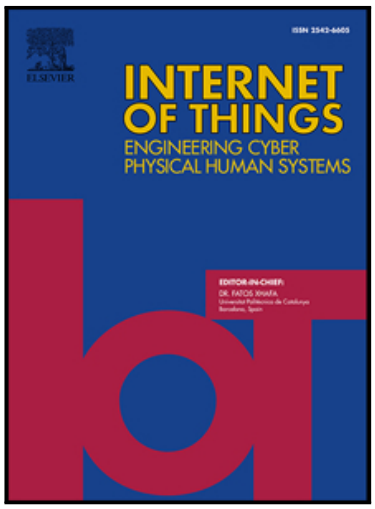


Perspectives on emerging directions in using IoT devices in blockchain applications

A. Ravishankar Rao PhD Fellow, IEEE ,
Daniel Clarke MS Student Member, IEEE

PII: S2542-6605(19)30130-1
DOI: https://doi.org/10.1016/j.iot.2019.100079
Article Number: 100079
Reference: IOT 100079

To appear in: *Internet of Things*

Please cite this article as: A. Ravishankar Rao PhD Fellow, IEEE , Daniel Clarke MS Student Member, IEEE , Perspectives on emerging directions in using IoT devices in blockchain applications, *Internet of Things* (2019), doi: https://doi.org/10.1016/j.iot.2019.100079

Perspectives on emerging directions in using IoT devices in blockchain applications

A.Ravishankar Rao, PhD (corresponding author)
Fellow, IEEE
School of Computer Sciences and Engineering
Fairleigh Dickinson University, NJ, USA
ravirao@fdu.edu
Tel: 914-960-9267

Daniel Clarke, MS
Student Member, IEEE
Icahn School of Medicine at Mount Sinai,
New York, NY, USA
danieljbclarke@gmail.com

ABSTRACT

The space of Internet-of-things has exploded, with billions of interconnected devices ranging from mainframes to refrigerators and thermostats. These devices offer the promise of greater automation and control, and the ability for micro-level transactions that did not exist before. The advent of blockchain offers an intriguing path to managing distributed transactions in this new ecosystem.

The use of blockchain in IoT applications is relatively new, especially at the lower end of the computing spectrum. Consequently, the roadmap for the future is unclear, and there are several challenges and questions that need to be addressed, such as trust, security, and efficiency. In this paper, we survey some of the promising applications that are being implemented including supply chains, smarter energy, and healthcare. We outline strategies for overcoming many of the challenges, which should lead to successful adoptions of blockchain for IoT. Finally, we sound a cautionary note on the potential cybersecurity implications in using IoT devices, including increased attack surfaces and device vulnerabilities.

KEYWORDS: Internet-of things, IoT, Blockchain, cybersecurity, trust, distributed computing

I. INTRODUCTION AND MOTIVATION

Both the internet-of-things (IoT)[1] and blockchain[2] are important building blocks in the future of an interconnected and increasingly automated world. They are enjoying rapid growth on their own. The intersection of these two areas creates interesting use cases and concomitant problems. A compelling reason propelling the synergy between these two areas is that there is a lack of secure methods to automate trust and exchange of real time data between IoT devices, and blockchain provides a viable solution [3].

An important challenge in the area of blockchain is that it is a relatively new technology, and has not seen widespread adoption across different industries. Consequently, there is a lack of academic papers that illuminate the issues

surrounding blockchain adoption. The scope of this paper is aimed at providing an overview of emerging application areas, that involve interactions between IoT devices and blockchain technology. We present and comment on three focus areas, consisting of healthcare, supply chain management, and the energy grid. There are many open questions in the area of healthcare such as protecting the privacy of medical records while allowing patients the freedom to share them with trusted parties. In the case of supply chain management, the availability of IoT sensors can be used to establish provenance and enable the execution of smart contracts. In the context of energy grids, early experiments are underway to use blockchain for smart metering and conducting distributed energy transactions. We chose these three important areas because they are witnessing increasing research, investment, and growth.

Blockchain uses distributed, append-only public ledgers to enable anonymous transactions that can be trusted [4]. An important problem that blockchain addresses is that of intermediation, in which buyers are matched to sellers through a trusted third party, typically a bank or broker in financial transactions. The bulk of current transactions involve a centralized model [5]. Blockchains offer a mechanism to assume the role of this intermediary[6], and moves us away from a centralized to a de-centralized model. Every party can verify the transactions of other parties through the blockchain. The vast scale of the Internet-of-things encompasses billions of devices, which may want to conduct transactions between each other. A major challenge in this scenario is the coordination of billions of devices. A centralized model is not applicable here, and blockchain offers a decentralized solution [7].

Blockchains also offer several desirable functions including transactional validity, transactional persistence and transactional privacy [7]. They address the issue of data sovereignty, where individuals are given control over their personal data, and are able to share it with only the parties they trust [8]. We will examine these desirable features of blockchain in conjunction with the three focus application areas we chose to address in this paper.

Keeping these developments in mind, we present the structure of our paper in Figure 1. Since there are many excellent review articles, books, and magazines devoted to explaining the basics of blockchain, we only provide a brief overview in order to keep the terminology in this paper self-contained. The reader is referred to the following sources for descriptions of the blockchain [2, 9, 10], and earlier surveys of blockchain for IoT [10].

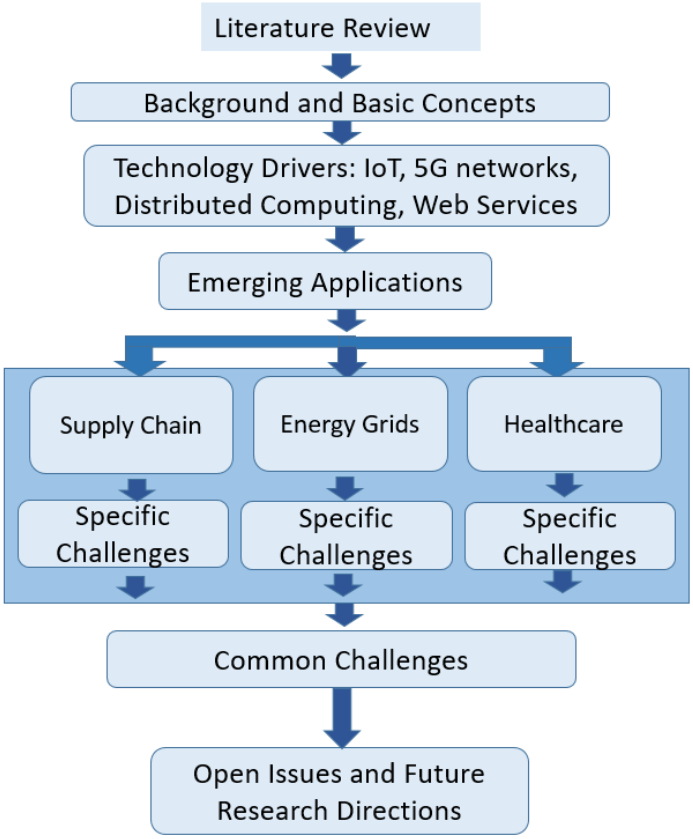


Figure 1: This figure describes the organization of the material in the current paper.

II. BACKGROUND: BASIC CONCEPTS AND TERMINOLOGY

A. INTERNET OF THINGS

A widely accepted definition of the **Internet of Things (IoT)** is that it is "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [11]. Since the introduction of this definition, there has been an explosion of IoT devices, research and applications in this area [12]. IoT devices are not merely connected, but perform a wide range of sophisticated computations, including sensing [13-15], automatic control [15, 16], and the support of smart cities[15, 17-19].

One of the enablers of the IoT space is the availability and growth of cloud computing platforms, which are able to store and process the vast amounts of data generated by IoT devices [20]. This is because IoT devices and the cloud are complementary in nature. Whereas IoT devices have limited storage, computation and communication capabilities, the cloud exceeds these factors by several orders of magnitude. For instance, whereas an Amazon Blink security camera has very little storage (1Megabyte), the cloud can hold at least 2.5 exabytes of data generated daily [21]. The resulting interplay between the cloud and IoT devices has given rise to a new area of computing, termed CloudIoT [20]. In a similar vein, we will examine the confluence of blockchain and IoT in the current paper.

A growing area of research in the IoT space concerns the development of **fog networks** [22]. IoT devices are capable of generating vast amounts of data, which are typically managed by cloud computing platforms. This places heavy demands on the network communication channels and the relatively centralized cloud servers. As a way of ameliorating this problem, and making the computation and storage more decentralized, fog networks utilize more devices at the edge of the network to offload computation from the cloud servers [22]. There are interesting implications associated with such edge of the network computing, as illustrated by the Argonne National Laboratories project on the array-of-things [23-25], which uses distributed sensor arrays to enable smart cities [24]. For instance, it is not necessary for the IoT device to transmit all the data it collects to the cloud servers, and it suffices only to send data for unusual circumstances, such as a water leak on a street. This necessitates that the IoT device does its own processing and filtering before transmitting data. This ability is actually useful from a privacy point of view, as only aggregate data need to be transmitted, such as the number of people walking through a traffic intersection, and not the images of the people themselves. The Argonne Laboratories array-of-things [23-25] architecture deliberately avoids sending unnecessary and private information to the cloud. Since the computing capabilities of IoT devices are also subject to Moore's law, it is becoming very feasible for sophisticated computations including machine learning algorithms to be performed by these devices [26].

B. BLOCKCHAIN

There are many definitions of a blockchain. A relatively simple one is provided here: "A public, permanent, append-only distributed ledger" [27]. The original proposal for bitcoin and the advent of blockchain was a solution to the double-spending problem in a peer-to-peer network which does not rely on trust[28]. It does so by establishing a consensus mechanism where nodes vote with their CPU power via the computation of a proof of work in the form of an ever-increasingly more difficult to compute SHA-256 hash for a given block which is based on the work that came before it (hence the term, blockchain). A blockchain as such can be considered an append-only series of publicly owned documents whose immutability is established by the hard-to-compute SHA-256 hash chain. In this system, as long as the collective CPU power of honest nodes is greater than a given attacker's, it will be impractical for an attacker to successfully alter the course of the distributed blockchain.

Because of certain unique and desirable properties of blockchain, namely decentralization, persistency, anonymity, and auditability, the technology has been considered for a number other applications beyond finance [29]. Though in its infancy, blockchain powered smart contracts are bonafide contractual agreements guaranteed to execute on a given condition [30]. This results in generic capabilities for blockchains supporting them and lays the foundations for driving all types of services through the same decentralized, resilient network. Smart contracts however can only guarantee things as far as the blockchain can, prompting us to consider how far we can extend the cyber-physical boundary of our society. Beyond cyber currency, it might be possible to represent other societal constructs on the

blockchain[31], bringing more power to the smart contracts. One must be careful, however, in the delineating the boundaries of trustlessness, as it extends only to what can be codified by the blockchain.

Figure 2 shows a simple schematic of a blockchain, where new entries are appended to an existing list. The use of cryptographic hash functions protects combined with distributed consensus prevents potential tampering of these entries. This feature of blockchains further protects the data in the event of a cyberattack.

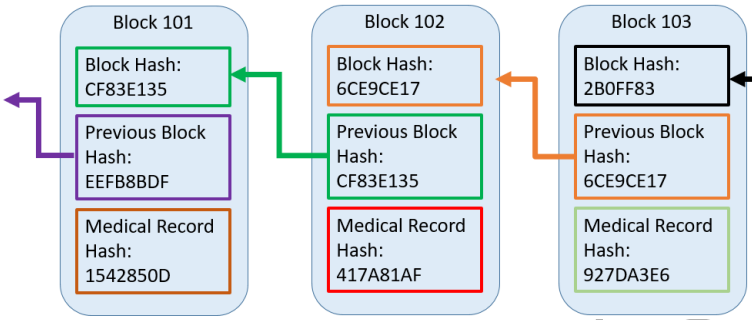


Figure 2: A simple depiction of a blockchain. For instance, we can consider each block to represent a medical record. This medical record could combine data related to patient vitals with biometrics collected by IoT devices.

C. The intersection of IoT and Blockchain

Blockchain has many potential applications in IoT, where a decentralized architecture resistant to misbehaving nodes is desirable. However, significant processing and storage requirements for blockchain make its adoption somewhat challenging. These heavy requirements are necessary for maximum security and resiliency, but architectures are beginning to emerge which make tradeoffs to make this more viable in a setting which supports low powered devices [32]. With embedded systems becoming more capable, it's only a matter of time before viability is no longer a concern.

Blockchain's security comes with numbers of diverse independent users. This is the case in IoT perhaps more-so than in its original domain, finance, given the exploding number of devices; the question remains: what can be encoded on the blockchain in the world of IoT? Besides using blockchain as a convenient fabric for which to safely store and process information collected by IoT devices, a web of IoT sensors would help bridge the gap between the cyber world and the physical one, enabling smart contracts driven by sensors. In fact, our focus application areas build off of this concept. Misbehavior in the sense of manipulation of what is captured can be mitigated, but still leaves room for device tampering. Cyber-physical systems must still be constructed carefully with thought to how readings can be scrutinized both from malfunctioning, and devices which have been tampered with. Along those lines, RFID offers a reliable way to track provenance for readings by at least providing a mechanism for asserting the origins of a reading [33].

It has been argued [34] that the blockchain provides a viable solution to managing the expanding scope and complexity of the IoT device landscape. Consumers may need to trust the IoT device manufacturers before installing and using these devices. A blockchain solves this problem by providing a scalable, trustless peer-to-peer model that is transparent and distributes data securely[34].

Smart contracts were proposed as an important use case for blockchains[7]. However, closer examination reveals that they are neither contracts in a legally enforceable sense nor smart [35]. Orcutt observed that "before smart contracts do anything really useful, they need a reliable way to connect with events in the real world, and that has proved impossible so far." A proposed solution is to have an "oracle" deliver real world events in the form of a real-time feed, such as weather information or flight information. This is where IoT devices play an important role, and could provide information to validate contractual clauses. For instance, if a container used for shipping a food product is expected to be maintained at a specified temperature, an IoT sensor can verify that this condition is met. By inserting proof of this condition at periodic intervals in a blockchain, the parties involved in the contract can verify that the contractual clause was met. This assumes that the IoT sensor itself is trusted by the parties in the contract, which is a separate issue. This issue is similar to the current debate about Huawei 5G equipment having a backdoor, which has not been decisively proven or refuted at the time this article was written [36].

Nevertheless, the use of IoT sensors offers a powerful method to make smart contracts viable, and enable many blockchain related applications. We will examine three specific application domains in this paper, which have been chosen based on their expected economic impact, and the likelihood that they will be adopted widely in the near future. The application areas are in supply chains, healthcare, and energy grids.

III. DRIVERS FOR INTEGRATION OF IOT AND BLOCKCHAIN

There is a lot of momentum in larger deployment of IoT devices, which moves computing away from centralized servers to the edge of the network. A consequence of this is that contracts and negotiations between IoT devices are arguably done better by these devices themselves, rather than involving centralized servers as the "middle-men". We examine the drivers behind the growth of IoT and blockchain.

A. The exponential growth of IoT devices

Figure 3 shows that the number of IoT devices is nearly doubling every two years, and is expected to reach 20 billion devices by the year 2020.

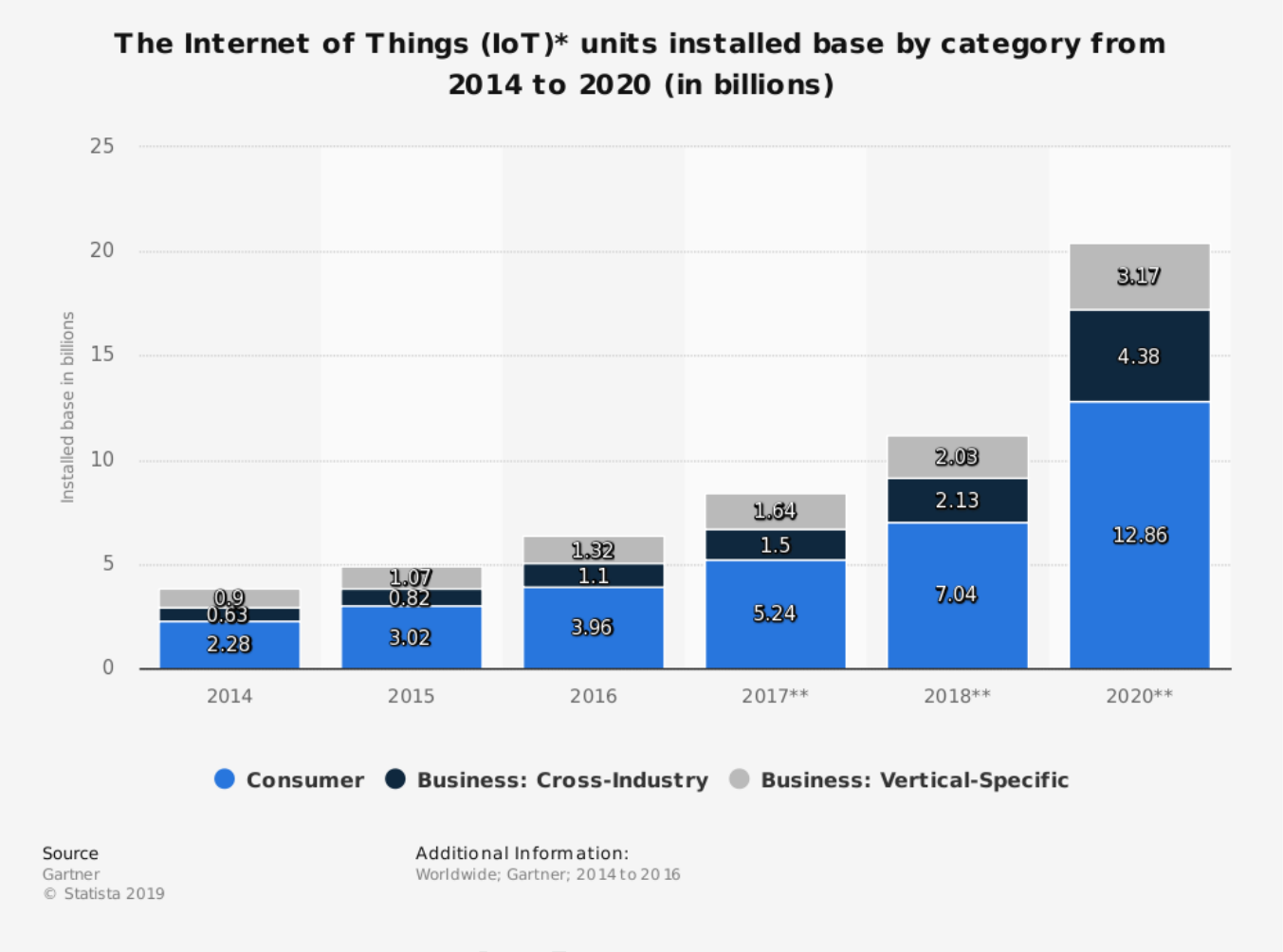


Figure 3: The growth curve for IoT devices. The expected number of IoT devices in 2020 is roughly 20 billion.

Source: https://www.statista.com/statistics/370350/internet-of-things-installed-base-by-category/ (accessible by creating a free account on statistica.com).

Though many new applications are being enabled through these devices, such as blockchain applications, it is a challenge to manage these devices at scale. The recent problems at the General Electric company [37] partly stem from a misunderstanding of the IoT business, and illustrate the issues with Industrial IoT devices such as sensors that measure jet engine performance. There is an enormous amount of data that is generated, and it is not feasible to have all this data sent to a cloud storage center, processed, and then sent back to the point of operation [38]. Furthermore, setting up storage services in-house is a challenging problem, and companies like GE may realize that it is not worthwhile to invest in building such a capability if it is available through existing cloud storage vendors[38].

The majority of IoT devices are low cost, and this puts pressure on manufacturers to include the necessary protection mechanisms to prevent cyberattacks, such as issuing regular patches and software updates [39].

B. The emergence of 5G networks

It is expected that 5G networks will become prevalent in 2019. These wireless communication networks will provide very high data rates (in the order of Gbps), low latency, and significant improvements in the quality of service. This makes it attractive to attach IoT devices to these networks for novel applications[40, 41]. Technical specifications of 5G networks may be found in survey articles [42]. 5G networks should provide peak data rates of 1Gbps for mobile users and 10 Gbps for stationary users[43, 44]. The availability of such network speeds will enable aspects of blockchain such as distributed consensus to run more efficiently.

C. Cloud Computing and Web Services

The rapid growth of cloud computing and web services has greatly reduced the need for computer processing to be done on site. Though storage and processing of generic data has been available for several years, it is only recently that specialized offerings for blockchains have come to market. For instance Amazon Web Services offers blockchain as a fully managed service [45], and this opens up a new direction for combining IoT devices with blockchain services[46].

IV. EMERGING APPLICATIONS

A. FOCUS APPLICATION #1: HEALTHCARE

Using RFID and Barcodes to tag medical devices

The FDA mandates unique device identification (UDI) for medical devices. We can create smart codes by having RFID sensors embedded in the barcode labels. RFID sensors can be used by hospitals to track medical assets easily. The medical device industry is exploring solutions that use a global RFID network for asset identification. A schematic that uses RFID and barcodes with an IoT device such as the Raspberry Pi is shown in Figure 4. This set of devices can serve as the foundation for a blockchain solution for trusted and immutable asset tracking.

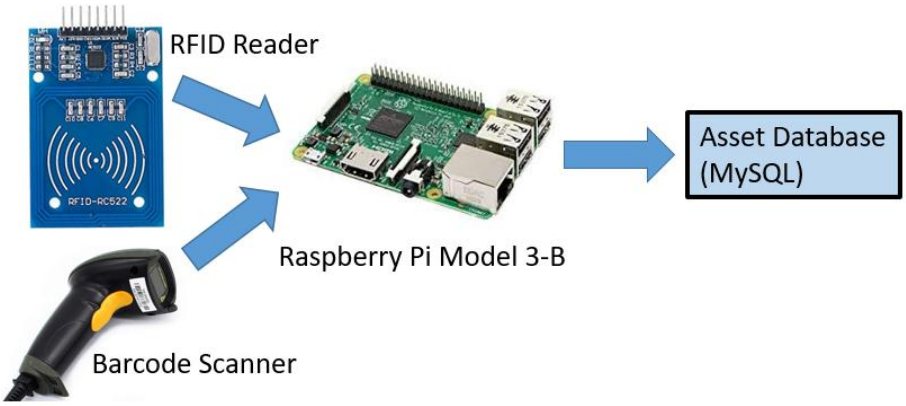


Figure 4: Using RFID readers and barcode scanners attached to an IoT device (Raspberry Pi). This can be used for device tagging in medical supply chains and for asset tracking in hospitals.

There are several open questions in the information technology space for healthcare, including the acquisition and use of biometric data for patient identification [47], the maintenance of patient privacy within an organization, and sharing of patient records securely across multiple organizations [48]. The protection of patient data across multiple IT systems creates several security challenges. Consequently, the intersection of cybersecurity, patient data and medical devices is witnessing significant growth [49, 50]. Blockchain is being proposed as a technology for sharing patient data while maintaining privacy [51].

Using patient biometrics for identification

Currently, most hospitals identify patients by their name and birthdate. This is causing increasing problems as multiple patients may have the same name and birthdate. The Wall Street Journal recently reported [47] that in a Texas healthcare system, "there are now 2,833 Maria Garcias, with 528 of them having the same date of birth." Since there is no nationally standardized approach to this problem in the USA, some hospitals are turning to biometrics for a potential solution. It is very feasible to attach a simple fingerprint reader to a Raspberry-PI. The scanned fingerprint can be converted to a private key to access medical records as shown in Figure 5.

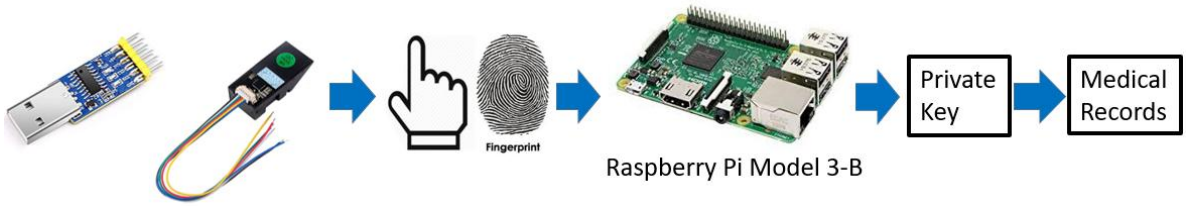


Figure 5: Biometric information (e.g. a fingerprint) can be used to access patient records

Using sensors to measure patient vitals

Furthermore, patient vitals are still usually measured by stand-alone devices without connecting them to any computer network. For instance, height, weight, blood pressure, blood glucose level, and oximeter readings are typically entered by a human into a computer.

These entries are subject to human errors, which are still occurring [47]. Using relatively inexpensive IoT devices, it is quite feasible to automatically enter this information into a patient medical record, as shown in Figure 6. The patient vitals can be part of the blockchain that constitutes the patient electronic health record [52]. This can also be combined with the patient biometric information for an end-to-end encryption [52], which provides a line of defense against cyberattacks targeting electronic health records.

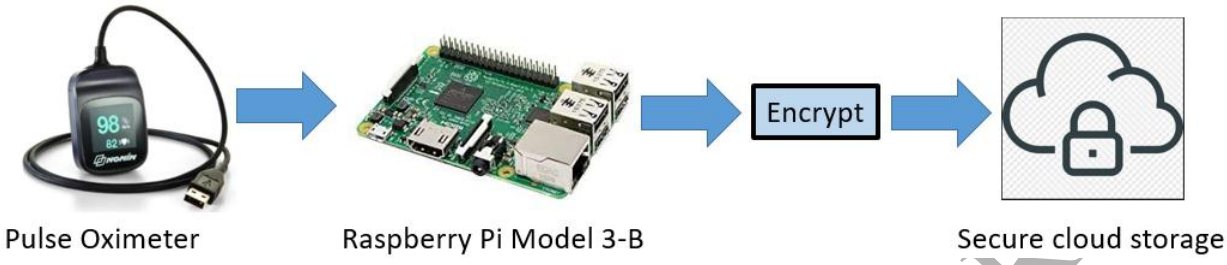


Figure 6: A pulse oximeter (e.g. Nonin or Contex CMS-50F) which provides USB and/or Bluetooth connectivity can be connected to an IoT device like the Raspberry Pi. This allows patient data to be directly stored on a computer without human intervention.

B. FOCUS APPLICATION #2: SUPPLY CHAIN

The shipping industry has been slow to adopt digital technologies, including web-based processing of information [53]. There are several barriers, including the need to obtain multiple regulatory clearances as goods move across borders [54]. Many of these clearances are paper-based, and their cost amounts to about 15-50% of the total shipping costs [54]. There are definite advantages to be gained by optimizing the global supply chain, including better inventory management, better accuracy in calculating cargo lead times, and faster fulfillment of orders. The advantages offered by blockchain technologies have provided significant momentum to the digital transformation of the shipping industry. Many contracts are still handled by human operators, leading to errors. Contracts can be managed in a smarter way, with automatic verification of information being entered into forms when containers move through multiple customs clearing areas [55]. Blockchain provides the foundation for trusted shipment documentation management, leading to a single version of truth and an immutable trail that can be promptly audited. It is also important to obtain data about the status of shipments and the condition of objects being shipped during transit. The use of IoT devices such as temperature sensors within the shipping containers and cameras can provide an audit trail that proves the contents were handled properly. The IoT devices automatically produce their data at regular intervals, and can be added to the required blockchains.

Ndraha et al. [56] review a specific challenge in the supply chain industry related to the maintenance of proper temperatures in the food supply chain. Even small temperature variations of a few degrees centigrade, where the container temperature is either higher or lower than the recommended temperature can result in spoilage of the transported food, or greatly reduce its expected shelf life. Both types of variations have been observed by Nunes [57], where cold-sensitive fruits were transported too cold, and heat-sensitive produce were transported too warm. This results in a wastage of at least 50% of the products [56]. In many cases, the basic problem is that the food supply chain operators are unaware of these temperature fluctuations and unable to react appropriately [58]. Lunden et al. [58] also estimated the duration over which the temperatures were out of range, and found that for nearly 50% of the cases, the temperature was more than 3 degrees Celsius for at least 30 minutes. Suggested solutions in the literature include temperature management control by using IoT sensors, RFID tags, and wireless sensor networks [59]. The use of blockchains offers a tamper-resistant way of capturing deviations from a desired time-temperature profile. Such deviations can be added to the blockchain as they occur, which avoids the need to continuously store sensor data. This is an example of the use of intelligence at the edge-of-the-network, which can be implemented with a few simple rules. The receiver of the container is notified of any such deviations, and the transporter is not able to conceal this information or tamper with it. With further sophistication, including utilizing training data to infer such rules, this scenario provides a path to connect artificial intelligence with blockchain technologies, as analyzed by Dinh and Thai [60] .

Even with these sensor measurements, it may be possible to thwart the monitoring system by altering the associations between the container, what it contains, and the measurements being recorded. For instance, the temperature sensor may be tracking temperature deviations in an empty container. Hence, we need a mechanism to verify that all the measurements are obtained from the true object we wish to monitor. This mechanism is discussed in the next paragraph concerning the establishment of provenance and avoidance of counterfeits.

Establishing provenance and a rightful chain of ownership is important for costly goods such as diamonds or critical items such as medicines. Traditionally, the ownership and authenticity have been established through paper certificates, which can be misplaced or tampered with. Blockchain based solutions are now available for diamonds [61]. A crucial aspect of establishing provenance is to bind the physical item to its metadata, including authenticity and certificates of origin. In the case of diamonds, this is achieved by

creating a set of physical features (forty in the solution reported in [61]) of an individual diamond and adding it to the blockchain. An ideal solution would be one where the object is physically inscribed with an immutable identification, which is then merged with its metadata. However, this is not possible for a wide range of objects, including diamonds. The next best solution appears to be one where physical features of the objects are measured and computed. IoT devices are well suited to perform these measurements and compute the required features. For instance, IoT devices such as cameras and barcode scanners can verify packaging information and the integrity of package seals during the shipment and movement of medical drugs[62]. The envisioned workflow is shown in Figure 7. This could be an enabling technology [63] to achieve the goals of the recently introduced European Union Falsified Medicines directive, which is aimed at curbing the rise of falsified medicines entering the supply chain [64].

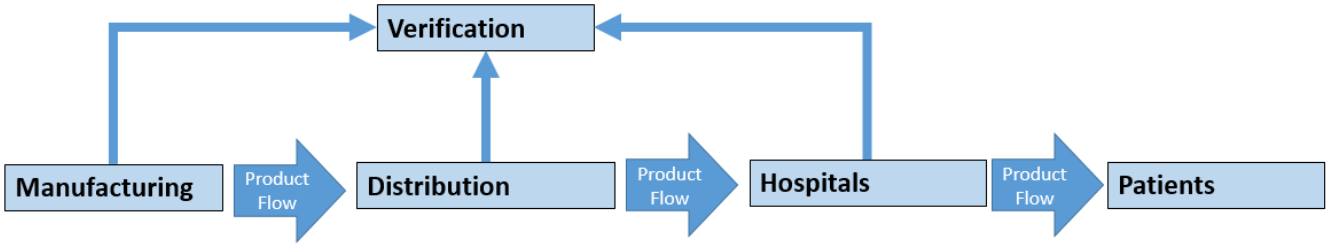


Figure 7: Product flow in a pharmaceutical supply chain. The end-to-end verification prevents the entry of counterfeits and illegal products.

A recent emerging application area is the use of blockchain technology to manage food supply chains. This helps identify sources of potential contamination so that corrective action can be applied quickly, especially in the case of food borne illnesses such as e-coli outbreaks[65]. Recent efforts include the research in [33, 66] and the pilot study being conducted by Walmart [67].

C. FOCUS APPLICATION #3: SMART ENERGY GRIDS

There is considerable interest in green and renewable energy sources today, including bio-fuels, hydroelectric, solar, and wind energy[68]. Due to encouragement from government policies, including tax rebates, solar panel installation has seen significant growth in states such as California in the USA. This has resulted in individual homeowners contributing electricity generated from solar panels into the larger electric grid [69]. However, in many cases, they may not receive the monetary compensation they expect, either in terms of the price per kilowatt-hour, or may be burdened by regulatory issues [70]. This has created the impetus for a peer-to-peer electricity trading arrangement, which is based on free market principles. An

example is the Brooklyn microgrid (www.brooklyn.energy), which is a community-powered microgrid. Though this is in very early stages, key components include the use of IoT devices for metering, and the use of blockchain for conducting transactions. The blockchain aspect of this project involves the management of contracts, and dynamically determining pricing according to the contracts. The creation of such microgrids can be especially useful developing countries, where many locations do not have well established centralized power grids[71]. Such peer-to-peer energy producing and trading systems are growing in the world, with installations in the USA, Germany and Australia[71].

From an IoT device point of view, an enabling technology is the smart electric meter[72]. There are many types of smart meters available, as reviewed in [73], and include minimum functionality smart meters, smart meters with in-home display and smart meters with a demand-control unit. Mengelkamp et al. [74] provide the architecture and technical specifications behind the Brooklyn microgrid. A pilot installation and test have revealed that blockchain combined with smart metering is able to connect all the market participants in the microgrid, and provide an operational platform. It is well-known that the pricing of energy is subject to hourly fluctuations depending on demand and supply [75]. The availability of a local energy market implies that participants have a choice of using the local grid when its price is lower than that of the external grid [74]. Furthermore, they even have the option to support the local grid and local renewable energy suppliers by paying a higher price. Hence, the availability of IoT-blockchain solutions can have significant socio-economic impact, and result in profits that stay within local communities.

Major external grid companies such as Con Edison in the New York region are planning to move their services to a distributed system model in the future [76]. One of planned components includes information sharing through an advanced metering infrastructure. This planned activity is similar to the work on the microgrid, due to the distributed nature of the transactions. Nevertheless, the energy sector seems to be challenging to penetrate due to stricter regulations. In comparison, it is easier to implement and experiment with enterprise blockchain applications such as the supply chain. The technology field is still in the early phase of testing out pilots in many promising application areas.

V. COMMON CHALLENGES

A. CYBERSECURITY CONSIDERATIONS

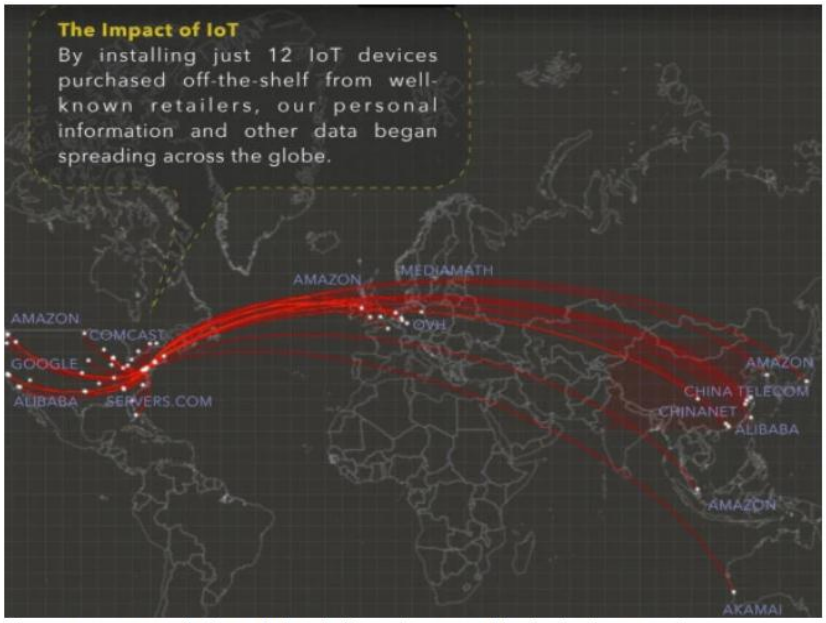
Significant research has been conducted on end-to-end encryption in sensor networks [77]. An interesting recent development in network communications is an increasing demand for end-to-end encryption driven by consumers, and their implementation by corporations. For instance, WhatsApp began end-to-end encryption of user messages only in 2016 [78]. It is important for communications between devices to be secure and protected. By using massive investments in physical infrastructure, many of the leading technology companies such as Apple, Facebook and Google are able to provide such end-to-end encryption services. However it is still challenging for independent software developers and startups to provide such capabilities in native applications. Nevertheless, negligence, when it comes to security, is still widely pervasive, and is exacerbated by the increasing number of devices potentially affected by new vulnerabilities.

The Verizon Data Breach Reports regularly disclose that negligence in applying security patches is a big contributing factor in cyberattacks. For instance, Grimes observes that "The Verizon Data Breach Report 2016 revealed that out of all detected exploits, most came from vulnerabilities dating to 2007. Vulnerabilities dating to 2003 still account for a large portion of hacks of Microsoft software. We're not talking about being a little late with patching. We're talking about persistent neglect." The Verizon Data Breach Report from 2018 [79] confirms this observation, and shows that cybercriminals continue to exploit known vulnerabilities. The Verizon Report [79] notes that "Some companies are failing to take the most basic of security measures— like keeping anti-virus software up to date." Though it is possible that a cloud service provider like Amazon could be up-to-date in applying security patches to their servers, the sheer number of IoT devices makes patching an enormous challenge. In a recent cyberattack, multiple machines including IoT devices were recruited in a coordinated fashion to create bot-nets[80], which were then used in the Dyn Distributed Denial of Service (DDoS) attack.

Given the low cost of the IoT devices that are being deployed, it is important for cryptography toolkits used in encryption and decryption to be democratized and made widely available. End-to-end encryption is by nature decentralized and doesn't require any infrastructure. The primary used encryption schemes are publicly well known and studied (e.g. RSA). With the judicious use of public and private keys, it is possible to attenuate the effect of potential cyberattacks. There are open-source cryptography toolkits being made available, along with guidelines for their usage (e.g. by virgilsecurity.com).

Figure 8 shows how easily personal information can inadvertently be spread through consumer smart-home embedded devices. Consumers purchase embedded devices from retailers, and immediately connect them to the public internet. This results in several anomalies and unexplained communications, as observed by a testing agency, Dark Cubed [39]. Thus, simply operating these devices leads to a distribution of personal data. When we consider that the expected number of IoT devices will be 20 billion by 2020 (Source: Gartner), this presents great concern to the security community. The 5G rollout occurring in 2019 will only accelerate the adoption of IoT devices. So much so

that the government of Japan has announced their intent to hack into their citizens' IoT devices to warn them of vulnerabilities before the 2020 Olympics in Tokyo[81].



Above: Pepper installed 12 off-the-shelf IoT devices and look what happened.

Image Credit: Pepper IoT

Figure 8: A recent article [39] highlights the unintended spread of personal information through IoT devices. Many of these IoT devices are insecure the moment they are installed. Since this poses security problems worldwide, it is imperative for each nation to secure its own cyberspace.

(Figure reproduced with permission from Pepper IoT).

People are already using multiple IoT devices including smartphones, fitness trackers, smart watches, and smart home appliances. This increases the number of security exposures per person. Phishing attacks are ubiquitous and occur on a daily basis, affecting all users of these devices. User privacy can be breached in totally unexpected ways, with a disturbing example offered by a fitness tracker app used by US Army personnel that revealed the location of secret army bases [82]. This story illustrates how using IoT devices such as a cellphone can result in unexpected security issues.

It is relatively easy to fix such a problem once it has been discovered. However, the preferred route is to prevent these incidents in the first place. One way to work towards prevention is to inculcate a "security mindset" in the users of these technologies. Users need to understand the mechanisms and ploys used by attackers, so they can stay alert and watchful. Educating the current generation of students at universities would be a great starting point, especially for students in STEM and engineering fields who can grasp the technicalities behind cyber-attacks. Accordingly, we have developed instructional material for detailed hands-on exercises for students in the area of cyber-security for embedded devices [83-86].

B. COMPUTATION AND STORAGE

Though the computational capabilities of IoT devices are increasing, it is still computationally intensive for such a device to participate as a node capable of adding a transaction to a blockchain. Current estimates are that it takes several minutes to add a block to bitcoin. Though permissioned blockchains can be used to speed up the addition of a new block, it is still difficult to add blocks at the speed with which IoT data can be generated. Similarly, the storage requirements will increase rapidly if additional metadata needs to be stored along with the IoT sensor data. Hence, viable solutions will require chunking of the data, or the identification of markers such as deviations from expected thresholds. In order to perform such processing, more computational power is required for the IoT or edge-of-network devices.

Though the IoT device itself may not have the required computational power, add-on devices that provide specialized processing capabilities are increasingly becoming available. For instance, the Intel Movidius neural compute stick, shown in Figure 9 implements deep neural networks in hardware, which can be used for tasks such as filtering and object detection [87]. For instance, an IoT temperature sensor can report only significant temperature deviations from an acceptable range. Similarly, an IoT camera can report only the number of people it detects, rather than the images of the people themselves. This can be integrated with the blockchain for video surveillance applications in smart cities[88].

There are increasing numbers of instances where IoT devices like the Raspberry Pi being used for process control applications in industrial manufacturing settings. For instance, Sony recently reported a 30% improvement in its processes by using about 60 Raspberry Pis in a manufacturing plant [89]. The low cost of these devices encourages more experimentation, as a potential failure does not involve excessive capital expenditures.

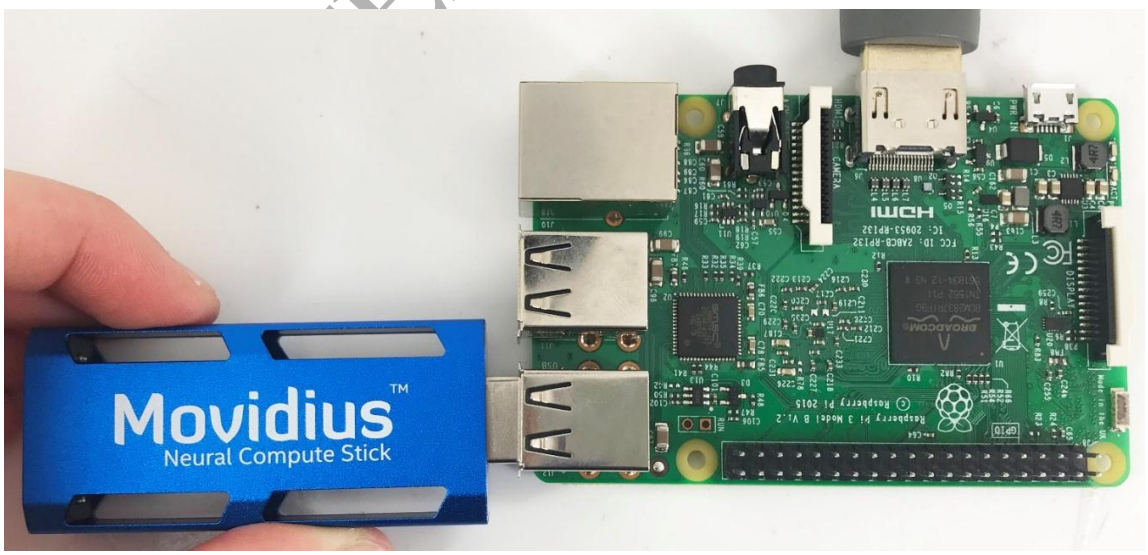


Figure 9: The Movidius neural compute stick is a low-power and small form factor device that can implement deep neural network algorithms for signal processing and image recognition. Here, a Movidius compute stick costing $75 it is shown attached to a USB port of a Raspberry Pi Model 3-B that costs $35.

C. GRANULARITY OF TRANSACTIONS

By granularity of a transaction, we refer to the resolution of the physical quantity that is metered and noted. For instance, in the realm of smart meters, we would like to determine whether we pay for the usage of 1 Watt at a time, especially if we are buying the power from suppliers that may constantly change. These are the types of details that need to be captured in the contracts. This also has implications for how frequently the blockchain ledgers will need to be updated, and whether it makes practical sense in a given domain. Also, given that such transactions need to be replicated across multiple nodes in the network, this could quickly snowball into irrelevant data being propagated and stored. It may be necessary to apply processing at the edge-of-the-network by using filters or rules. For instance, in the supply chain use case we considered earlier, the temperature can be stored only at pre-determined intervals, or if there is a deviation beyond a specified range.

Such edge-of-the-network intelligence is being utilized in the array-of-things project at the Argonne National Laboratory, where cameras at traffic intersections only count the number of pedestrians without storing pictures of individual pedestrians [90].

D. TRUST

Trust is another issue related to granularity. At what level should the party delivering the service be trusted? And at what level should the ability of the recipient of the service to pay for it be trusted? For instance, if the service provider in an electric grid wants to be to be paid for every watt of energy as and when it is delivered, then that may impose an unnecessary burden on the system. Interestingly, Amazon Web Services requires a credit card to be on file for customers who use their services, so that they are guaranteed payment.

Another issue is that there is it is difficult to establish true validation of the transaction. For instance, a service provider could transmit 10 Watts of power, and the receiver may record only 9 Watts. How does one resolve this collision? It is important for the meters need to be calibrated. We need an independent way of evaluating the amount of electricity transmitted and received. All the players in the ecosystem need to trust that. Furthermore, there could be the potential for fake devices, or it may prove very difficult to verify that a device functions exactly as specified. For instance, the evaluation of Huawei 5G equipment has proven to be very challenging, even for the security agencies of the leading powers in the world[36, 91]. Hence there is room for significant innovation in the space of IoT sensors.

These issues indicate that there may be room for rating agencies to provide information about trust. This is similar to the use of ratings for sellers and buyers in online marketplaces such as eBay[92], or that of bond credit rating agencies

such as Moody's [93]. In summary, the resolution of trust is outside the ecosystem of the blockchain. For instance the sending and receiving of a certain amount of bitcoin is guaranteed, but not the service that it may represent.

E. PRIVACY

With IoT sensors such as cameras being used to monitor traffic and pedestrians in cities, it is important for the privacy of citizens to be protected. Though law enforcement agencies may have such cameras, public service organizations such as the Robert Woods Johnson Foundation are funding efforts to monitor traffic and pedestrian flow. This leads to a better understanding of urban efficiencies, and an improvement in public health due to increased pedestrian safety and activity [94]. The technology being used is designed to protect privacy by only storing extracted features from the images, such as pedestrian counts at different times of the day. In the interest of making such data available to the public through an "open data" principle [18, 95-101], this data can be stored in a public blockchain. This not only makes the data accessible, but also elevates the level of public trust, as the data is immutable.

F. JUMPSTARTING THE ECOSYSTEM

There are very few peer reviewed research publications that present the status of current blockchain projects in the industry. As a consequence, we have to rely on reports by consulting and marketing firms. A recent Forrester report claims that 90 percent of blockchain pilots will fail [102]. Similar observations were made in a Computerworld article [103] about the lack of successful blockchain projects, and also the lack of data about the status of these projects. The overwhelming consensus seems to be to proceed with caution, as there are many more unknowns and kinks, both actual and potential. **Figure 10** illustrates the steep relative decline in interest in blockchain, though this is only through the metric of google searches. Nevertheless, the current interest appears to be comparable with other emerging technologies such as machine learning and data science, which are seeing widespread adoption and business penetration. In contrast, the technology of cloud computing is quite mature, and it is accompanied by a relatively low number of searches for this topic. A more detailed comparison would examine the trends in the publications of research papers in these areas, which may be a lagging indicator of the more widespread searches in Figure 10.

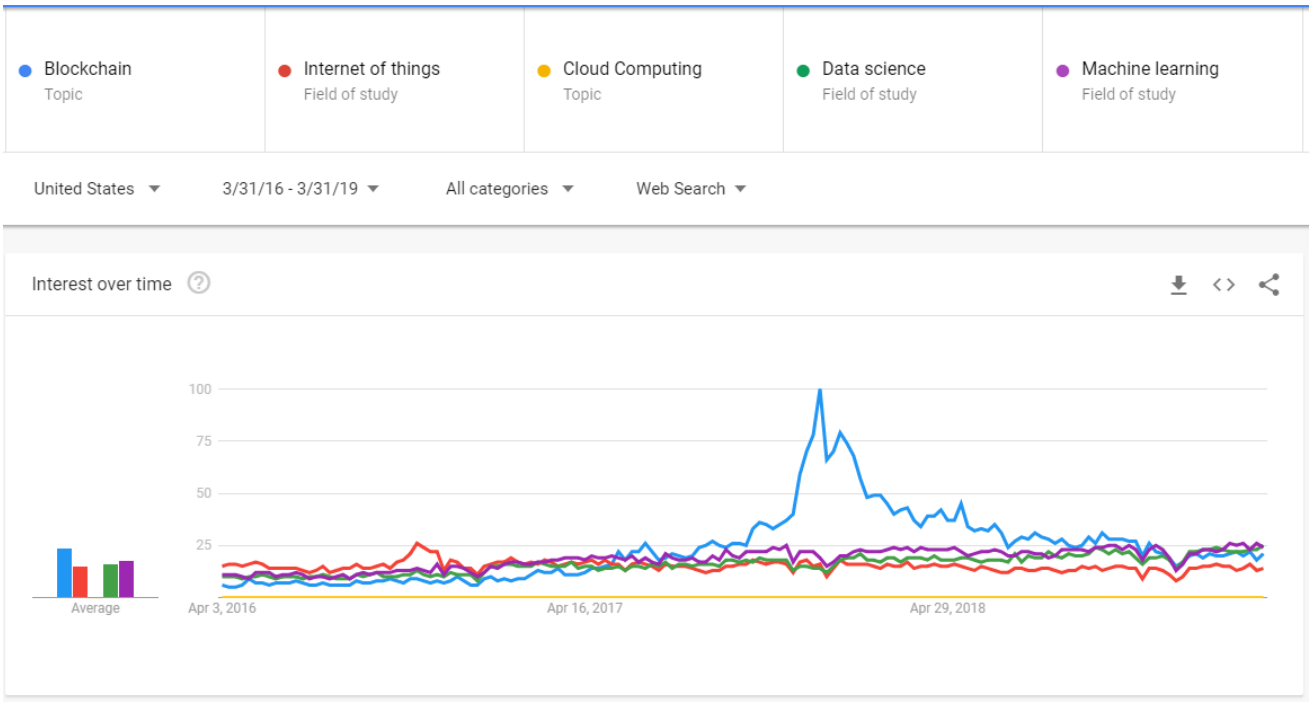


Figure 10**:** This figure shows the trends in google searches for the different topics including blockchain, and internet of things. The other topics such as cloud computing, data science and machine learning are used to gauge the interest in other popular areas in the field of computing today. A 3-year window is used for the comparison. (Data source: Google Trends, **(https://www.google.com/trends).**

These trends, and the sense of caution developing around blockchain indicate that the ecosystem needs to be jump-started with a few successful pilots, which would encourage further investment and research in this area. More fundamental research needs to be conducted, including that along the lines discussed in this paper on different applications of blockchain, and use cases with intersecting areas such as IoT and machine learning.

G. EDUCATION AND WORKFORCE TRAINING

In addition to the projected shortage of STEM (Science, Technology, Engineering, Mathematics) professionals in the USA[104], there is an even more acute shortage of professionals in areas such as cybersecurity [105] and blockchain. The rapid growth of these new technologies creates challenges from the academic and teaching viewpoint, as there is a widening gap between what the students learn in traditional courses and the cutting edge of industrial technologies. Students in the USA are already dropping from STEM majors at a high rate, and this widening gap is likely to exacerbate the problem. This necessitates rapid changes to existing curricula, and the adoption of new pedagogical techniques.

Furthermore, there is a severe lack of instructional material that offers an integrated view of emerging technologies such as the internet-of-things [12], cloud computing [106], security [107], cryptography [108], and blockchain [109]. Though there are individual books in these areas [108, 109], they may not be suitable at the undergraduate level.

Publishers are experiencing declining revenues [110] and may not be interested in creating textbook material in fast-changing fields.

An interesting development is the creation of new courses on MOOC (massively open online course) platforms such as Coursera and EdX [111]. Just in 2018 the demand for course materials in areas such as blockchain and cryptocurrency was so high that *undergraduate* students in University of California Berkeley offered a course entitled "Blockchain Fundamentals", on EdX.org in [111].

The National Security Agency in the USA has been funding efforts to develop educational materials in the areas surrounding cybersecurity [105] and cryptography. Rao et al. started using the Raspberry-Pi to develop new course material based on embedded systems, IoT and cybersecurity [84-86]. The introduction of hands-on laboratory exercises was found to significantly improve student interest, and engagement. A set of lab exercises to understand blockchain uses in IoT devices was introduced recently. These exercises help students to develop a "security mindset", which is important in the world of cybersecurity[112].

VI. OPEN ISSUES AND FUTURE DIRECTIONS

The current status of blockchain in IoT resembles the classic chicken-and-egg problem. Companies and individuals will not use blockchain unless there is demonstrated value and an obvious return-on-investment. However, it is difficult to generate value unless a sufficient number of applications are deployed, and economies of scale have been established.

This indicates that a necessary milestone is that successful pilot projects are executed. Some areas where this is close to happening is the accounting sector and retail applications. Walmart and IBM have reported that their food supply chain project will exit the pilot phase in 2019 [67].

A challenge with deploying blockchain in the energy sector through decentralized smart meters is government regulation. The developers of this technology may not be able to seamlessly scale and deploy this technology worldwide, as regulations vary from country to country. Furthermore, energy transfer across international borders such as through an electric grid is also highly regulated. For this reason, many blockchain startups in the field of energy are struggling to establish a viable business model [71, 74].

The promise of decentralized solutions to transactive energy are likely to be realized in the longer term, after a five-year timeframe. This is because energy companies like ConEdison are first tackling lower complexity problems such as automating internal business processes, and working with ESCOs (Energy supply companies) to integrate them seamlessly into the energy supply chain. There is a more attractive return-on-investment and shorter term viability for such projects. In addition, data exchange and privacy issues need to be resolved.

Enterprise blockchain is a potentially easier application of blockchain and IoT. The tracking of inventory is an important problem. RFID tags have become popular in this space, and constitute an enabling technology [33]. Some RFID tags are passive. It is possible to use active tags that can communicate with a server or peers and disclose the contents of a package. Maersk Shipping is using blockchain for managing shipping of containers [54].

The issue of a private (or permissioned) versus public blockchain is important. Early adopters in the energy sectors are finding out that a public blockchain (based on ether) is too expensive as a mechanism to pay for contracts. Hence, many entities are using private implementations of ether so that they can control transaction costs [113]. Another potential solution is to use intranets, as details for data sharing on public blockchains have yet to be worked out [114]. Hence, it is easier to start with deployments on intranets first.

In the energy sector, the energy grid is actually private, as users need to be registered to connect to the grid. Hence a private structure is appropriate for the energy grid. Furthermore, there are different latency expectations for applications running at different portions of the energy grid. At the edge of the grid, transactions may need to be very fast, for instance, negotiations may need to be conducted rapidly before a fuse is blown. However, the speed of transactions between two substations could be slower as larger loads may not fluctuate as quickly. This implies that one can utilize two separate blockchains with different latency requirements. These ideas need to be implemented and tested out, which necessitates a significant amount of experimentation in real marketplaces.

Finally, a gray zone is that of legal enforcement of blockchain contracts. The legal framework needs to be expanded to handle use cases based on blockchains, and this is a very new area [115]. The speed of technological advancement in this area has been very fast, and the existing contract laws have not kept pace. This requires the cultivation of experts conversant both with the capabilities of blockchain and an understanding of the legal world. Hence, we need a regulatory sandbox for business model development.

One of the implications of a blockchain enabled ecosystem is that accounting ledgers may need to be held on indefinitely. In the case of IoT devices, this requires the accounting data to be offloaded from the IoT device to local or remote servers. Some open questions are: at what level of detail should this data be collected and stored, and at

what temporal frequency (e.g. every millisecond, or second, or minute, or hour)? Though storage costs are shrinking rapidly, the solution providers need to determine where and when this data is stored.

One relevant technology in this context is that of fog networks [22], where the multitude of devices in a connected home pool their storage and computation resources together. There is a significant amount of unused storage and computation on many IoT devices, including laptops, refrigerators, personal assistants such as Alexa, and cell-phones within a home. If the capabilities within these devices are harnessed in a coordinated fashion, the limitation of a single device can be overcome.

Another aspect to keep in mind is that processing power, storage and memory size are all increasing according to Moore's law. So a solution that is not possible with today's devices may become viable in the longer term. The underlying technology can be developed and tested, and widespread deployment could possibly take a decade or more. This is a common theme in the development of technologies such as the internet, which took a long time to develop, but exploded once it started seeing wider adoption.

The granularity of IoT device participation in the blockchain is an important design issue. For instance, should a smart thermostat be directly connected to the energy grid, or should it communicate data to a centralized server in the basement of a home? The home server can then participate in blockchain transactions with other homes or the utility service provider. This shows that total decentralization may not be necessary, where every single IoT device participates in transactions.

The recent cyberattack [116] on IoT devices demonstrates the vulnerability of these devices. There are various levels at which the IoT devices can be compromised, from totally disabling them to rigging them so false data is provided. For instance, a thermostat can be hacked to provide wrong temperature values, which then has an adverse effect on the energy grid. Hence there are many physical variables that are measured by IoT devices that are not part of the blockchain environment. This is a compromised situation that is outside end-to-end encryption channels or the security provided by blockchain transactions.

Similarly, the trust that exists when you provided an expected service to another party is outside the scope of blockchain transactions. The blockchain cannot verify that you actually provided the service that meets a service level agreement. This is especially true in more complex transactions that may involve human labor.

The extraction of commercial value from the data generated by IoT devices has proven to be challenging. GE had high expectations of creating a predictive analytics platform that utilized data from industrial IoT devices [54, 117]. This did not materialize as envisioned, and the reasons are complex, ranging from the core technical challenges to

make this happen to marketing issues. This has resulted in a scaling back of expectations being scaled back, and an extension of the time horizon. As a result, GE is focusing on specific use cases rather than trying to build a generic platform. This case study is relevant to the broad issues discussed in the current paper, as a cautious approach is likely to be used by the early adopters.

In the area of logistics and supply chain management, Kersten et al. [118] note that logistics companies, especially the smaller and medium sized companies have very limited expertise in blockchains. Though companies such as Cargosmart [55] are creating specialized offerings to fill this void, the larger logistics and shipping companies are reluctant to experiment with newer technologies [53].

It is possible to establish provenance for expensive items like diamonds by using IoT devices to measure a wide range of object features. The cost of the IoT devices can be justified in such a business solution. However, the use of IoT devices in containers for perishable food items may take longer to get established. Even though IoT devices and sensors are getting cheaper, retailers are constantly cutting costs and will be reluctant to utilize solutions without demonstrable cost savings [119].

VII. CONCLUSION

The number of IoT devices has increased greatly, and is accompanied by increases in processing power and 5G networking speeds. Since it is becoming difficult to have centralized computational models in this environment, we are witnessing a shift to decentralized models. There are additional requirements that users seek, including privacy, trust, and immutability of stored information. These requirements can be met with blockchain technology. The intersection of IoT with blockchain provides potential solution paths to existing problems with smart contracts, where the boundaries of cyber physical systems need to be better defined. IoT sensors can verify information contained in smart contract clauses by providing continuous measurements from the physical world. We examined three specific scenarios consisting of healthcare applications, supply chain applications and smart energy applications. In each of these scenarios we highlighted the interplay between IoT devices and the blockchain. We also outlined several existing problems that need careful research. By advancing such research, we expect that fruitful progress can be made in realizing the full potential of the confluence of IoT with blockchain technology.

ACKNOWLEDGMENTS

CONFLICT OF INTEREST STATEMENT

The authors indicate that they have no conflicts of interest.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, pp. 2347-2376, 2015.

[2] (2018). *MIT Technology Review: The Blockchain Issue*. Available: https://www.technologyreview.com/magazine/2018/05/

[3] L. Mearian. (2018). *IoT could be the killer app for blockchain*.

[4] H. Subramanian, "Decentralized blockchain-based electronic marketplaces," *Commun. ACM*, vol. 61, pp. 78-84.

[5] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Banking beyond banks and money*, ed: Springer, 2016, pp. 239-278.

[6] A. Tapscott and D. Tapscott, "How blockchain is changing finance," *Harvard Business Review*, vol. 1, 2017.

[7] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292-2303, 2016.

[8] P. De Filippi, "The interplay between decentralization and privacy: the case of blockchain technologies," 2016.

[9] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, 2016, pp. 1-6.

[10] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979-33001, 2018.

[11] "Internet of things in 2020: a roadmap for the future," INFSO D.4 NETWORKED ENTERPRISE & RFID INFSO G.2 MICRO & NANOSYSTEMS, in co-operation with the RFID WORKING GROUP OF THE EUROPEAN TECHNOLOGY PLATFORM ON SMART SYSTEMS INTEGRATION (EPOSS), 5 September, 2008.

[12] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, pp. 2787-2805, 2010.

[13] M. Lee, J. Hwang, and H. Yoe, "Agricultural production system based on IoT," in *Computational Science and Engineering (CSE), 2013 IEEE 16th International Conference on*, 2013, pp. 833-837.

[14] G. Zhang, C. Li, Y. Zhang, C. Xing, and J. Yang, "SemanMedical: A kind of semantic medical monitoring system model based on the IoT sensors," in *e-Health Networking, Applications and Services (Healthcom), 2012 IEEE 14th International Conference on*, 2012, pp. 238-243.

[15] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Sensing as a service model for smart cities supported by internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 25, pp. 81-93, 2014.

[16] J.-c. Zhao, J.-f. Zhang, Y. Feng, and J.-x. Guo, "The study and application of the IOT technology in agriculture," in *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, 2010, pp. 462-465.

[17] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things journal*, vol. 1, pp. 22-32, 2014.

[18] B. Ahlgren, M. Hidell, and E. C.-H. Ngai, "Internet of things for smart cities: Interoperability and open data," *IEEE Internet Computing*, pp. 52-56, 2016.

[19] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-things-based smart cities: Recent advances and challenges," *IEEE Communications Magazine*, vol. 55, pp. 16-24, 2017.

[20] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," *Future Generation Computer Systems*, vol. 56, pp. 684-700, 2016.

[21] R. Jacobson. (July 1). *2.5 quintillion bytes of data created every day. How does CPG & Retail manage it?*

[22] H. Zhang, Y. Xiao, S. Bu, D. Niyato, F. R. Yu, and Z. Han, "Computing resource allocation in three-tier IoT fog networks: A joint optimization approach combining Stackelberg game and matching," *IEEE Internet Things J.*, vol. 4, pp. 1204-1215, 2017.

[23] (2018). *Array of Things*.

[24] S. Jernigan, S. Ransbotham, and D. Kiron, "Data sharing and analytics drive success with IOT," *MIT Sloan Management Review (September 2016)*, 2016.

[25] R. L. Jacob, C. Catlett, P. Beckman, and R. Sankaran, "Early results from the Array of Things," in *AGU Fall Meeting Abstracts*, 2017.

[26] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE communications surveys & tutorials*, vol. 16, pp. 414-454, 2014.

[27] (2018, Explainer: What is a blockchain? *MIT Technology Review*, *https://www.technologyreview.com/s/610833/explainer-what-is-a-blockchain/*.

[28] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[29] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, pp. 352-375, 2018.

[30] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy (SP)*, 2016, pp. 839-858.

[31] F.-Y. Wang, "The emergence of intelligent enterprises: From CPS to CPSS," *IEEE Intelligent Systems*, vol. 25, pp. 85-88, 2010.

[32] K. R. Özyılmaz and A. Yurdakul, "Integrating low-power iot devices to a blockchain-based infrastructure: work-in-progress," in *Proceedings of the Thirteenth ACM International Conference on Embedded Software 2017 Companion*, 2017, p. 13.

[33] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *2016 13th international conference on service systems and service management (ICSSSM)*, 2016, pp. 1-6.

[34] P. Brody and V. Pureswaran, "Device democracy: Saving the future of the internet of things," *IBM, September*, 2014.

[35] M. Durovic and A. Janssen, "The Formation of Blockchain-based Smart Contracts in the Light of Contract Law," *European Review of Private Law*, vol. 26, pp. 753-771, 2018.

[36] A. Satariano, "Huawei Security 'Defects' Are Found by British Authorities," in *New York Times*, ed, 2019.

[37] Dana Cimilluca, D. Mattioli, and T. Gryta, "GE Puts Digital Assets on the Block," in *Wall Street Journal*, ed, 2018.

[38] D. Tokar. (2018, Dec 13, 2018) Three Recommendations For GE's Newly Formed Industrial IoT Software Company. *Forbes*.

[39] D. Takahashi. (2019, Jan 29, 2019) Smart devices aren't so bright when it comes to security. Available: https://venturebeat.com/2019/01/29/pepper-iot-smart-devices-arent-so-bright-when-it-comes-to-security/

[40] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619-3647, 2018.

[41] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *Journal of Industrial Information Integration*, vol. 10, pp. 1-9, 2018.

[42] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 18, pp. 1617-1655, 2016.

[43] I. Chih-Lin, S. Han, Z. Xu, Q. Sun, and Z. Pan, "5G: rethink mobile communications for 2020+," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 374, p. 20140432, 2016.

[44] E. J. Oughton and Z. Frias, "The cost, coverage and rollout implications of 5G infrastructure in Britain," *Telecommunications Policy*, vol. 42, pp. 636-652, 2018.

[45] *Blockchain on AWS: Easily build scalable blockchain and ledger solutions*. Available: https://aws.amazon.com/blockchain/

[46] M. Samaniego and R. Deters, "Hosting virtual iot resources on edge-hosts with blockchain," in *2016 IEEE International Conference on Computer and Information Technology (CIT)*, 2016, pp. 116-119.

[47] B. Gormley, "Hospitals Turn to Biometrics to Identify Patients," in *Wall Street Journal*, ed, 2019.

[48] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE transactions on parallel and distributed systems*, vol. 24, pp. 131-143, 2013.

[49] K. Fu and J. Blum, "Inside risks controlling for cybersecurity risks of medical device software," *Communications of the ACM*, vol. 56, 2013.

[50] E. D. Perakslis and M. Stanley, "A cybersecurity primer for translational research," *Science translational medicine*, vol. 8, pp. 322ps2-322ps2, 2016.

[51] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications policy*, vol. 41, pp. 1027-1038, 2017.

[52] D. Augot, H. Chabanne, T. Chenevier, W. George, and L. Lambert, "A user-centric system for verified identities on the bitcoin blockchain," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, ed: Springer, 2017, pp. 390-407.

[53] E. Samwel, "Redefining e-commerce," *Containerisation International*, vol. 41, 2008.

[54] N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: trick or treat?," in *Proceedings of the Hamburg International Conference of Logistics (HICL)*, 2017, pp. 3-18.

[55] Cargosmart, "CargoSmart Launches Blockchain Initiative to Simplify Shipment Documentation Processes," in *Global Newswire*, ed, 2018.

[56] N. Ndraha, H.-I. Hsiao, J. Vlajic, M.-F. Yang, and H.-T. V. Lin, "Time-temperature abuse in the food cold chain: Review of issues, challenges, and recommendations," *Food control*, vol. 89, pp. 12-21, 2018.

[57] M. C. N. Nunes, J. P. Emond, M. Rauth, S. Dea, and K. V. Chau, "Environmental conditions encountered during typical consumer retail display affect fruit and vegetable quality and waste," *Postharvest Biology and Technology*, vol. 51, pp. 232-241, 2009.

[58] J. Lundén, V. Vanhanen, T. Myllymäki, E. Laamanen, K. Kotilainen, and K. Hemminki, "Temperature control efficacy of retail refrigeration equipment," *Food control*, vol. 45, pp. 109-114, 2014.

[59] K. P. Koutsoumanis and M. Gougouli, "Use of time temperature integrators in food safety management," *Trends in Food Science & Technology*, vol. 43, pp. 236-244, 2015.

[60] T. N. Dinh and M. T. Thai, "Ai and blockchain: A disruptive integration," *Computer*, vol. 51, pp. 48-53, 2018.

[61] N. Lomas, "Everledger is using blockchain to combat fraud, starting with diamonds," *URL: https://techcrunch. com/2015/06/29/everledger*, 2015.

[62] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain," in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2017, pp. 772-777.

[63] N. Alzahrani and N. Bulusu, "Block-supply chain: a new anti-counterfeiting supply chain using NFC and blockchain," in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 2018, pp. 30-35.

[64] S. Houlton, "Tackling the problem of falsified medicines in the UK," *Prescriber*, vol. 29, pp. 33-35, 2018.

[65] S. Luna, V. Krishnasamy, L. Saw, L. Smith, J. Wagner, J. Weigand, *et al.*, "Outbreak of E. coli O157: H7 Infections Associated with Exposure to Animal Manure in a Rural Community—Arizona and Utah, June–July 2017," *Morbidity and Mortality Weekly Report*, vol. 67, p. 659, 2018.

[66] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation," in *2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany)*, 2018, pp. 1-4.

[67] B. Tan, J. Yan, S. Chen, and X. Liu, "The Impact of Blockchain on Food Supply Chain: The Case of Walmart," in *International Conference on Smart Blockchain*, 2018, pp. 167-177.

[68] E. S. Shuba and D. Kifle, "Microalgae to biofuels:'Promising'alternative and renewable energy, review," *Renewable and Sustainable Energy Reviews*, vol. 81, pp. 743-755, 2018.

[69] T. von Wirth, L. Gislason, and R. Seidl, "Distributed energy systems on a neighborhood scale: Reviewing drivers of and barriers to social acceptance," *Renewable and Sustainable Energy Reviews*, vol. 82, pp. 2618-2628, 2018.

[70] M. Muro and D. Saha. Rooftop solar: Net metering is a net benefit [Online]. Available: https://www.brookings.edu/research/rooftop-solar-net-metering-is-a-net-benefit/

[71] D. Cardwell, "Solar Experiment Lets Neighbors Trade Energy Among Themselves," in *New York Times*, ed, 2017.

[72] S. Blumsack and A. Fernandez, "Ready or not, here comes the smart grid!," *Energy*, vol. 37, pp. 61-68, 2012.

[73] E. Andrey and J. Morelli, "Design of a smart meter techno-economic model for electric utilities in Ontario," in *2010 IEEE Electrical Power & Energy Conference*, 2010, pp. 1-7.

[74] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: A case study: The Brooklyn Microgrid," *Applied Energy*, vol. 210, pp. 870-880, 2018.

[75] A. Ghasemi, H. Shayeghi, M. Moradzadeh, and M. Nooshyar, "A novel hybrid algorithm for electricity price and load forecasting in smart grids with demand-side management," *Applied energy*, vol. 177, pp. 40-59, 2016.

[76] (2018). *Distributed system platform*. Available: https://www.coned.com/en/our-energy-future/our-energy-projects/distribution-system-platform

[77] Y. Sang, H. Shen, Y. Inoguchi, Y. Tan, and N. Xiong, "Secure data aggregation in wireless sensor networks: A survey," in *Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT'06. Seventh International Conference on*, 2006, pp. 315-320.

[78] K. Ermoshina, F. Musiani, and H. Halpin, "End-to-end encrypted messaging protocols: An overview," in *International Conference on Internet Science*, 2016, pp. 244-254.

[79] (2018). *Verizon 2018 Data Breach Investigations Report*. Available: https://enterprise.verizon.com/resources/reports/dbir/

[80] B. Rashidi, C. Fung, and E. Bertino, "A collaborative DDoS defence framework using network function virtualization," *IEEE Transactions on Information Forensics and Security*, vol. 12, pp. 2483-2497, 2017.

[81] C. Cimpanu, "Japanese government plans to hack into citizens' IoT devices," in *Zdnet*, ed. zdnet.com, 2019.

[82] A. Hern, "Fitness tracking app Strava gives away location of secret US army bases," in *The Guardian*, ed, 2018.

[83] A. R. Rao and R. Dave, "Developing hands-on laboratory exercises for teaching STEM students the internet-of-things, cloud computing and blockchain applications," in *IEEE Integrated STEM Education Conference*, Princeton, NJ, 2019.

[84] A. R. Rao, D. Clarke, and N. Mohammed, "Creating an anchor hands-on cybersecurity course using the Raspberry Pi," in *Colloquium for Information Systems Security Education (CISSE)*, New Orleans, 2018.

[85] A. R. Rao, D. Clarke, D. Yeskepalli, and M.-R. Mallu, "Teaching cybersecurity concepts through Internet-of-things applications based on the Raspberry Pi," in *Colloquium for Information Systems Security Education (CISSE)*, New Orleans, 2018.

[86] A. R. Rao, D. Clarke, M. Bhadiyadra, and S. Phadke, "Development of an Embedded System Course to Teach the Internet-of-Things," in *IEEE STEM Education Conference, ISEC*, Princeton, 2018, pp. 154-160.

[87] M. H. Ionica and D. Gregg, "The movidius myriad architecture's potential for scientific computing," *IEEE Micro*, vol. 35, pp. 6-14, 2015.

[88] P. Gallo, S. Pongnumkul, and U. Q. Nguyen, "BlockSee: Blockchain for IoT Video Surveillance in Smart Cities," in *2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*, 2018, pp. 1-6.

[89] P. Olson. (2019, March 10, 2019) How Sony Sped Up A Factory With These Tiny, $35 Computers. *Forbes*.

[90] C. E. Catlett, P. H. Beckman, R. Sankaran, and K. K. Galvin, "Array of things: a scientific research instrument in the public way: platform design and early lessons learned," in *Proceedings of the 2nd International Workshop on Science of Smart City Operations and Platforms Engineering*, 2017, pp. 26-33.

[91] B. Pancevski and S. Germano, "In Rebuke to U.S., Germany Considers Letting Huawei In," in *Wall Street Journal*, ed, 2019.

[92] D. Gregg and M. Parthasarathy, "Factors affecting the long-term survival of eBay ventures: a longitudinal study," *Small Business Economics*, vol. 49, pp. 405-419, 2017.

[93] M. Adelino, I. Cunha, and M. A. Ferreira, "The economic effects of public financing: Evidence from municipal bond ratings recalibration," *The Review of Financial Studies*, vol. 30, pp. 3223-3268, 2017.

[94] (2018). *Technology for healthy communities*. Available: http://www.communityhealthtech.org/pilots

[95] S. Baack, "Datafication and empowerment: How the open data movement re-articulates notions of democracy, participation, and journalism," *Big Data & Society*, vol. 2, p. 2053951715594634, 2015.

[96] R. Kitchin, *The data revolution: Big data, open data, data infrastructures and their consequences*: Sage, 2014.

[97] E. G. Martin, N. Helbig, and N. R. Shah, "Liberating data to transform health care: New york's open data experience," *Jama*, vol. 311, pp. 2481-2482, 2014.

[98] T. Davies and F. Perini, "Researching the emerging impacts of open data: revisiting the ODDC conceptual framework," *The Journal of Community Informatics*, vol. 12, 2016.

[99] T. Jetzek, *The Sustainable Value of Open Government Data: Uncovering the Generative Mechanisms of Open Data through a Mixed Methods Approach*: Copenhagen Business SchoolCopenhagen Business School, Institut for IT-LedelseDepartment of IT Management, 2015.
[100] P. Conradie and S. Choenni, "On the barriers for local government releasing open data," *Government Information Quarterly*, vol. 31, pp. S10-S17, 2014.
[101] G. Boulton, M. Rawlins, P. Vallance, and M. Walport, "Science as a public enterprise: the case for open data," *The Lancet*, vol. 377, pp. 1633-1635, 2011.
[102] O. Kharif, "Blockchain, Once Seen as a Corporate Cure-All, Suffers Slowdown," in *Bloomberg.com*, ed, 2018.
[103] L. Mearian. (2018) Blockchain: What's it good for? Absolutely nothing, report finds. *Computerworld*. Available: https://www.computerworld.com/article/3324359/blockchain-what-s-it-good-for-absolutely-nothing-report-finds.html
[104] (2016, 3/17/18). *US. Department of Education, https://innovation.ed.gov/files/2016/09/AIR-STEM2026_Report_2016.pdf*.
[105] "Cybersecurity Workforce Education - CNAP Initiatives' Number H98230- I 7- I -032. "Developing Hands-on Exercises for Secure Embedded System Design & Security Data Analytics for Computing and Engineering Students.", CNAP-CAE CNAP-CAE2017 Grant# H98230-17-1-0321.," ed: National Security Agency, 2017.
[106] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, *et al.*, "A view of cloud computing," *Communications of the ACM*, vol. 53, pp. 50-58, 2010.
[107] P. W. Singer and A. Friedman, *Cybersecurity: What everyone needs to know*: Oxford University Press, 2014.
[108] Y. Lindell and J. Katz, *Introduction to modern cryptography*: Chapman and Hall/CRC, 2014.
[109] M. Swan, *Blockchain: Blueprint for a new economy*: " O'Reilly Media, Inc.", 2015.
[110] C. Straumsheim. (2017, January 31, 2017) Is 'Inclusive Access' the Future for Publishers? Available: https://www.insidehighered.com/news/2017/01/31/textbook-publishers-contemplate-inclusive-access-business-model-future
[111] L. Mearian. (2018, June 19, 2018) UC Berkeley puts blockchain training online; thousands sign up. *Computerworld*. Available: https://www.computerworld.com/article/3282791/blockchain/uc-berkeley-puts-blockchain-training-online-thousands-sign-up.html
[112] S. Hooshangi, R. Weiss, and J. Cappos, "Can the security mindset make students better testers?," in *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, 2015, pp. 404-409.
[113] W. Li, A. Sforzin, S. Fedorov, and G. O. Karame, "Towards scalable and private industrial blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, 2017, pp. 9-14.
[114] M. Ferguson, "Preparing for a Blockchain Future," *MIT Sloan Management Review*, vol. 60, pp. 1-4, 2018.
[115] G. Governatori, F. Idelberger, Z. Milosevic, R. Riveret, G. Sartor, and X. Xu, "On legal contracts, imperative and declarative smart contracts, and blockchain systems," *Artificial Intelligence and Law*, vol. 26, pp. 377-409, 2018.
[116] K. Bhardwaj, J. C. Miranda, and A. Gavrilovska, "Towards IoT-DDoS Prevention Using Edge Computing," in *{USENIX} Workshop on Hot Topics in Edge Computing (HotEdge 18)*, 2018.
[117] K. Moskvitch, "When machinery chats [Connections Industrial IOT]," *Engineering & Technology*, vol. 12, pp. 68-70, 2017.
[118] W. Kersten, M. Seiter, B. von See, N. Hackius, and T. Maurer, "Trends and Strategies in Logistics and Supply Chain Management–Digital Transformation Opportunities," *BVL International*, 2017.
[119] M. Hingley, A. Lindgreen, D. B. Grant, and C. Kane, "Using fourth-party logistics management to improve horizontal collaboration among grocery retailers," *Supply Chain Management: An International Journal*, vol. 16, pp. 316-327, 2011.