forge cooperative to explore blockchain-based IoT security*. CioDive. Retrieved from http://www.ciodive.com/news/companies-forge-cooperative-to-explore-blockchain-based-iot-security/435007/.

Bünger M.. 14 (2017). Blockchain for industrial enterprises: Hype, reality, obstacles and outlook, Retrieved from (http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Blockchain-for-industrial-enterprises-Hype-reality-obstacles-and-outlook).

Bussmann, O. (2017). *BankThink A public or private blockchain? New Ethereum project could mean both*. American Banker. Retrieved from https://www.americanbanker.com/opinion/a-public-or-private-blockchain-new-ethereum-project-could-mean-both.

del Castillo, M. (2017, August 14). *Legally binding smart Contracts? 10 law firms join enterprise Ethereum alliance*. Retrieved from https://www.coindesk.com/legally-binding-smart-contracts-9-law-firms-join-enterprise-ethereum-alliance/.

Catallini, C. (2017). *How blockchain applications will move beyond finance*. Retrieved from https://hbr.org/2017/03/how-blockchain-applications-will-move-beyond-finance.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of things. *IEEE Access, 4*, 2292–2303.

CISCO. (2017). *What is a firewall?*. Retrieved from http://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.

Cisco Public. (2016). *Cisco global cloud Index: Forecast and methodology, 2015–2020*. White Paper.

Cognizant Reports. (2016). *Blockchain in banking: A measured approach*.

Constantin, L. (2015). *Researchers show that IoT devices are not designed with security in mind*. IDG News Service http://www.networkworld.com/article/2906953/researchers-show-that-iot-devices-are-not-designed-with-security-in-mind.html.

Coward, J. (2016). *Meet the visionary who brought blockchain to the industrial IoT*. IOT World News. Retrieved from http://www.iotworldnews.com/author.asp?section_id=495&doc_id=728962.

Crawford, K., & Schultz, J. M. (2013). *Big data and due process: Toward a framework to redress predictive privacy harms*. New York University Public Law and Legal Theory Working Papers. Paper 429. Retrieved from http://lsr.nellco.org/nyu_plltwp/429/.

Deans, D. H. (2016). *How M2M and IoT enable new data-intensive applications*. TelecomsTech. Retrieved from https://www.telecomstechnews.com/news/2016/sep/26/m2m-and-iot-enable-new-data-intensive-applications/.

Debucquoy-Dodley, D. (2016). *Did Michigan officials hide the truth about lead in Flint?*. Retrieved from http://www.cnn.com/2016/01/14/us/flint-water-investigation/.

Dickson, B. (2016a). *Blockchain could help fix IoT security after DDoS attack*. Retrieved from http://venturebeat.com/2016/10/29/blockchain-could-help-fix-iot-security-after-ddos-attack/.

Dickson, B. (2016b). *How blockchain can change the future of IoT*. VentureBeat. Retrieved from http://venturebeat.com/2016/11/20/how-blockchain-can-change-the-future-of-iot/.

Due.com. (2017). *How blockchain improves security and transaction times*. Nasdaq. Retrieved from http://www.nasdaq.com/article/how-blockchain-improves-security-and-transaction-times-cm771339.

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). *A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data, White paper*. MIT Media Lab, Beth Israel Deaconess Medical Center.

Etzioni, A. (2015). A cyber age privacy Doctrine: More coherent, less subjective, and operational. *Brooklyn Law Review, 80*(4). Article 2.

Finch, B. (2014). *Why cybersecurity must be defined by process, not tech*. Retrieved from http://blogs.wsj.com/cio/2014/12/11/why-cybersecurity-must-be-defined-by-process-not-tech/.

Galang, J. (2017). *With IBM partnership, SecureKey enters next phase of developing secure digital identity network*. Betakit. Retrieved from http://betakit.com/with-ibm-partnership-securekey-enters-next-phase-of-developing-secure-digital-identity-network/.

Gaudiosi, J. (2014). *Why Sony didn't learn from its 2011 hack*. Fortune. Retrieved from http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/.

Geroski, P. (1995). Markets for Technology: Knowledge, innovation, and appropriability. In P. Stoneman (Ed.), *Ch. 4 in handbook of the economics of innovation and technological change* (pp. 90–131). Oxford UK: Blackwell Publishers.

Goodburn, M. A., & Hill, S. (2011). The cloud transforms business. *Financial Executive, 26*(10), 34–39.

Groenfeldt, T. (2017). *IBM and maersk apply blockchain to container shipping*. Retrieved from https://www.forbes.com/sites/tomgroenfeldt/#17a4405c5004.

Hackett, R. (2017). *How blockchains could save us from another Flint-like contamination crisis*. Venturebeat. Retrieved from http://venturebeat.com/2017/02/25/how-blockchains-could-save-us-from-another-flint-like-contamination-crisis/.

Halamka, J. D., Lippman, A., & Ekblaw, A. (2017). *The potential for blockchain to transform electronic health records*. Retrieved from https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records.

Health Data Management. (2017). FDA, IBM Watson health to study application of blockchain technology. *Fred Bazzoli, 12*(5), 1.

Higgins, S. (2016). *Hours after launch, OpenBazaar sees first Drug listings*. CoinDesk. Retrieved from http://www.coindesk.com/drugs-contraband-openbazaar/.

Ho, S. (2017). *Canada's SecureKey receives U.S. grant to build digital identity network*. The Globe and Mail. Retrieved from http://www.theglobeandmail.com/technology/canadas-securekey-wins-us-grant-to-help-build-digital-identity-network/article34022647/.

Hughes, N. (2017). *IBM, SecureKey partner on blockchain identity service for consumers*. One World Identity. Retrieved from https://oneworldidentity.com/2017/03/20/ibm-securekey-partner-blockchain-identity-service-consumers/.

IBM. (2017). *Explore Watson IoT with blockchain*. Retrieved from https://www.ibm.com/internet-of-things/platform/private-blockchain/.

Jones, D. (2017). *Verizon & friends light up filament with $15M, April 4*. Retrieved from http://www.lightreading.com/iot/industrial-iot/verizon-and-friends-light-up-filament-with-$15m/d/d-id/731812.
Kaul, A. (2016). *IBM Watson IoT and its integration with blockchain*. Tractica. Retrieved from https://www.tractica.com/automation-robotics/ibm-watson-iot-and-its-integration-with-blockchain/.
Kestenbaum, R. (2017). *Why bitcoin is important for your business*. Forbes. Retrieved from https://www.forbes.com/sites/richardkestenbaum/2017/03/14/why-bitcoin-is-important-for-your-business/3/#2da6d4c72b3b.
Knight, W. (2017). *Blockchain's weak spots pose a hidden danger to users, April 18*. Retrieved from https://www.technologyreview.com/s/604219/blockchains-weak-spots-pose-a-hidden-danger-to-users/.
Kshetri, N. (2013). Privacy and security issues in cloud Computing: The role of institutions and institutional evolution. *Telecommunications Policy, 37*(4–5), 372–386.
Kshetri, N. (2014). Big Data's impact on privacy, security and consumer welfare. *Telecommunications Policy, 38*, 1134–1145.
Kshetri, N. (2015). India's cybersecurity Landscape: The roles of the private sector and public-private partnership. *IEEE Security & Privacy, 13*(3), 16–23.
Kshetri, N. (2017a). Can blockchain strengthen IoT? *IEEE IT Professional, 19*(4), 68–72.
Kshetri, N. (2017b). Cybersecurity in India: Regulations, governance, institutional capacity and market mechanisms. *Asian Research Policy, 8*(1), 64–76.
Kumar, S. (2017). *Not just for cryptocash: How blockchain tech could help secure IoT*, 13 February Retrieved from http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Not-just-for-cryptocash-How-blockchain-tech-could-help-secure-IoT.
Lewis, R. (2017). *Internet of things and blockchain Technology: How does it work?*. May 18, Retrieved from https://cointelegraph.com/news/internet-of-things-and-blockchain-technology-how-does-it-work.
Lohade, N. (2017). *Dubai aims to Be a city built on blockchain*. Retrieved from https://www.wsj.com/articles/dubai-aims-to-be-a-city-built-on-blockchain-1493086080.
Mainelli, M. (2017). Blockchain will help us prove our identities in a digital world. *Harvard Business Review*. Retrieved from https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world.
Marshall Gerstein & Borun LLP. (2017). *The emerging blockchain patent landscape*. Lexology. Retrieved from http://www.lexology.com/library/detail.aspx?g=cf0c71c5-055a-4d57-92f8-c75d1e282414.
Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work and think*. Boston: Houghton Mifflin Harcourt.
McCreary, L. (2008). What was privacy? *Harvard Business Review, 86*(10), 123–131.
Munro, D. (2015). *Data breaches in healthcare totaled over 112 million records in 2015*. Forbes. Retrieved from https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#5a1974687b07.
NBCNewYork. (2016). *3rd cyberattack 'has been resolved' after hours of major outages: Company*. Retrieved from http://www.nbcnewyork.com/news/local/Major-Websites-Taken-Down-by-Internet-Attack-397905801.html.
Ore, J. (2016). *How a $64M hack changed the fate of Ethereum, Bitcoin's closest competitor: Cryptocurrency alternative to bitcoin was co-founded by 19-year-old Canadian-Russian in 2015*. CBC News. Retrieved from http://www.cbc.ca/news/technology/ethereum-hack-blockchain-fork-bitcoin-1.3719009.
Pajot-Phipps, S. (2017). *Op Ed: Energizing the blockchain — a canadian perspective*. Retrieved from https://bitcoinmagazine.com/articles/op-ed-energizing-blockchain-canadian-perspective/.
Pauli, D. (2016). *Google reveals own security regime policy trusts no network, anywhere, ever*. The Register. Retrieved from https://www.theregister.co.uk/2016/04/06/googles_beyondcorp_security_policy/.
Perlroth, N. (2016). *Hackers used new weapons to disrupt major websites across U.S*. NYTimes. Retrieved from http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0.
Popp, D. (2010). R&D subsidies and climate Policy: Is there a "free lunch"? *Climatic Change, 77*, 311–341.
Rizzo, P. (2015). *Filament nets $5 million for blockchain-based Internet of things hardware*. CoinDesk. Retrieved from http://www.coindesk.com/filament-nets-5-million-for-blockchain-based-internet-of-things-hardware/.
Rizzo, P. (2017). *Cisco, Bosch reveal new details on IoT-blockchain projects*. Retrieved from http://www.coindesk.com/cisco-bosch-reveal-new-details-iot-blockchain-projects/.
Rubinstein, I. S. (2013). *Big data: A pretty good privacy solution*. New York: New York University School of Law.
Schutzer, D. (2016). *CTO Corner: What is a Blockchain and why is it important?* FSRoundtable. Retrieved from http://fsroundtable.org/cto-corner-what-is-a-blockchain-and-why-is-it-important//.
Scott, M. (2017). *Fusing blockchain and IoT: An interview with Filament's CEO, March 14*. Retrieved from https://bitcoinmagazine.com/articles/fusing-blockchain-and-iot-interview-filaments-ceo/.
Seth, S. (2017). *Banks need to Be centralized – could blockchain be the answer?* Finance Magnates. http://www.financemagnates.com/cryptocurrency/bloggers/banks-need-centralized-blockchain-answer/.
Siegel, S. (2016). *Understanding the DAO hack for journalists*. Retrieved from https://medium.com/@pullnews/understanding-the-dao-hack-for-journalists-2312dd43e993#.9dt17ge8c.
Silverman, L. (2017). *How bitcoin technology could securely share medical records among your doctors*. Kera News. Retrieved from http://keranews.org/post/how-bitcoin-technology-could-securely-share-medical-records-among-your-doctors.
Tan, C., & Lim, E. T. K. (2017). *Blockchain could help advertisers lock up our attention*. Retrieved from https://which-50.com/blockchain-help-advertisers-lock-attention/.
Tausanovitch, N. (2016). *Zero-trust security for cloud data centers – how much does it cost?* Netronome. Retrieved from https://www.netronome.com/blog/zero-trust-security-for-cloud-data-centers-how-much-does-it-cost/.
Tech. (2017). *Kaspersky releases more evidence that North Korea was linked to Bangladesh SWIFT hack*. Retrieved from http://tech.firstpost.com/news-analysis/kaspersky-releases-more-evidence-that-north-korea-was-linked-to-bangladesh-swift-hack-370229.html.
Teufel, H., II (2008). *Privacy policy guidance memorandum, memorandum number: 2008-01, December 29*. The Privacy Office U.S. Department of Homeland Security.
The Economist. (2016). *Not-so-clever contracts: For the time being at least, human judgment is still a better bet than cold-hearted code*. Retrieved from http://www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted.
Tillery, S. (2010). *How safe is the cloud?*. Retrieved from http://www.baselinemag.com/c/a/Security/How-Safe-Is-the-Cloud-273226.
Utterback, J., & Murray, S. (1979). *The influence of defense procurement and sponsorship of research and development on the development of civilian electronics industry*. Cambridge, MA: Center for Policy Alternatives, Massachusetts Institute of Technology.
Van der Meulen. (2015). *Gartner says 6.4 billion connected "things" will Be in use in 2016, up 30 percent from 2015*. Gartner. Retrieved from http://www.gartner.com/newsroom/id/3165317.
Veracode. (2017). *The Internet of things poses cybersecurity risk*. Retrieved from https://info.veracode.com/whitepaper-the-internet-of-things-poses-cybersecurity-risk.html.
WARC. (2017). *Blockchain ripples media*. Waters Retrieved from https://www.warc.com/LatestNews/News/Blockchain_ripples_media_waters.news?ID=38272.
Waterman, S. (2016). *Industry to government: Hands off IoT security*. Fedscoop. Retrieved from http://fedscoop.com/industry-to-government-hand/s-off-iot-security.
World Economic Forum. (2013). *Unlocking the value of personal data: From collection to usage 7-8*. Retrieved from http//www.weforum.org/reports/unlocking-value-personal-data-collection-usage.
Young, J. (2016). *Hackers eye e-commerce platforms, bitcoin-based OpenBazaar to capitalize*. The Cointelegraph. Retrieved from https://cointelegraph.com/news/hackers-eye-e-commerce-platforms-bitcoin-based-openbazaar-to-capitalize.
Young, E. (2017a). *Tech giants and blockchain startups unite to make IoT apps more secure*. Retrieved from https://cointelegraph.com/news/tech-giants-and-blockchain-startups-unite-to-make-iot-apps-more-secure.
Young, J. (2017b). *The unbreachable data made possible with bitcoin & Ethereum blockchain, Here's how, April 19*. Retrieved from https://cointelegraph.com/news/the-unbreachable-data-made-possible-with-bitcoin-ethereum-blockchain-heres-how.