Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How Blockchain Can Help Secure Connected Devices

By **Elisabeth Arko**
(January 28, 2019, 3:10 PM EST)


Elisabeth Arko

In 2017, there were 8.4 billion "internet of things" devices in use, and this number is expected to explode to 75 billion by 2025.[1] Given this exponential growth, industries, governments and regulators have started taking steps to implement laws, practices, technologies and regulations to address and identify potential cybersecurity and safety hazards facing internet of things consumers.

As a result, companies are beginning to explore whether blockchain, a technology that uses a decentralized distributed ledger to record transactions, is a solution to make these products safer, more efficient and more secure. This article explores why blockchain is a potential solution to the obstacles facing internet of things devices. In addition, it looks at where the liability could fall if the product malfunctions.

Internet of Things

The internet of things refers to a network of connected devices that are capable of collecting and exchanging data. These networked devices transfer their data to a central location using a common language that allows them to communicate with each other.[2]

Broadly speaking, internet of things consumer products require an entire internet of things system to operate properly. This includes hardware (i.e., physical sensors within the product, such as a heart rate monitor in a wearable tracker), connectivity (i.e. a mechanism to transmit the data, such as a router), software (i.e., programs responsible for analyzing the data from the devices, which may be cloud-based) and an interface (i.e., a way for customers to interact with the device and give it commands, such as a mobile app).

These components are connected using platforms. Once implemented, these platforms analyze the data to extract valuable information and share it with other devices to initiate specific commands or actions.[3] The results include a better user experience, greater automation and improved efficiencies.

Despite this potential, internet of things consumer products are not perfect. These devices continuously share critical information back and forth over the internet, making the devices a prime target for hackers. While connected devices make our lives easier, and often more efficient, they are also engaged

in constant and pervasive collection, processing and dissemination of data, including our private information.

This gives rise to serious security and privacy concerns. In fact, several intrinsic features of the internet of things amplify its security and privacy challenges, including centralization, heterogeneity in device resources, multiple attack surfaces and scale.

First, internet of things systems are centralized in that they depend on a client/server communication as well as centralized trust brokers to identify nodes and control communications. As these networks begin to grow and interconnectivity begins to increase, these centralized networks could soon become overwhelmed, leading to lags or potential failures of critical commands. Manufacturers face increasing costs and expenses to meet the rising infrastructure demands and ensure these devices satisfy consumer needs and expectations.

Second, one of the great innovations surrounding the internet of things is its ability to seamlessly connect a wide range of devices to improve our everyday life. The problem, however, is that each of these devices run its own operating system and applications. As a result, connected devices are often not equipped with sufficient resources to implement complex security protocols that would protect against cyberattacks.[4] This is exacerbated by the fact that oftentimes the security systems that are in place are not properly monitored or updated.

Third, it is axiomatic that as the number of internet of things devices increases, so do the vulnerabilities of the systems. Each and every connected device represents a new potential access point to the network, and thereby creates additional vulnerabilities.

Finally, the internet of things faces significant scalability obstacles. Scalability refers to “the capability of a system, network or process to handle a growing amount of work, or its potential to be enlarged in order to accommodate that growth.”[5] As the number of connected devices is expected to grow, internet of things networks will have to change and adapt, as currently the infrastructure has limited scalability.

In sum, with billions of devices set to join internet of things networks in the coming years, centralized systems have limited scalability and interoperability. In addition, these networks expose millions of weak points that compromise network security. As a result, manufacturers are required to check and monitor each transaction on an internet of things network. This will lead to an increase in cost and a decrease in speed and efficiency.

Many leaders in the internet of things field see blockchain as a powerful way to address these intrinsic weaknesses in the internet of things, and bring scalable, decentralized security and trust to networked devices. But what exactly is blockchain technology, and why is it uniquely positioned to address some of these concerns?

What Is Blockchain?

Blockchain is the technology underlying cryptocurrencies like bitcoin. The technology, however, has applications that far exceed cryptocurrencies. This is because blockchain is an incorruptible digital ledger that can be programmed to record not just financial transactions, but virtually anything of value. As such, it features three principal technologies that in and of themselves are not new, but when put together form a revolutionary technology that has the potential to disrupt a variety of sectors, including

the internet of things.

Decentralization

Decentralization means that a network operates on a user-to-user (or peer-to-peer) basis. Unlike traditional ledgers, a blockchain database is decentralized and has no “master.” The result of decentralization is distribution. The blockchain allows digital information to be distributed, but not copied. This means that each entry on the ledger has only one owner.

Consensus

For the blockchain to make decisions, or for a block to be added to the chain, the nodes need to come to a consensus using “consensus mechanisms.” On the blockchain, this involves someone proposing a transaction to the block. Then all of the computers or “nodes” on the blockchain attempt to solve a cryptographic puzzle.

This takes an immense amount of computing power. The computer that solves the puzzle then shares that solution with the computers on the network. The network then verifies the work; if it is correct, the block is added to the chain. Any transaction must be verified by 51 percent of the network.

Immutability

Once a block is added to a blockchain, it becomes “immutable”; that is, it theoretically cannot change. Compare this to an Excel spreadsheet, where you are able to add, edit or delete columns or rows with relative ease. With the blockchain, this is not possible. Rather, changes to the information on the blockchain must be entered into a new block.

These principal technologies, together, are what makes blockchain technology so revolutionary. It replaces the need for third-party intermediaries, by allowing direct peer-to-peer transactions. As such, blockchain allows users to trust and interact directly with data in ways never possible before.

Blockchain’s Unique Position

The decentralized, autonomous and trustless capabilities of the blockchain make it a prime candidate to become a foundational element of the internet of things. Specifically, blockchain has the potential to improve internet of things networks through "trustlessness," oversight and increased security.

Trustless Peer-to-Peer Communication

Blockchain has the potential to remove the intermediary from the equation and allow devices to communicate directly with one another, resulting in a “trustless” interaction between the devices. This is done by treating each message between devices as a “transaction” on the blockchain, which means that there is validation and consensus before permitting the message to go through.

Oversight

Given that blockchain creates an immutable record of all transactions, it has the ability to track the entire history of a connected device. In the internet of things, blockchain treats messages between smart devices as “economic transactions.”

This allows for an easy audit and a central custodian of all of the messages, or transactions, that occur on the blockchain. As such, it is easy and efficient to discern where something went wrong by simply reviewing the ledger.

Increased Security

Blockchain's decentralized form eliminates the single points of failure, thereby creating a much more resilient ecosystem within which internet of things devices can operate. Blockchain's consensus requirements also bolster its cybersecurity potential.

No longer would an individual be able to "hack" into one device and access multiple other devices. Instead, the hacker would have to overtake 51 percent of the network in order to have control. This takes an immense amount of computing power, and is nearly impossible to accomplish.

Legal Issues Facing the Internet of Things and Blockchain

Despite its potential, blockchain sets forth a number of obstacles of its own before it reaches maturity in the internet of things space. For purposes of this article, we focus on the potential legal hurdles for the implementation of blockchain technology in internet of things networks.

Jurisdiction and Choice of Law

Unlike traditional ledgers and databases, blockchain networks can go beyond the boundaries set by legal jurisdictions, because servers for digital ledgers can be based anywhere.

In case of a fraudulent or erroneous communication between devices, identifying its origin within the blockchain could be a challenge. Therefore, courts, and lawyers, will face hurdles when trying to discern what court has jurisdiction and what laws apply.

Liability

With the number of different components involved in internet of things networks, the question of who bears liability for a consumer product will be at the forefront of this discussion. For example, who has to take responsibility if a device takes action based on a rule that has been automatically executed by a blockchain-based program triggered by another blockchain-based program, but that action turns out to cause damage or malfunction in an internet of things device?

There is no clear answer to this question, but current legal landscapes could offer some guidance related to manufacturer liability. For example, a manufacturer that fails to take precautions when designing a connected device with software that is equipped with inadequate security measures could be deemed liable for selling a product with a "defective design." This is actionable in many jurisdictions.

Moreover, in some jurisdictions, manufacturers have a post-sale duty to warn. Under this theory, a manufacturer has a duty to warn consumers of dangers that become, or should have become, known to it. This traditional theory of liability could even be expanded to include a duty of a manufacturer to ensure that its connected devices are continuously updated with the most current software and security practices associated with such devices.

Of course, manufacturers, and even software developers, can also be held liable under a theory of negligence. Under this theory, a manufacturer has a duty to prevent reasonably foreseeable risks. Recently, the Federal Trade Commission's Bureau of Consumer Protection put out a report on internet of things devices indicating that events such as hackers compromising credentials are a reasonably foreseeable risk.

The report also indicates that companies should exercise "due diligence" when selecting service providers and incorporating security standards. Although not binding, this document provides insight as to what regulatory agencies consider "reasonable" and "foreseeable," which could have an impact on internet of things product liability cases as they begin to move through the courts.

Conclusion

Blockchain technology is positioned to be a unique solution to some of the inherent weaknesses and challenges facing internet of things devices. These include fostering an ecosystem where devices are able to communicate directly with one another securely, which in turn increases consumer confidence in, and speed and efficiency of, connected products.

Nevertheless, manufacturers and software engineers should be aware of the legal complexities and potential liabilities they could be facing as this technology continues to grow and expand.

Elisabeth C. Arko is an associate at Tucker Ellis LLP.

[1] See Alex Rolfe, Base of IoT devices to hit 75 billion — TEE spec adoption to reach 10 billion, Payments Cards & Mobile (Nov. 21, 2018), https://www.paymentscardsandmobile.com/base-of-iot-devices-to-hit-75-billion/.

[2] See Steven Ranger, What is the IoT? Everything you need to know about the Internet of Things right now, ZD Net (Aug. 21, 2018), https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/.

[3] See Michael Porter & James Heppelmann, How Smart, Connected Products Are Transforming Competition, Harv. Bus. Rev. (Nov. 2014), https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition.

[4] See Alan Grau, What is Really Needed to Secure the Internet of Things?, Icon Labs, Device Security for Internet of Things (last visited Dec. 31, 2018), https://www.iconlabs.com/prod/internet-secure-things-%E2%80%93-what-really-needed-secure-internet-things.

[5] Ryan Lester, Scalability — What it means and why it's so critical in the IoT, ITProPortal (Jan. 5, 2017), https://www.itproportal.com/features/scalability-what-it-means-and-why-its-so-critical-in-the-iot/.