EDITORS: Rick Kuhn, NIST, kuhn@nist.gov
Tim Weil, Scram Systems, tweil.ieee@gmail.com

Can Blockchain Strengthen the Internet of Things?

Nir Kshetri, *University of North Carolina at Greensboro*

Blockchain—a kind of distributed ledger technology—has been described in the popular press as the next big thing. Put simply, a blockchain is a data structure that makes it possible to create a tamper-proof digital ledger of transactions and share them. This technology uses public-key cryptography to sign transactions among parties. The transactions are then stored on a distributed ledger. The ledger consists of cryptographically linked blocks of transactions, which form a blockchain (bit.ly/2sgabnq). It is impossible or extremely difficult to change or remove blocks of data that are recorded on the blockchain ledger.

Regarding the question of whether blockchain can strengthen the Internet of Things (IoT), the answer—based on this research—is "maybe." Observers have noted that the blockchain–IoT combination is powerful and is set to transform many industries.[1] For instance, IoT devices can carry out autonomous transactions through smart contracts.[2] Combined with artificial intelligence (AI) and big data solutions, more significant impacts can be produced.

A natural question is thus what roles can blockchain play in strengthening IoT security? To demonstrate this problem's significance, consider the following example. In October 2016, the US-based DNS provider Dyn faced cyberattacks. Dyn said the attacks originated from "tens of millions of IP addresses,"[3] and at least some of the traffic came from IoT devices, including webcams, baby monitors, home routers, and digital video recorders.[4] These IoT devices had been infected with malware called Mirai, which controls online devices and uses them to launch distributed denial-of-service (DDoS) attacks. The process involves phishing emails to infect a computer or home network. Then the malware spreads to other devices, such as DVRs, printers, routers, and Internet-connected cameras employed by stores and businesses for surveillance.[5]

From a security standpoint, a main drawback of IoT applications and platforms is their reliance on a centralized cloud. A decentralized, blockchain-based approach would overcome many of the problems associated with the centralized cloud approach. Some point out that blockchain could provide military-grade security for IoT devices.[6] There is no single point of failure or vulnerability in blockchain, except with the clock needed for time stamping.

Considering these observations, this column provides insights into ways in which blockchain might strengthen IoT security.

Incorporating Blockchain into IoT Security

Blockchain's incorporation into IoT is being supported through a wide variety of measures intended to strengthen security. Several companies are leading initiatives to integrate blockchain into their production and supply chains. For instance, IBM is using its large cloud infrastructure to provide

Published by the IEEE Computer Society

blockchain services for tracking high-value items as they move across supply chains.

The IBM Watson IoT Platform's built-in capability also allows users to add selected IoT data to private blockchain ledgers that 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 to satisfy the contract (ibm.co/2rJWCPC). All business partners can access and supply IoT data in a decentralized fashion and can verify each transaction.[7] Data is not collected, stored, or managed centrally. Rather, it is protected and shared among only the parties involved in the transaction.

Startups such as Provenance use blockchain to promote trust in the supply chain by providing transparency and visibility when the product moves from the source to the customer.[8] Others are creating new business models that eliminate the need for centralized cloud servers. For example, Filament, a blockchain-based solutions provider for IoT, has launched wireless sensors, called Taps, that allow communication with computers, phones, or tablets within 10 miles (bit.ly/2rsxZYf).

Taps create low-power, autonomous mesh networks that enable companies to manage physical mining operations or water flows over agricultural fields. Taps don't rely on cloud services. Device identification and intercommunication is secured by a blockchain that holds the unique identity of each participating node.[9] One key application is likely to be in the next generation of the industrial network (the Industrial Internet). Filament's blockchain-based applications involve sensors connected in a decentralized system and use autonomous smart contracts. This means that devices communicate securely with each other, exchange values, and execute actions automatically. For instance, Filament's Tap can be attached to drilling rigs in remote locations. Based on predefined conditions, a rig might know that it requires a piece of machinery and thus might send a request to an autonomous drone.[10]

Measures are also taken at interorganizational levels. A group of technology and financial companies have announced that they have formed a group to set a new standard for securing IoT applications using blockchain. Companies joining the group include Cisco, Bosch, Bank of New York Mellon, Foxconn Technology, Gemalto, and blockchain startups Consensus Systems, BitSE, and Chronicled.[11] This group hopes to establish a blockchain protocol to build IoT devices, applications, and networks.[12]

Blockchain-based identity and access management systems can be leveraged to strengthen IoT security.

Identity and Access Management Systems

Blockchain-based identity and access management systems can be leveraged to strengthen IoT security. Such systems have already been used to securely store information about goods' provenance, identity, credentials, and digital rights. As long as the original information entered is accurate, blockchain's immutability can be achieved.[13] 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 handled relatively easily for most IoT devices. For instance, a private blockchain can be used to store cryptographic hashes of individual device firmware. Such a system creates a permanent record of device configuration and state. This record can be used to verify that a given device is genuine and that its software and settings have not been tampered with or breached. Only then is the device allowed to connect to other devices or services.

Returning to the Dyn example, IP spoofing attacks were launched for 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. Because it is not possible to alter approved blockchains, it is not possible for devices to connect to a network by disguising themselves by injecting fake signatures into the record.[14] The earlier example involving Filament's Taps illustrates this point.

Cloud vs. Blockchain Models

In the cloud model, IoT devices are identified, authenticated, and connected through cloud servers,

Table 1. How blockchain can address Internet of Things (IoT) challenges.

Challenge	Explanation	Potential blockchain solution
Costs and capacity constraints	It is a challenge to handle exponential growth in IoT devices: by 2020, a network capacity at least 1,000 times the level of 2016 will be needed.	No need for a centralized entity: devices can communicate securely, exchange value with each other, and execute actions automatically through smart contracts.
Deficient architecture	Each block of IoT architecture acts as a bottleneck or point of failure and disrupts the entire network; vulnerability to distributed denial-of-service attacks, hacking, data theft, and remote hijacking also exists.	Secure messaging between devices: the validity of a device's identity is verified, and transactions are signed and verified cryptographically to ensure that only a message's originator could have sent it.
Cloud server downtime and unavailability of services	Cloud servers are sometimes down due to cyberattacks, software bugs, power, cooling, or other problems.	No single point of failure: records are on many computers and devices that hold identical information.
Susceptibility to manipulation	Information is likely to be manipulated and put to inappropriate uses.	Decentralized access and immutability: malicious actions can be detected and prevented. Devices are interlocked: if one device's blockchain updates are breached, the system rejects it.

where processing and storage are often carried out. Even if devices are a few feet apart, connections between them go through the Internet.[15]

First, IoT networks that have high costs are a concern in the centralized cloud model. Gartner estimated that in 2016, 5.5 million new IoT devices were connected every day.[16] It is estimated that by 2020, a network capacity that is at least 1,000 times the level of 2016 will be needed.[17] The amount of communication that needs to be handled will increase costs exponentially.

Second, even if economic and manufacturing challenges are addressed, each block of the IoT architecture could act as a bottleneck or point of failure that can disrupt the entire network.[18] For instance, IoT devices are vulnerable to DDoS attacks, hacking, data theft, and remote hijacking. Criminals might also hack the system and misuse data. If an IoT device connected to a server is breached, everyone connected to the server could be affected.

Consider smart water meters and associated risks. Twenty percent of California's residents have smart water meters, which collect data and send alerts on water leakage and usage to consumers' phones. Likewise, the Washington Suburban Sanitary Commission (WSSC) in Washington, DC, is planning to integrate IoT into its system. Water-usage data can tell criminals when residents are not home. Perpetrators can then burglarize homes when their residents are away.[19]

Third, the centralized cloud model is susceptible to manipulation. Collecting real-time data does not ensure that the information is put to good and appropriate use. Consider the water supply system example just discussed. If state officials or water service companies believe that the evidence might result in high costs or lawsuits, they can censor, edit, or delete data and analysis. They can also manipulate findings. For instance, consider the water crisis in the city of Flint, Michigan, which began in 2014. Flint authorities insisted for months that city water was safe to drink.[19] Citing official documents and findings of researchers who conducted extensive tests, a CNN article asserted that Michigan officials might have altered sample data to lower the city's water lead level.[20] It was reported that the Michigan Department of Environmental Quality and the city of Flint discarded two of the collected samples. A researcher said that the discarded samples had high lead levels. Including them in the analysis would have increased the level above 15 parts per billion (PPB). According to the US Environmental Protection Agency, water supply companies are required to alert the public and take action if lead concentrations exceed the "action level" of 15 PPB in drinking water (bit.ly/1qKMLVE).

Blockchain can eliminate many of the drawbacks described in Table 1. In blockchain, message exchanges between devices can be treated in a similar way as financial transactions in a bitcoin network. To exchange messages, devices rely on smart contracts. Blockchain cryptographically signs

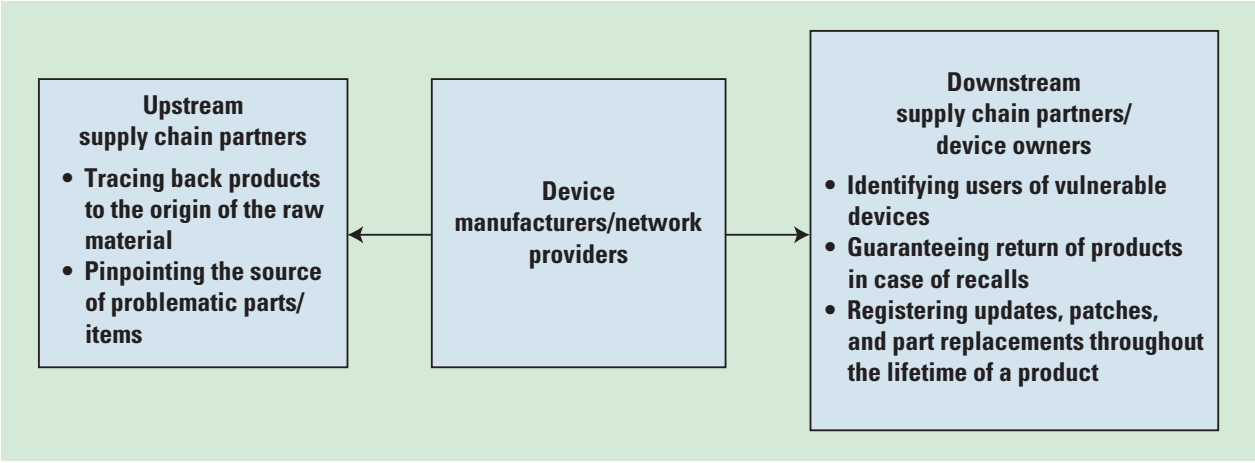

Figure 1. Blockchain's role in improving overall security in supply chain networks. With blockchain, it is possible to access immutable records for various aspects of transactions involving a product to understand key vulnerabilities in the upstream supply chain. This technology can also help strengthen downstream supply chain partners' and device owners' precautionary and defensive cybersecurity measures.

transactions and verifies those cryptographic signatures to ensure that only the message's originator could have sent it. This can eliminate the possibility of man-in-the-middle, replay, and other attacks.[6]

Blockchain's proponents have forcefully argued that this new technology can save us from "another Flint-like contamination crisis."[19] Projects such as the WSSC's integration of the IoT in supply systems can be upgraded with sensors such as near-infrared reflectance spectroscopy (NIRS) to include data on chemical levels. If such a system had been installed in Michigan, Flint's water service company could have found the lead contamination when it exceeded healthy levels. Blockchain can provide the "second layer of crisis prevention" in such cases.[20]

Ensuring Supply Chain Security

Blockchain can ensure supply chain security (see Figure 1). It also makes it possible to contain an IoT security breach in a targeted way after discovery of the breach. Blockchain can facilitate handling and dealing with crisis situations such as product recalls due to security vulnerabilities. Blockchain's public availability means that it is possible to trace back every product to the origin of the raw materials, and transactions can be linked to identify users of vulnerable IoT devices.

IoT-linked security crises, such as the cyberattacks on Dyn, could have been handled better if the supply chains had adopted blockchain. For instance, China-based Hangzhou Xiongmai Technologies, which makes Internet-connected cameras and accessories, recalled its products in the US that were vulnerable to the Mirai malware. However, it is difficult to determine the devices' owners. Blockchain is suitable for complex workflows. It can be used to register time, location, price, parties involved, and other relevant information when an item changes ownership. The technology can also track raw materials as they move through the supply chain, are transformed into circuit boards and electronic components, are integrated into products, and are sold to customers. Blockchain can also be used to register updates, patches, and part replacements applied to any product or device throughout its lifetime. It is easier to track progress in addressing vulnerabilities and send warnings and notifications to owners.[8]

Based on the evolving mechanisms and forces described here, a promising future seems likely for the use of blockchain in addressing IoT security. For instance, some of the key security challenges associated with the cloud can be addressed by using the decentralized, autonomous, and trusted capabilities of blockchain. Blockchain's decentralized and consensus-driven structures are likely to provide more secure approaches as the network size increases exponentially.

Blockchain enables the verification of the attributes it carries. Blockchain-based transactions are easily auditable. Due primarily to this and other features, blockchain

can play a key role in tracking the sources of insecurity in supply chains as well as in handling and dealing with crisis situations such as product recalls that occur after safety and security vulnerabilities are found. And as mentioned, blockchain-based identity and access management systems can address key IoT security challenges such as those associated with IP spoofing.

Acknowledgments

I thank Jeff Voas for numerous edits and suggestions on previous versions of this article. Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

References

1. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, May 2016, pp. 2292–2303.
2. *Blockchain in Banking: A Measured Approach*, Cognizant Reports, 2016.
3. "3rd Cyberattack 'Has Been Resolved' After Hours of Major Outages: Company," NBC New York, 21 Oct. 2016; bit.ly/2eYZO46.
4. N. Perlroth, "Hackers Used New Weapons to Disrupt Major Websites Across US," *New York Times*, 21 Oct. 2016; nyti.ms/2eqxHtG.
5. E. Blumenthal and E. Weise, "Hacked Home Devices Caused Massive Internet Outage," *USA Today*, 21 Oct. 2016; usat.ly/2eB5RZA.
6. J. Coward, "Meet the Visionary Who Brought Blockchain to the Industrial IoT," *IOT World News*, 14 Dec. 2016; bit.ly/2s8la1w.
7. A. Kaul, "IBM Watson IoT and Its Integration with Blockchain," Tractica, 1 Aug. 2016; bit.ly/2rsOp2M.
8. B. Dickson, "Blockchain Could Help Fix IoT Security after DDoS Attack," *VentureBeat*, 29 Oct. 2016; bit.ly/2dXNaNO.
9. B. Dickson, "How Blockchain Can Change the Future of IoT," *VentureBeat*, 20 Nov. 2016; bit.ly/2qXZWXw.
10. S. Pajot-Phipps, "Energizing the Blockchain—A Canadian Perspective," *Bitcoin Magazine*, 26 Jan. 2017; bit.ly/2r7IIEc.
11. J. Brown, "Companies Forge Cooperative to Explore Blockchain-Based IoT Security," *CioDive*, 30 Jan. 2017; bit.ly/2quIMfv.
12. E. Young, "Tech Giants and Blockchain Startups Unite to Make IoT Apps More Secure," *The Cointelegraph*, 30 Jan. 2017; bit.ly/2kNtm7w.
13. C. Catallini, "How Blockchain Applications Will Move Beyond Finance," *Harvard Business Rev.*, 2 Mar. 2017; bit.ly/2m2ZIZQ.
14. S. Kumar, "Not Just for Cryptocash: How Blockchain Tech Could Help Secure IoT," IoT Agenda, 13 Feb. 2017; bit.ly/2m8H9Gr.
15. A. Banafa, "IoT and Blockchain Convergence: Benefits and Challenges," *IEEE Internet of Things* newsletter, Jan. 2017; bit.ly/2n1y8jq.
16. R. Van der Meulen, "Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015," Gartner press release, 10 Nov. 2015; www.gartner.com/newsroom/id/3165317.
17. S. Waterman, "Industry to Government: Hands Off IoT Security," Fedscoop, 17 Nov. 2016; bit.ly/2g4oXYX.
18. A. Banafa, "A Secure Model of IoT with Blockchain," OpenMind, 21 Dec. 2016; bit.ly/2j2QUkH.
19. R. Hackett, "How Blockchains Could Save Us from Another Flint-Like Contamination Crisis," Venturebeat, 25 Feb. 2017; bit.ly/2mx11zp.
20. D. Debucquoy-Dodley, "Did Michigan Officials Hide the Truth about Lead in Flint?" CNN, 14 Jan. 2016; cnn.it/2r0aiF9.

Nir Kshetri *is a professor of management in the Bryan School of Business and Economics at the University of North Carolina at Greensboro. Contact him at nbkshetr@uncg.edu.*

IT Professional (ISSN 1520-9202) is published bimonthly by the IEEE Computer Society. IEEE Headquarters, Three Park Avenue, 17th Floor, New York, NY 10016-5997; IEEE Computer Society Publications Office, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; voice +714 821 8380; fax +714 821 4010; IEEE Computer Society Headquarters, 1828 L St. NW, Suite 1202, Washington, DC 20036. Visit www.computer.org/subscribe for subscription information.

Postmaster: Send undelivered copies and address changes to *IT Professional*, Membership Processing Dept., IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854-4141. Periodicals Postage Paid at New York, NY, and at additional mailing offices. Canadian GST #125634188. Canada Post Publications Mail Agreement Number 40013885. Return undeliverable Canadian addresses to PO Box 122, Niagara Falls, ON L2E 6S8, Canada. Printed in the USA.

Editorial: Unless otherwise stated, bylined articles, as well as product and service descriptions, reflect the author's or firm's opinion. Inclusion in *IT Professional* does not necessarily constitute endorsement by the IEEE or the Computer Society. All submissions are subject to editing for style, clarity, and space.