# ORF 597A Final Report:
# Survey of Blockchain in IoT Applications

Oleg Golev, Rishi Mago, Frederick Qiu

June 6, 2023

## 1 Introduction

### 1.1 What is IoT?

Everything from the simplest RFID tags to smart thermostats belong to the category of the Internet of Things (IoT). These devices are low-powered, often smart sensors or chips that add intelligence to common-place objects and have the capacity to be connected to the worldwide web. The spread of IoT devices became pervasive as (1) small low-power wireless programmable chips could now be manufactured at scale with very small per-unit cost, (2) the widespread broadband Internet access and the adoption of IPv6 allowed each device to be uniquely recognizable, and (3) data became more valuable [20]. The turning of fridges, cameras, light bulbs, speakers, sensors, and even ID cards into small IoT devices is not only motivated by the added convenience of wireless control via our phones and computers, but also by the possible optimizations, processing, and automation that can be performed based on the data that IoT devices collect. Most notably, IoT devices' capability for (often real-time) data collection can enable:

- Better business decisions and customer satisfaction based on the analysis of this data
- Product and process optimization and automation based on data patterns
- Interconnectivity and interoperability with other smart devices or larger electronics.

These devices can be connected by Wi-Fi, Zigbee, Bluetooth, LTE, satellite, or most recently 5G, to both each other and other devices, allowing many avenues to integrate them into different environments. The talks of smart houses and even smart cities all stem from everything "turning IoT," with IDC predicting a total of 41.6 billion IoT devices collecting and sharing ~79 zettabytes of data via air by 2025 [17].

## 1.2 IoT Security Issues

Like any device connected to the Internet and collecting data, IoT devices are susceptible to hacking and data theft. Their sheer surface area and massive amounts of data acquisition make them prime targets for attacks, and their focus on conserving power and minimalist function often comes at the cost of their security:

- Lack of encryption is common to remove overhead, causing collected data and even account information to be fully exposed in-transit and in-storage to anyone curious enough. Since data collected from IoT devices can range from video files from surveillance cameras to audio recordings from PC microphones to activity-tracking information from motion sensors and $CO_2$ detectors, IoT devices can carry but often do not encrypt highly confidential and privacy-violating media.
- Most IoT devices lack the ability to update their firmware in response to discovered vulnerabilities. This means that once a vulnerability is found in a product, all IoT devices of that product line remain at risk and can be compromised at any point in their lifetime, requiring their complete replacement if security is important to the users.
- Most manufacturers do not clearly define whether and for how long their production IoT devices will continue being supported. Thus most of the time, IoT devices could be discontinued and abandoned at any point. This leaves users on their own in case vulnerabilities get discovered with an IoT product after its discontinuation.
- IoT devices often use easy-to-guess or easy-to-find default passwords for entire product lines, allowing any attacker to walk to a victim's device and tap into them unrestricted.
- Multiple models of the same IoT product or similar products rarely go through iterative security testing and can have similar vulnerabilities. Therefore, a vulnerability found on one model is likely to exist on related models or the entire line of that product [19].

The IoT devices' minimal or nonexistent security features place them at the hackers' doorstep. Recall that these devices may communicate compromising information over air or through a connected device (e.g. a web camera connected to a PC), and they have a unique IPv6 address to do so. Hence, compromised IoT devices are often used to create botnets for DDoS'ing targets. In 2016, the Dyn attacks took down a large portion of the Internet in Europe and North America [26]. Likewise in 2016, Botnet 14 took down Liberia's main ISP, cutting the entire country off from the Internet. The same attacker took down a million users connected to Deutsche Telecom in Germany less than a year later [14]. All attacks were facilitated by large networks of compromised IoT devices.

IoT device vulnerabilities and hacks are so commonplace that there are numerous underground marketplaces that sell access to devices like compromised routers, gas meters, electrical meters, VPN exit nodes, etc [11].

The ubiquity of IoT devices and their many security issues even caused some politicians to step up and propose requirements that IoT devices must meet in order to be sold in that country. For instance, the

United Kingdom recently introduced a new law which requires any commercial IoT device to have (1) a unique password that is non-resettable to factory settings, (2) a clear length of support guaranteed by the manufacturer, and (3) an easy way to report bugs [6].

While laws like this definitely address some security concerns with IoT devices and prompt manufacturers to be more careful with how they design the firmware for their IoT products, the question remains as to how the manufacturers should actually implement their IoT firmware securely.

### 1.3 IoT Trust Issues

IoT devices likewise suffer from other issues related to trust:

- IoT devices often communicate with one another over a private or public shared network with a single master node or centralized server, which assumes a single point of failure
- IoT devices connected to the Cloud often assume a centralized cloud-based server-client paradigm
- Closed-source manufacturing and programming of IoT device chips means that the extent of the manufacturer's data collection and use is not known. The users must trust that the manufacturer does due diligence with the gigantic volumes of data collected by the IoT devices.

In order for users to trust their IoT devices, users must therefore make the unreasonable assumption that the manufacturer's or central authority's implementation of device functionality is non-malicious and non-exploitable. However, the world has seen too many brands, even well-respected ones, suffer from countless hacks, and users have had their collected data misused, exploited, and often monetized. The general lack of security on IoT devices already exacerbates the problem with external data breaches and data theft, yet IoT data is often exploited even from the side of the manufacturer.

## 2 The Unclear Promises of Blockchain

Blockchain, at its core, is a consensus algorithm that builds a decentralized ledger in a peer-to-peer network. Blockchain does not rely on a centralized authority to work, assumes no trust between peers, and provides some protections, including transparency and asymmetric cryptography to confirm user identity and validity of transaction information. Looking at the security risks of IoT, many researchers and engineers turned to blockchain as a potential solution to all of the aforementioned problems. The "hype" of blockchain promised to fix everything bad about IoT, yet it is unclear how blockchain is actually the best solution.

**First**, the cryptography of blockchain would protect credentials and collected data. However, encryption is not unique to blockchain. There are already IoT devices that encrypt their data to ensure security in-transit and in-storage without the use of higher level exotic algorithms.

**Second**, some people assert that the trustless nature of the blockchain algorithm would ensure that only non-compromised data is agreed upon by the network. The original Bitcoin algorithm punished miners for submitting invalid data via the wasted computational cost involved in proof-of-work. However, many IoT devices (e.g. cameras) generate large amounts of data, and this data must be delivered quickly either to the Cloud or peers. Given that IoT peer networks can number in dozens, hundreds, or even thousands of nodes, the cost of using proof-of-work in IoT consensus is impractical. Real-time monitoring will be near impossible given the added latency, and the power requirements of proof-of-work go directly against many of the IoT devices' promise and contingency on low power operation. When looking at the proof-of-stake concept, it is hard to distinguish how it is different from running some other distributed consensus algorithm or simply running data validity checks. In some cases, it may even be bad to invalidate suspicious data. For instance, suppose there are ten smart temperature sensors communicating with each other over 5G in a completely decentralized way (no Cloud), and each sensor maintains some log of snapshots where each snapshot is a map of each sensor's temperature recording at a certain time. Suppose the sensors use some blockchain algorithm to reach consensus on the log (each snapshot is a block, and a temperature recording of each sensor is a transaction in a block). Now suppose an attacker takes over one of the sensors:

- There is actually nothing in the blockchain algorithm that somehow invalidates the hacker's control of the sensor's functionality. That is, given a vulnerability in the sensor's firmware, the attacker may inject code that does nothing but upload the temperature data to the attacker's server with no repercussions.
- The attacker may inject bogus temperature readings into the snapshots. Let's say the attacker injects a reading that indicates that a room is at 96 degrees Celsius. However, what if the house was actually on fire? A temperature-sensing system may want to treat such recordings as valid to notify the user of a real potential danger or a malfunctioning sensor.

This anecdotal example serves two purposes: it explains that a blockchain doesn't actually offer the "hype" security promise but rather offers a consensus algorithm which may as well be replaced by something like Raft (which is also faster), and it shows that data invalidation is trickier than just saying "this doesn't look right." Even assuming that an attacker has full control of an IoT device does not somehow change that device's identity, its ability to validate blocks or transactions, or otherwise tamper with the device's function in a way that would immediately make it recognizable as malicious.

**Third**, some people proposed that firmware updates and patches can be done via smart contracts, and that devices can be forced to update by peer IoT devices to ensure that no devices remain vulnerable. However, it is again unclear why IoT devices need a blockchain protocol to (1) update as soon as an update is available uplink, and (2) periodically verify current peer versions and stop communicating with those out of date. In any scenario, a firmware update must be provided by a centralized authority uplink, hence it is unclear why putting IoT systems like above on the blockchain solves any issues of trust either.

A lot of companies invested large sums of money into research on how to optimize between power consumption and security for its IoT devices. These IoT systems address all security concerns detailed above

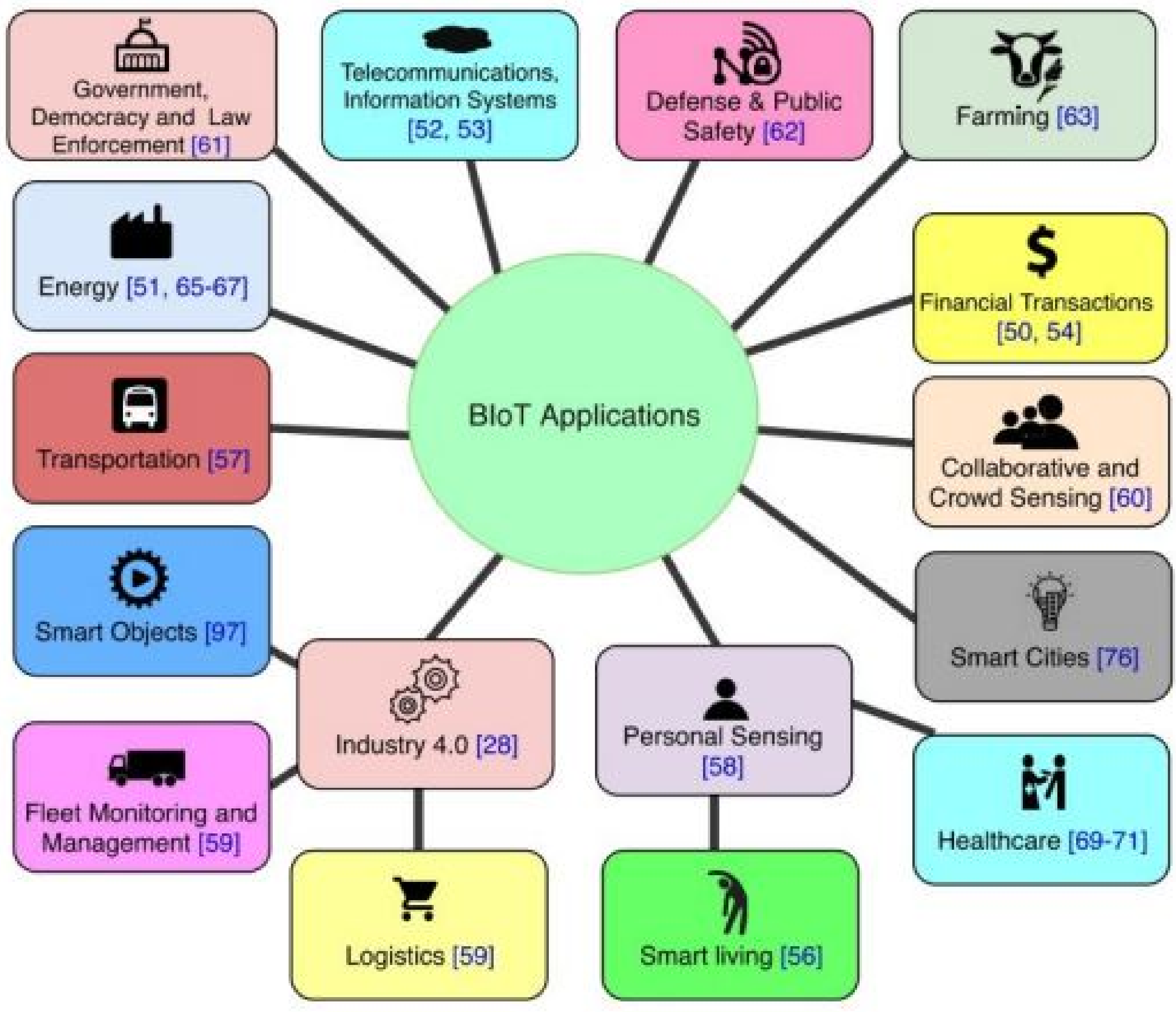
Government, Democracy and Law Enforcement [61]
Telecommunications, Information Systems [52, 53]
Defense & Public Safety [62]
Farming [63]
Energy [51, 65-67]
Financial Transactions [50, 54]
Transportation [57]
BIoT Applications
Collaborative and Crowd Sensing [60]
Smart Objects [97]
Smart Cities [76]
Industry 4.0 [28]
Personal Sensing [58]
Healthcare [69-71]
Fleet Monitoring and Management [59]
Logistics [59]
Smart living [56]

Figure 1: Applications of blockchain and IoT, according to [8].

but without the latency limitations of blockchain. Huawei in particular proposed a very comprehensive IoT security solution that goes above and beyond to ensure reliability, proper verification and encryption of data, and malicious vector detection of IoT systems [12].

## 3 The Applications of Blockchain

Aside from blockchain "fixing" IoT devices' security issues, many people put a lot of thought into where IoT and blockchain together may actually be useful in commercial applications. While survey papers such as [8, 15, 5] would seem to suggest blockchain and IoT have an extremely wide range of applications, many of the applications are dubious upon closer inspection.

For instance, [10] presents a blockchain-based smart lock which has almost no reliance on blockchain, except that intrusions will be recorded on a blockchain ledger (which will be of great value to the homeowner, assuredly). 3 of the 4 articles in [8] cited as applications of blockchain and IoT to the energy sector do not mention blockchain at all, and the fourth article just explores paying for electricity using cryptocurrency without explaining the need for an actual implementation of a blockchain algorithm in their IoT systems [28, 2, 13, 7]. Many others state the obvious (that bitcoin can be used to pay for services) or make vague claims about how blockchain is secure (has military grade encryption, requires compromising 51% of the network, etc.), painting a picture that the vast majority of the space is just "hype" rather than practical applications [1].

However, there are some seemingly valid applications of IoT and blockchain. In particular, blockchain and smart contracts, together with data collected by IoT, could be used by government to transparently enforce laws [27]. Clinical trials sometimes see data tampering by researchers trying to publish more appealing results or companies pushing their drugs onto the market, which could be made much harder by IoT devices automatically collecting data and storing it on a tamper-proof record created using blockchain [21]. Blockchain may also be used in quickly blacklisting devices. Some companies, notably T-Systems (part of Deutsche Telekom) use blockchain as a public ledger (1) to record and then recognize stolen phones to get them off networks quicker and (2) to have any communicating devices mark and be aware which phones are stolen [22]. One of the most promising applications, however, might be found in the supply chain.

### Relevant Application: Supply Chain

In supply chain applications, there are a few key differences from the more common blockchain settings. First, the blockchains are generally private, meaning only authorized users are allowed to join, and permissioned, meaning only certain users are allowed to mine, which is completely different from the public, permissionless setting of Bitcoin. In existing blockchain and supply chain applications, the full nodes are run by a single provider [3] but could theoretically be run by the different parties involved in the supply chain (suppliers, retailers, carriers, etc.) for greater decentralization. The regular users are the IoT devices and people broadcasting “transactions” to be recorded on the blockchain.

In this scenario, the low computational power of IoT devices is not an issue because they are only required to broadcast data instead of run a computationally expensive blockchain protocol. Further, the throughput of a private blockchain can be much higher than that of a public blockchain, allowing for wider applications. This is because carefully restricting the set of miners completely prevents many attacks that foil simple consensus schemes. For example, a consensus scheme that chooses a uniformly random user to mine is impossible for a public blockchain where you can easily create multiple public keys, but is completely fine for a private blockchain where there are only a handful of nodes, each identifiable with a real-world entity.

One big problem in supply chain that blockchain and IoT can help resolve is in invoicing disputes. Since there are many disparate parties (suppliers, retailers, carriers, etc.) involved in the supply chain, it usually ends up that each maintains their own private records. This can cause serious problems when discrepancies arise and must be resolved. Prior to blockchain solutions, the most common way to do this was via a manual “match and compare” of records, which takes a significant amount of time and often just results in one side capitulating. It is estimated that over $140 billion USD is tied up in invoicing disputes, and that 20% of transportation costs are administrative [3]. Even as the size of data pools increases with the increased use of IoT devices, the data must still be manually compared in disputes and is not generally useful.

In a similar vein, traceability is another problem in supply chain. In 2018, there were 18 reported outbreaks of foodborne illness in the US [4]. It would be optimal in these scenarios to be able to quickly trace the source and cut off the problematic supply, but this often takes days or weeks because of the large number of self-interested parties involved in the supply chain (nobody wants to have responsibility put on them for a problem). Aside from immediate health concerns, this has larger economic effects due to people avoiding large categories of products (e.g. when people were advised to stop consuming romaine lettuce for a few weeks during the E-coli outbreak) when the exact source of the problem is unknown.

In both of these cases, the main issue is the lack of trust between parties. Broadly, blockchain would solve the trust problem by creating a shared, immutable record, and IoT would provide the necessary tracking data. The flexibility of blockchain with smart contracts would allow complex transactions to take place automatically.

### Case Study: DLT Labs

Walmart is one of the largest suppliers in Canada, delivering a wide array of products to over a million customers every single day. Dealing with transportation companies, tracking over a hundred thousand unique products, and ensuring timely payments to carriers require bulletproof logistics. As in most supply chain operations, the intermediate carriers, suppliers, and retailers each keep their own private records of shipments, quantities and type of products, as well as their current location. For Walmart Canada, this process comes with overbearing administrative costs associated with settling invoice disputes. In the U.S. alone, "14 billion [dollars] a year is captive and allocated to disputes," which means there is a large sum of money that is being wasted due to logistical inefficiencies and lack of a verifiable and reliable log of transportation records [3].

While Walmart Canada and its carriers use IoT devices for tracking and record-keeping, there is lack of infrastructure that consolidates tracking information in one place and ensures that it is reliable for further reference. To resolve disputes faster by utilizing IoT technologies to its full potential, Walmart Canada hired DLT Labs who implemented DL Freight, a private distributed ledger system for carrier networks based on the Hyperledger Fabric blockchain framework (which provides immutability and transparency of ledger data) to be used by Walmart Canada’s 70 carriers.

DLC Labs hosted 600 virtual machine nodes geographically spread across the country to be accessed only by the 70 carriers (via OIDC authentication) when recording invoices and shipping information. As a result, "what was previously an overwhelming number of invoice disputes in the range of 70% has now been virtually eliminated to only small number of discrepancies of approximately 1.5%" and "the timeline to agree on and approve carrier invoices that formerly varied from 6-8 weeks, but often extended over many months, went to less than one week" [3]. Not only did DLT Labs's blockchain system speed up dispute resolution, it also saved everyone a ton of money and did so with a simpler "user" experience (participating companies didn't need to set up their own nodes).

This is a clear example of how a private distributed ledger system (as can be provided by blockchain) can be advantageous for supply chain applications, especially if that ledger is private. This case study however requires that Walmart Canada and its carriers trust in DLT Labs since they own and operate the 600 virtual nodes that run the blockchain algorithm. However, it is not hard to imagine each carrier hosting their own nodes, therefore achieving full decentralization and a completely trustless network. In turn, it is also not hard to imagine each carrier being required to put some money at stake for each shipping record, which is lost if the record is found to be invalid.

**Case Study: IBM**

Prior to Walmart's blockchain traceability solution, figuring out the source of a bag of mangoes required days of back and forth with various suppliers and distributors. When the E-coli outbreak in romaine lettuce occurred, Walmart pulled millions of heads of lettuce from their shelves because figuring out exactly which lettuce was bad would have taken too long. The problem with a shared standard database is that it requires a certain degree of trust between the different parties, which doesn't always exist. On the other hand, the transparency and immutability of a blockchain solution builds the needed trust in the system. This, along with a new labeling system enabled Walmart to reduce the time taken to track certain products from weeks down to seconds using IBM's (similar to BLT Labs') custom port of the Hyperledger Fabric blockchain framework. Today, 25 products across 5 different suppliers are tracked using blockchain technology [4].

## 4 Key Players and Their Incentives

When discussing the use of IoT devices, the key players involved are (1) the consumer using the device, (2) the manufacturer, and (3) the cloud provider, if any, handling the data for the device.

Consumers are often both uneducated about security and uncaring about its presence or lack thereof. Part of this issue is due to the fact that the harms of hacked IoT devices are often largely external—the highest profile breaches of IoT devices are typically to use them as parts of botnets, a large negative externality that consumers often simply don't care about. The result is that consumers often fail to take even simple security measures such as change the default username and password of a device. Their incentives are better aligned in cases where the IoT device has access to sensitive user information, e.g., a cloud-based security camera system. Lowering the energy required from consumers to make IoT devices secure and enabling security features by default may also help protect some consumers.

The manufacturers of IoT devices are incentivized to produce devices as quickly and cheaply as possible. Because the lifetime of many IoT devices is so short and consumers are both uneducated and uncaring about security, it is often in manufacturers' best interest to cut corners when it comes to security. However, increasing awareness and publicization of IoT security issues via high-profile articles written about major hacks have helped change consumers' views on the importance of security. Given the importance that manufacturers place on customer retention, the manufacturers are in turn incentivized to respond to increased consumer demand for security. Additionally, manufacturers may fear enforcement action from government entities in response to breaches that threaten the security or privacy of their customers, some of which may be firms or government entities.

Because just a few major cloud providers control the majority of the IoT market—Amazon Web Services leading with a 34% share followed by Microsoft Azure with 23% and Google Cloud with 20% [18]—these entities are extremely powerful, with their decisions and practices having immense ramifications for the security of many IoT devices. Because these providers are more broadly used than just serving the IoT market, their technology has often been developed to the higher security standards demanded by other enterprise users. However, since their consumers—the manufacturers of the IoT devices—don't have a high demand for security, they are still incentivized to cut corners or offer cheaper (and lower quality) solutions when possible.

With blockchain-based solutions, the players involved are typically the same. However, one theoretical benefit of blockchain is in decentralizing IoT infrastructure, potentially mitigating the impact of centralized entities such as manufacturers or cloud providers raising problems over misaligned incentives. Blockchain would help limit the ability of one key player with bad incentives to cause harm to the rest of the system. Nevertheless, when devices lack the resources to use cryptographic protocols or when manufacturers simply aren't incentivized to prioritize security, blockchain either can't or won't be used.

## 5 Questions from Lecture

### How much overhead (and of what kind) does encryption cause?

"Low-Energy Security: Limits and Opportunities in the Internet of Things" [23] illustrates some of the issues with implementing encryption and more advanced security features on IoT devices through a comparison between a Samsung Galaxy S5 smartphone and a miniature sensor tag intended to report information including presence, temperature, and humidity for years or even decades. The smartphone has "a 2.5-GHz quad core processor, 2 Gbytes of RAM (with up to 128 Gbytes of SD card), and a 30kJ battery that is typically recharged daily" while the tag merely has "a single 16-bit processor, often running at 6 to 12 MHz to save energy, with 512 bytes (not megabytes or gigabytes, but bytes!) of RAM and 16 Kbytes of flash for program storage".

We can see that the tag has a processor that's orders of magnitude worse, over 2000 times less RAM, and less than 1/15 the energy storage compared to the phone. While the phone has to last on the order of tens of hours and will likely be recharged daily, the tag has to last tens of thousands of hours with a minimum-size battery that will never be recharged. Because of these constraints, any resource that uses computational power must be used sparingly. While executing a few million instructions would be relatively quick and cheap on a phone, it is prohibitively expensive to do so on small IoT devices like the tag.

There is, however, work being done on lightweight cryptographic solutions for embedded devices that have limited computational and energy resources [16]. An emphasis is placed on speed of operations so that a device can return to an idle state with reduced power consumption as quickly as possible. One improvement for devices that need only one-way authentication is to use specialized ciphers and protocols that don't involve decryption. Other improvements include keys hardwired onto devices in order to eliminate the need for key generation operations. Trading off security for performance by reducing key and block sizes is another approach that can allow some security without compromising the utility of the IoT device by using up too many of its resources.

### Are central authorities involved with IoT devices actually in a position of power? Were there any serious incidents where this was a problem?

In early 2021, Verkada, a startup providing cloud-based security camera solutions was hacked. The company was relatively well trusted until that point, being backed by Sequoia Capital, valued at $1.6 billion, and having a wide range of customers including hospitals, schools, jails, and many businesses and offices including higher-profile customers like Tesla and Cloudfare. While many attacks gain access to IoT devices by targeting individual vulnerable devices, this attack was distinctive in that the attackers were able to gain access to an internal account at Verkada itself with administrator privileges and used these privileges to compromise 150,000 surveillance cameras at once. Here, Verkada acted as a single point of failure through which all IoT devices sending data to it were compromised. Attackers were able to access live feeds from the compromised cameras and also, through root access on the cameras, remotely execute code on them, potentially gaining access to the broader corporate networks many of the cameras were on [24].

### What was the change in the business logic in the DLT Labs case study, and what was the source of the speedup from 6-8 weeks to 1 week?

The main change in business logic is the book-keeping. Without a shared, trusted record, each individual party in the supply chain maintains their own records, which often have discrepancies, leading to disputes, sometimes "in the range of 70% or more over every load a carrier delivers" [3]. Invoice reconciliation at this point devolves into a manual "match and compare," which is a large time sink and often just results in one side capitulating.

With a shared record in the form of the blockchain ledger, the exact terms can be agreed upon at the time of invoice creation, and so long as everyone trusts the shared record, there is no possibility of dispute based on discrepancies between private records.

As a side note, it seems that the DLT Labs case study focuses entirely on the blockchain side of things (which makes some sense, since the blockchain is the service they were providing). It is possible that IoT only comes into play in further automating the supply chain, or that IoT just seemed vaguely relevant and some paper wrote down that IoT had applications to supply chain. Either way, there seems to be a real use case for blockchain in supply chain.

### What exactly is DLT Labs being trusted to do?

DLT Labs "runs the platform on more than 600 virtual machines (VMs) to securely store and manage data points from thousands of transactions per day" [3]. In other words, it seems that DLT Labs itself is trusted by all entities, and the blockchain is more of a distributed fault tolerance mechanism, especially considering malicious actors taking control of some (but not a majority) of the network. Individual actors could broadly verify that their transactions are being recorded, but subtle manipulations could fly under the radar.

### What is the point of using blockchain in supply chain applications instead of a collection of signed statements? The complexity introduced by a ledger is generally intended for applications where order matters (e.g., financial transactions).

Actually, supply chain applications do make financial transactions ("at the end of the process is payment authorization, entirely through the solution, and Walmart relies on that authorization for payment with no further checks or balances" [3]). The use of factoring (getting liquidity in a more timely manner by "selling an invoice" to a bank, which pays you immediately and can wait for the other party to pay it) also indicates that timely payment is important ("the only thing parties can agree on is that there are delayed payments, which in turn drives up working capital costs because of the need to borrow, often through accounts receivable financing, or 'factoring"' [3]). That is, even if double spends aren't true double spends (e.g., Alice double spends $5 on Bob, with the intent of paying him the other $5 after she receives a payment tomorrow), they are still undesirable to have, which means a ledger makes sense to some extent.

The flip side is that most likely, transactions in supply chain applications are made in some physical currency anyways, so having no double spends in the ledger is less important because tools like factoring can again mitigate these issues (albeit at the cost of transaction fees). However, the potential need for a ledger in future applications is still there.

Another benefit of using blockchain is that it makes it much more tamper-resistant. If bad transactions are made and are then dispute a week later, they will be cemented under a week's worth of transactions and it would be computationally intractable for the offending party to then retroactively alter the records in their favor, as opposed to a collection of signed statements, where it may be feasible to alter a single record.

### How is blockchain being applied to clinical trials, or how could it be applied?

The primary concern with clinical trials that blockchain could help with is data integrity, as self-interested parties (e.g., a company trying to push a drug to production) may have incentives to tamper with data. A blockchain maintained by multiple parties would increase increase the trust in collected data and make integrity breaches and other problems easily traceable. A secondary benefit is that the flexibility of smart contracts means certain guidelines can be enforced more strictly, e.g., the ethical standard that patient consent forms must be obtained prior to randomization [25]. It is also proposed that blockchain helps with privacy through data encryption, but this is not a blockchain specific benefit.

In terms of practical implementation, the Mayo Clinic announced in September that they would be conducting a clinical trial using blockchain technology, but we were not able to find details on what role blockchain will play in the clinical trial [9].

## 6 Conclusion

In our research, we found that, while there are some valid uses for blockchain in Internet of Things devices, much of the hype around the technology is overblown speculation and misunderstandings about how cryptography and blockchains work. One of the strongest reasons to use a blockchain is a lack of mutual trust amongst players in an ecosystem. Here, blockchain can provide value by shifting from a centralized infrastructure to a decentralized one, ensuring that parties involved don't need to rely on some single trusted entity that may not exist, e.g., the supply chain case study. Since private blockchains can function just like a distributed database, blockchains can also be used if the chain structure makes sense for data being stored, e.g., audit log in supply chain. Nevertheless, blockchain is nowhere near as widely applicable as many sources in the literature claim. In particular, blockchain is not the miracle or even best solution to IoT devices' security issues, especially given the manufacturers' and customers' incentives. While blockchain does help via its use of asymmetric cryptography, the rest of the blockchain algorithm is expensive—computationally, energy-wise, and monetarily. Overall, we found that using blockchain protocols for distributed ledgers in IoT devices has several real-world applications and can be a powerful paradigm but is not a universal solution to all of IoT's problems.

# References

[1] Kamanashis Biswas and Vallipuram Muthukkumarasamy. "Securing Smart Cities Using Blockchain Technology". In: *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. 2016, pp. 1392–1393. doi: 10.1109/HPCC-SmartCity-DSS.2016.0198.

[2] Óscar Blanco-Novoa et al. "An electricity price-aware open-source smart socket for the internet of energy". In: *Sensors* 17.3 (2017), p. 643.

[3] *Case Study: DLT Labs™ & Walmart Canada Transform Freight Invoice Management with Hyperledger Fabric*. url: https://www.hyperledger.org/learn/publications/dltlabs-case-study.

[4] *Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric*. url: https://www.hyperledger.org/learn/publications/walmart-case-study.

[5] Hong-Ning Dai, Zibin Zheng, and Yan Zhang. "Blockchain for Internet of Things: A Survey". In: *IEEE Internet of Things Journal* 6.5 (2019), pp. 8076–8094. doi: 10.1109/JIOT.2019.2920987.

[6] Media; Sport Department for Digital Culture and The Rt Hon Nadine Dorries MP. *New Smart Devices Cyber Security Laws One Step Closer*. Jan. 2022. url: https://www.gov.uk/government/news/new-smart-devices-cyber-security-laws-one-step-closer.

[7] Tiago M Fernández-Caramés. "An intelligent power outlet system for the smart home of the Internet of Things". In: *International Journal of Distributed Sensor Networks* 11.11 (2015), p. 214805.

[8] Tiago M. Fernández-Caramés and Paula Fraga-Lamas. "A Review on the Use of Blockchain for the Internet of Things". In: *IEEE Access* 6 (2018), pp. 32979–33001. doi: 10.1109/ACCESS.2018.2842685.

[9] Andrea Fox. "Mayo Clinic to use blockchain for hypertension clinical trial". In: *Healthcare IT News* (Mar. 12, 2017). url: https://www.healthcareitnews.com/news/mayo-clinic-use-blockchain-hypertension-clinical-trial.

[10] Donhee Han, Hongjin Kim, and Juwook Jang. "Blockchain based smart door lock system". In: *2017 International conference on information and communication technology convergence (ICTC)*. IEEE. 2017, pp. 1165–1167.

[11] Stephen Hilt et al. *Trend Micro: The internet of things in the Cybercrime Underground*. Sept. 2019. url: https://www.iotbusinessnews.com/download/white-papers/TREND-MICRO-the-internet-of-things-in-the-cybercrime-underground.pdf.

[12] Huawei. *2018 IOT security white paper*. Oct. 2018. url: https://e.huawei.com/en/news/global/2018/201810191720.

[13] Y. R. Kafle et al. “Towards an internet of energy”. In: *2016 IEEE International Conference on Power System Technology (POWERCON)*. 2016, pp. 1–6. DOI: 10.1109/POWERCON.2016.7754036.

[14] Michael Kan. *2 years for hacker who crippled Liberia’s internet with Mirai botnet*. Jan. 2019. URL: https://www.pcmag.com/news/2-years-for-hacker-who-crippled-liberias-internet-with-mirai-botnet.

[15] Nir Kshetri. “Can Blockchain Strengthen the Internet of Things?” In: *IT Professional* 19.4 (2017), pp. 68–72. DOI: 10.1109/MITP.2017.3051335.

[16] Charalampos Manifavas et al. “Lightweight Cryptography for Embedded Systems – A Comparative Analysis”. In: *Data Privacy Management and Autonomous Spontaneous Security*. Ed. by Joaquin Garcia-Alfaro et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 333–349. ISBN: 978-3-642-54568-9.

[17] M. M. Méndez-Villamil et al. *Analytics by Design: Demonstrating the Value of IoT*. Apr. 2020. URL: https://cdn.idc.com/cms/ccFile/9c07f286d6cae7e1b84c/EUR146187419_-_Excerpt_SAS_Web.pdf.

[18] Peter Newman. *Microsoft is ramping up Azure’s IoT products ahead of its Build 2019 developer conference*. May 2019. URL: https://www.businessinsider.com/microsoft-strengthening-iot-azure-growth-2019-5.

[19] Danny Palmer. *175,000 IOT cameras can be remotely hacked thanks to Flaw, says security researcher*. July 2017. URL: https://www.zdnet.com/article/175000-iot-cameras-can-be-remotely-hacked-thanks-to-flaw-says-security-researcher/.

[20] Steve Ranger. *What is the IoT? Everything you need to know about the Internet of Things right now*. Feb. 2020. URL: https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/.

[21] Zonyin Shae and Jeffrey JP Tsai. “On the design of a blockchain platform for clinical trial and precision medicine”. In: *2017 IEEE 37th international conference on distributed computing systems (ICDCS)*. IEEE. 2017, pp. 1972–1980.

[22] T-Systems. *Predictive blockchain*. Feb. 2018. URL: https://www.t-systems.com/de/en/newsroom/best-practice/02-2018-brilliant-prospects/blockchain-blacklist-for-smartphones-prevents-data-theft.

[23] Wade Trappe, Richard Howard, and Robert S. Moore. “Low-Energy Security: Limits and Opportunities in the Internet of Things”. In: *IEEE Security & Privacy* 13.1 (2015), pp. 14–21. DOI: 10.1109/MSP.2015.7.

[24] William Turton. *Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals*. Mar. 2021. URL: https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams.

[25] *Understanding the Value of Blockchain for Clinical Trial Data*. Mar. 2022. URL: https://www.anjusoftware.com/about/all-news/insights/blockchain-for-clinical-trial-data.

[26] Nicky Woolf. *DDoS attack that disrupted internet was largest of its kind in history, experts say*. Oct. 2016. URL: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[27] Aaron Wright and Primavera De Filippi. "Decentralized blockchain technology and the rise of lex cryptographia". In: *Available at SSRN 2580664* (2015).

[28] Yu Zhang and Jiangtao Wen. "An IoT electric business model based on the protocol of bitcoin". In: *2015 18th international conference on intelligence in next generation networks*. IEEE. 2015, pp. 184–191.