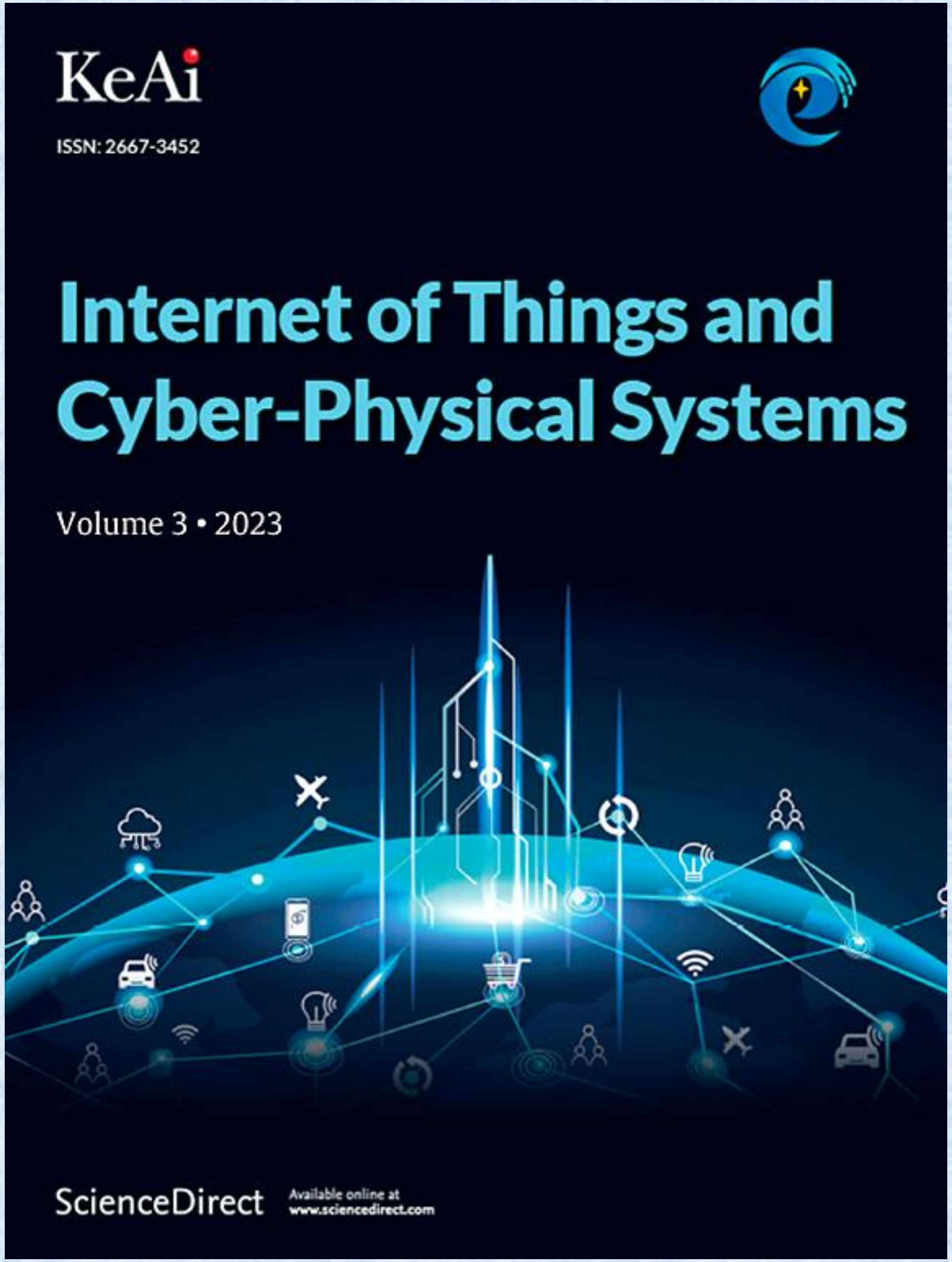
Security of cyber-physical systems

A. Ravishankar Rao
Ph.D
IEEE Fellow

FAIRLEIGH
DICKINSON
UNIVERSITY

AI and Cybersecurity
Organized by
Dr. Maksim Iavich and the team
Caucasus University and
Scientific Cyber Security Association

კავკასიის უნივერსიტეტი
CAUCASUS UNIVERSITY



KeAi

ISSN: 2667-3452

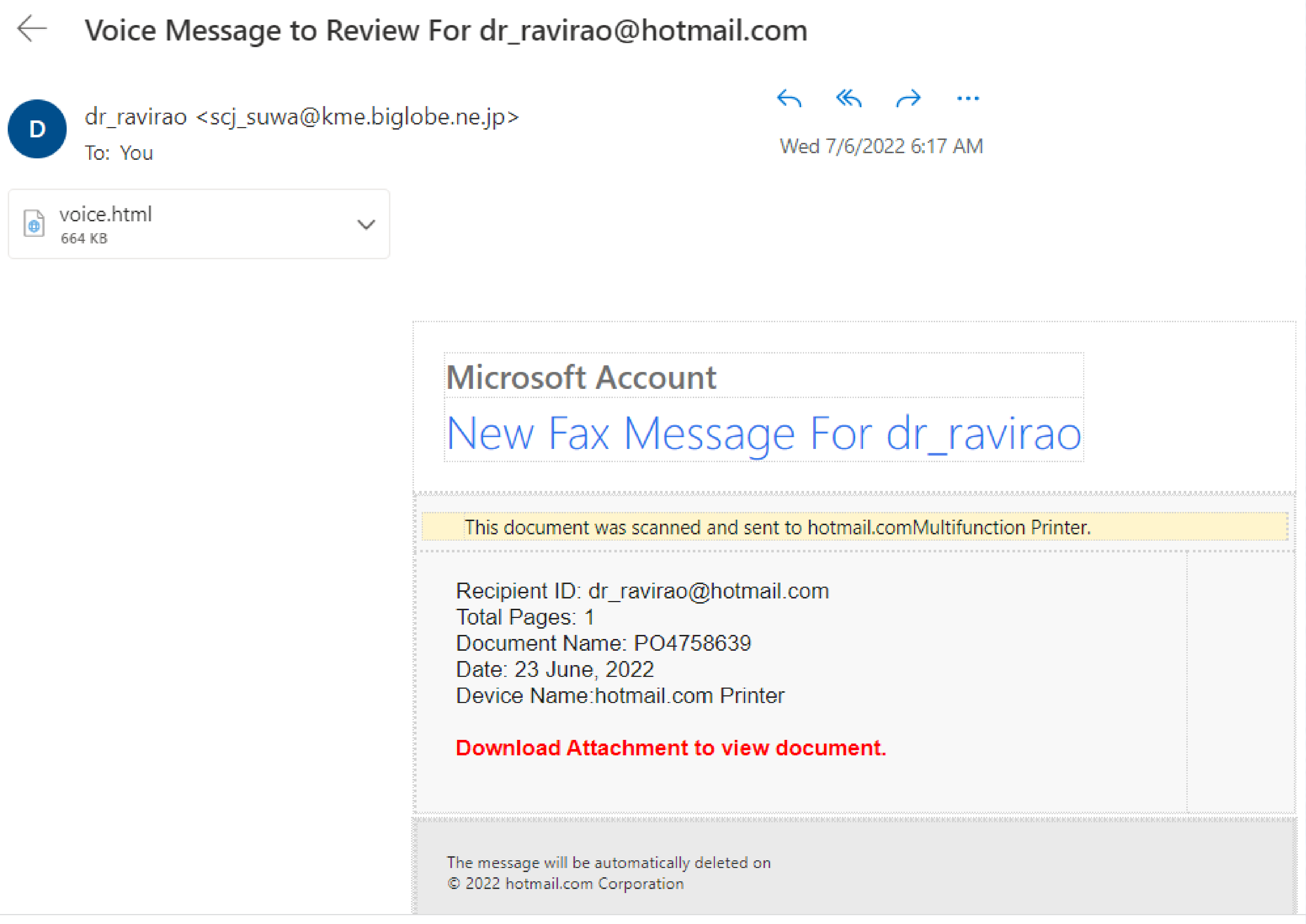
Internet of Things and Cyber-Physical Systems

Volume 3 • 2023

ScienceDirect Available online at www.sciencedirect.com

A.R. Rao, A. Elias-Medina, “Designing an internet-of-things laboratory to improve student understanding of secure IoT systems”, Journal of Internet of Things and Cyber-physical Systems, Elsevier Publishers, to appear in November 2023.

How do we trust communication between parties?



Voice Message to Review For dr_ravirao@hotmail.com

dr_ravirao <scj_suwa@kme.biglobe.ne.jp>
To: You

Wed 7/6/2022 6:17 AM

voice.html
664 KB

Microsoft Account

New Fax Message For dr_ravirao

This document was scanned and sent to hotmail.comMultifunction Printer.

Recipient ID: dr_ravirao@hotmail.com
Total Pages: 1
Document Name: PO4758639
Date: 23 June, 2022
Device Name:hotmail.com Printer

Download Attachment to view document.

The message will be automatically deleted on
© 2022 hotmail.com Corporation

Use case : Monitoring a food supply chain

Walmart is betting on the blockchain to improve food safety

Ron Miller @ron_miller / 6 months ago

Comment

Techcrunch, 2018

Context: Salmonella outbreak

United Nations humanitarian efforts

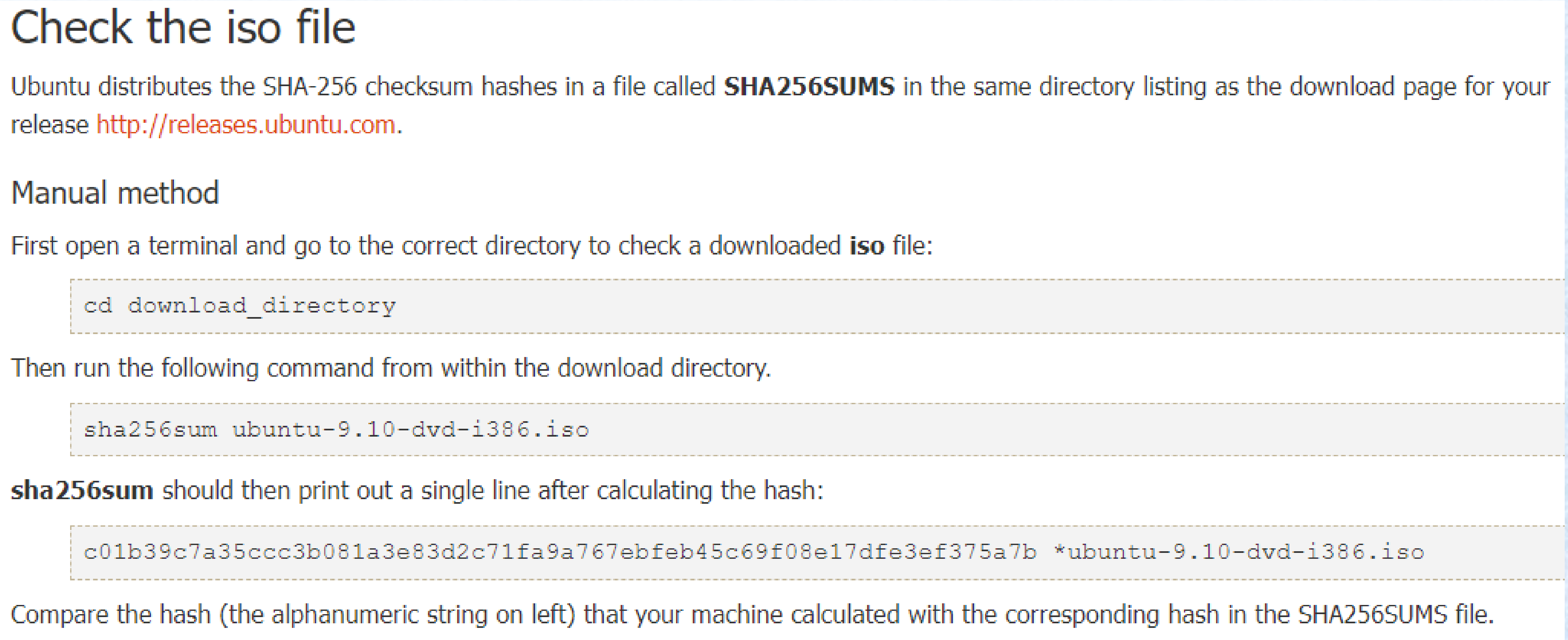
Only 10 percent of the supplies reach the intended people

https://www.cbsnews.com/news/supply-chain-issues-cargo-theft/

SHA-256 hashes used properly can confirm both file integrity and authenticity.

Comparing hashes makes it possible to detect changes in files that would cause errors. The possibility of changes (errors) is proportional to the size of the file; the possibility of errors increase as the file becomes larger. It is a very good idea to run an SHA-256 hash comparison check when you have a file like an operating system install CD that has to be 100% correct.

https://help.ubuntu.com/community/HowToSHA256SUM



Check the iso file

Ubuntu distributes the SHA-256 checksum hashes in a file called **SHA256SUMS** in the same directory listing as the download page for your release http://releases.ubuntu.com.

Manual method

First open a terminal and go to the correct directory to check a downloaded **iso** file:

```
cd download_directory
```

Then run the following command from within the download directory.

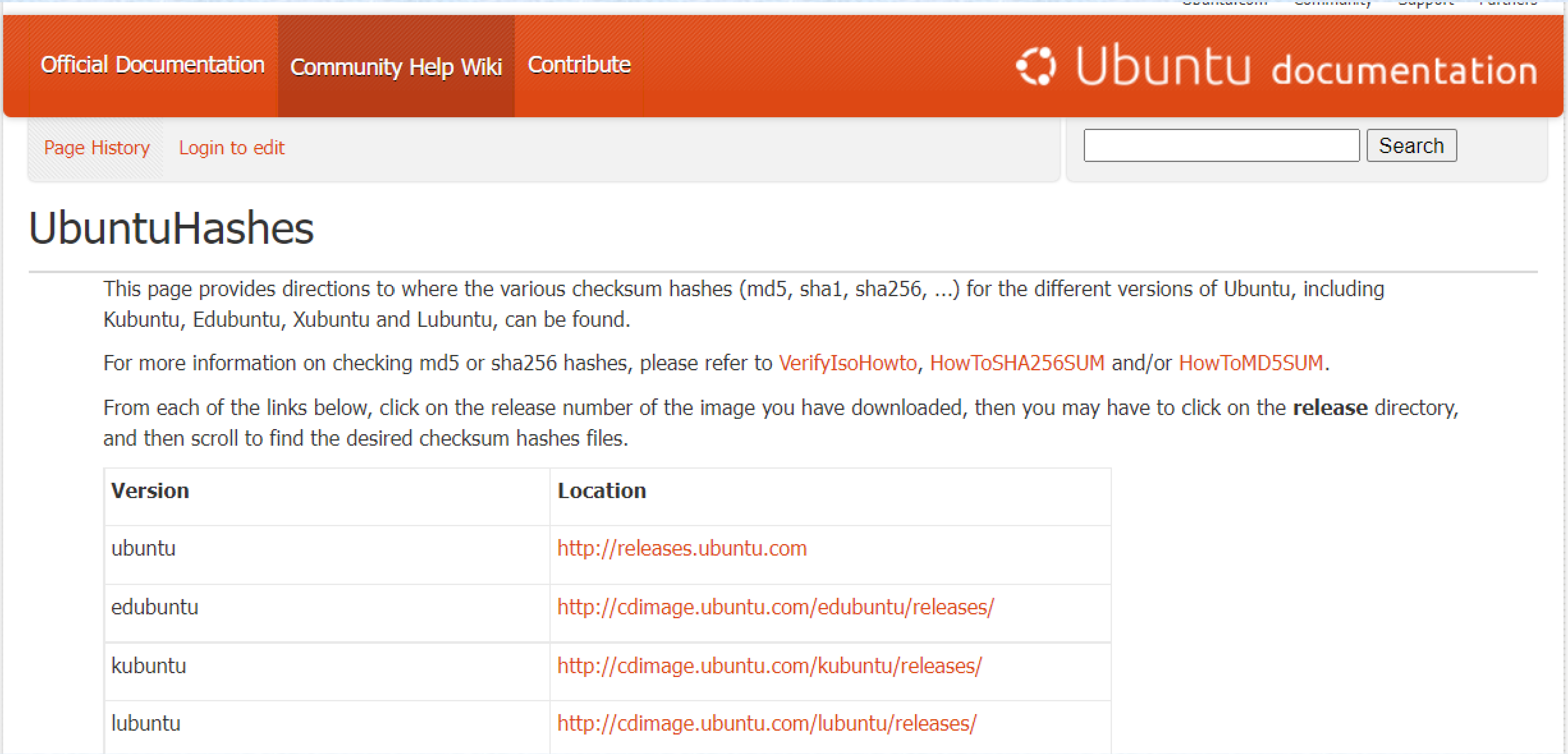
```
sha256sum ubuntu-9.10-dvd-i386.iso
```

sha256sum should then print out a single line after calculating the hash:

```
c01b39c7a35ccc3b081a3e83d2c71fa9a767ebfeb45c69f08e17dfe3ef375a7b *ubuntu-9.10-dvd-i386.iso
```

Compare the hash (the alphanumeric string on left) that your machine calculated with the corresponding hash in the SHA256SUMS file.

https://help.ubuntu.com/community/HowToSHA256SUM



UbuntuHashes

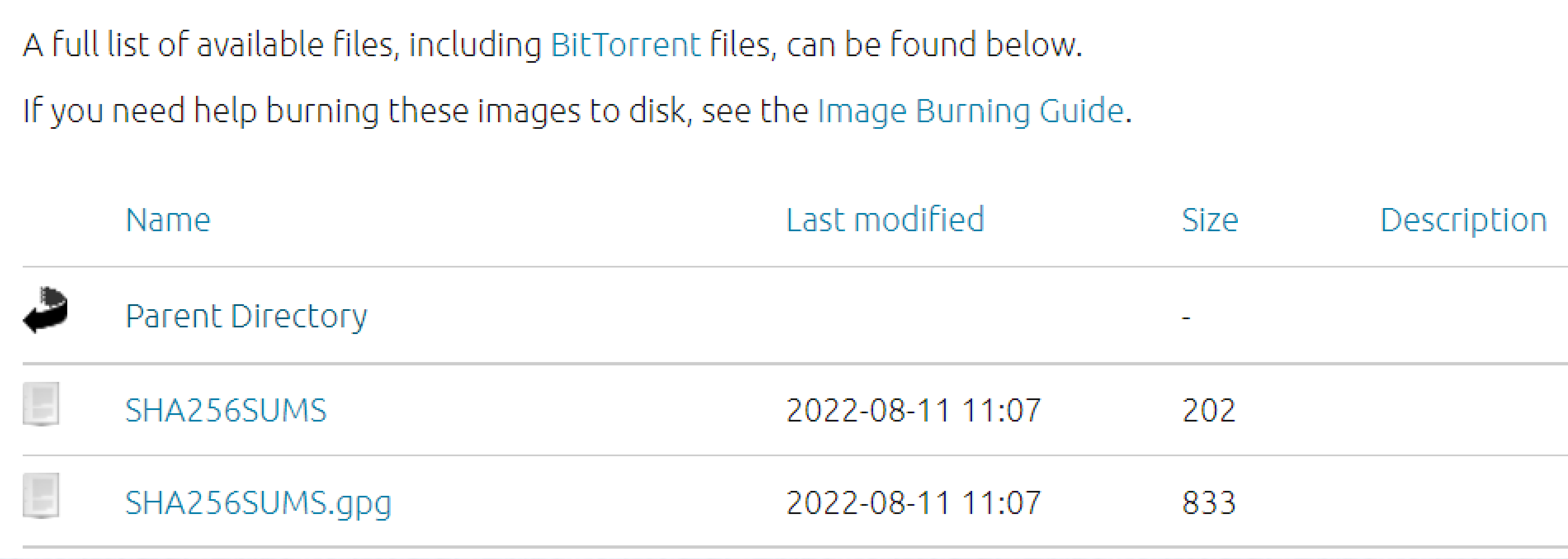
This page provides directions to where the various checksum hashes (md5, sha1, sha256, ...) for the different versions of Ubuntu, including Kubuntu, Edubuntu, Xubuntu and Lubuntu, can be found.

For more information on checking md5 or sha256 hashes, please refer to VerifyIsoHowto, HowToSHA256SUM and/or HowToMD5SUM.

From each of the links below, click on the release number of the image you have downloaded, then you may have to click on the **release** directory, and then scroll to find the desired checksum hashes files.

Version	Location
ubuntu	http://releases.ubuntu.com
edubuntu	http://cdimage.ubuntu.com/edubuntu/releases/
kubuntu	http://cdimage.ubuntu.com/kubuntu/releases/
lubuntu	http://cdimage.ubuntu.com/lubuntu/releases/

https://help.ubuntu.com/community/UbuntuHashes http://releases.ubuntu.com/jammy/



A full list of available files, including BitTorrent files, can be found below.

If you need help burning these images to disk, see the Image Burning Guide.

Name	Last modified	Size	Description
Parent Directory		-	
SHA256SUMS	2022-08-11 11:07	202	
SHA256SUMS.gpg	2022-08-11 11:07	833	

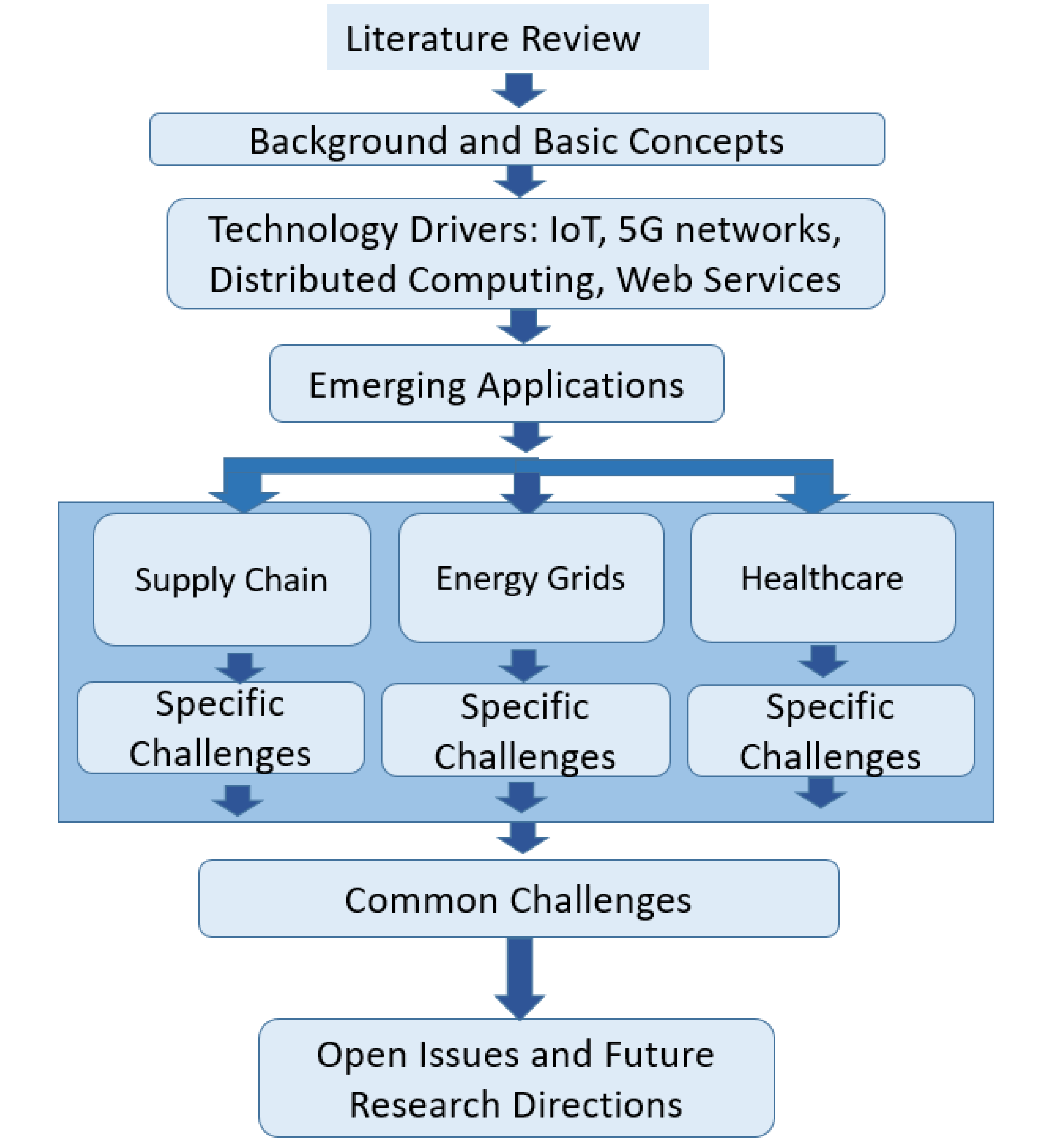
http://releases.ubuntu.com/jammy/SHA256SUMS

c396e956a9f52c418397867d1ea5c0cf
1a99a49dcf648b086d2fb762330cc88d

→ ubuntu-22.04.1-desktop-amd64.iso

Basic questions

- How are medical tests done today?
- What is the potential for errors?
- If we automate the system, there is more potential for cyberattacks (the attack surface increases)



Literature Review

Background and Basic Concepts

Technology Drivers: IoT, 5G networks, Distributed Computing, Web Services

Emerging Applications

Supply Chain

Energy Grids

Healthcare

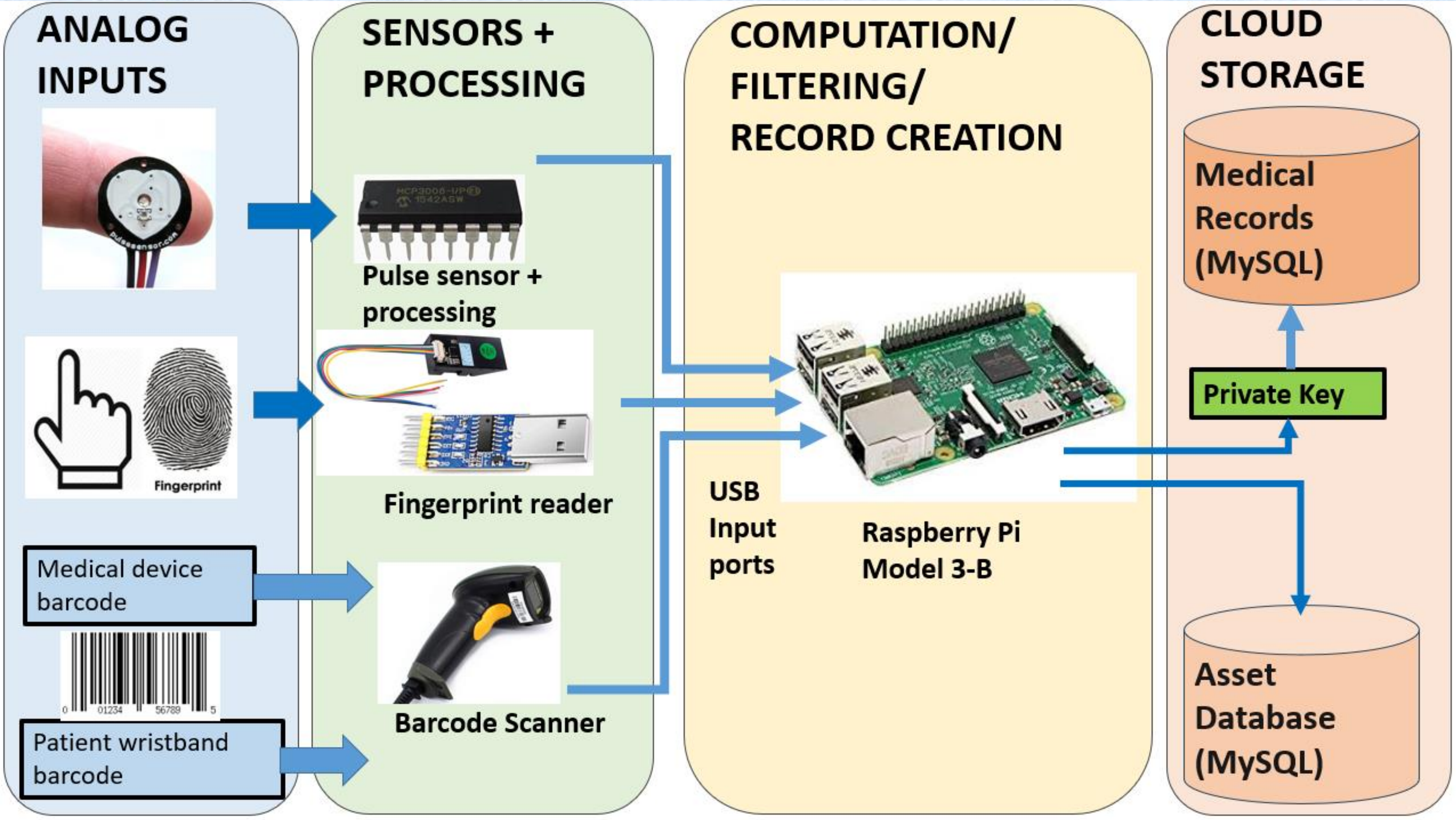
Specific Challenges

Specific Challenges

Specific Challenges

Common Challenges

Open Issues and Future Research Directions



ANALOG INPUTS

SENSORS + PROCESSING

COMPUTATION/ FILTERING/ RECORD CREATION

CLOUD STORAGE

Pulse sensor + processing

Fingerprint reader

Medical device barcode

Patient wristband barcode

Barcode Scanner

USB Input ports

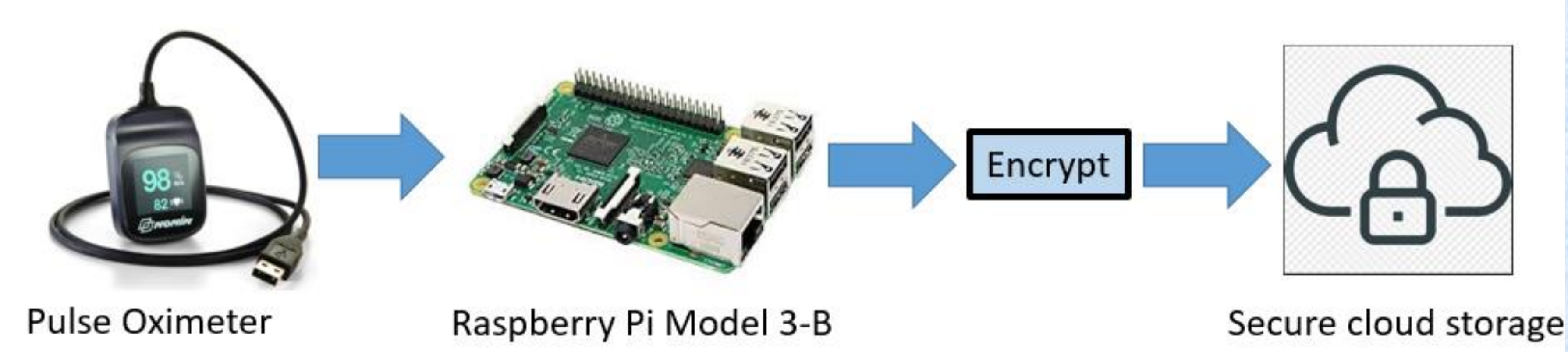
Raspberry Pi Model 3-B

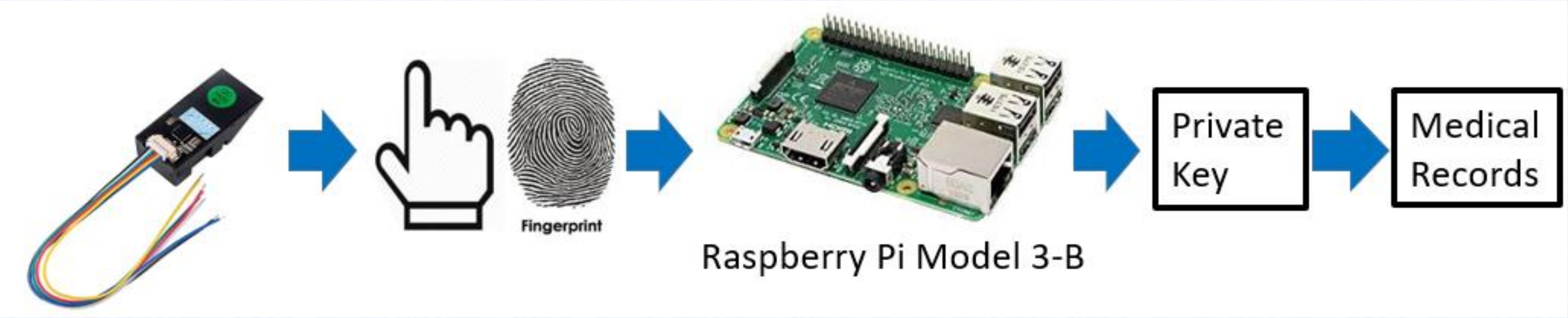
Private Key

Medical Records (MySQL)

Asset Database (MySQL)

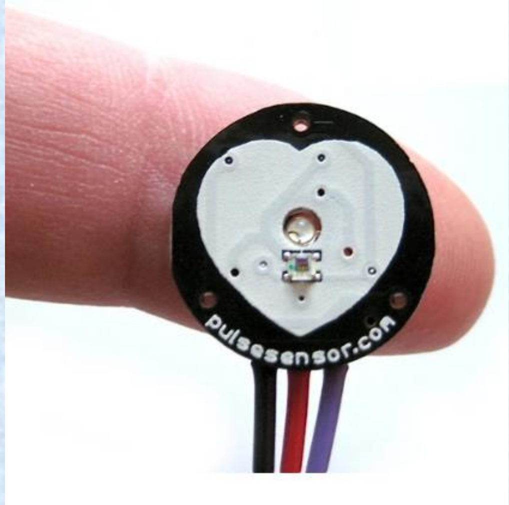
Simple Medical Devices



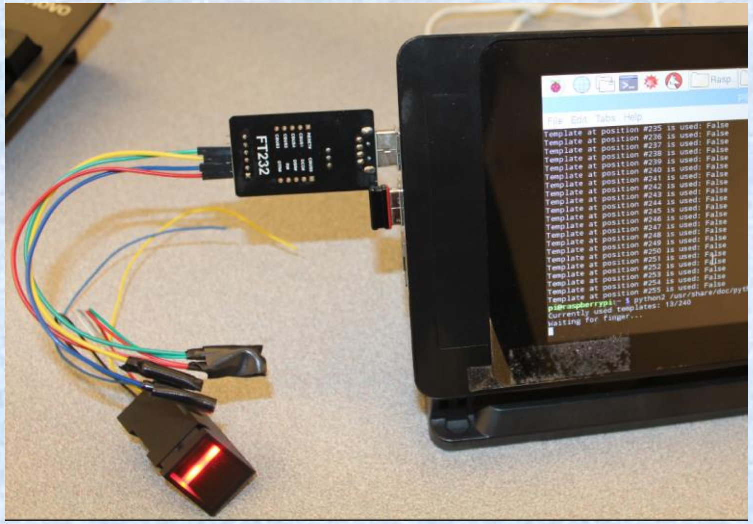


Scanning of patient barcodes

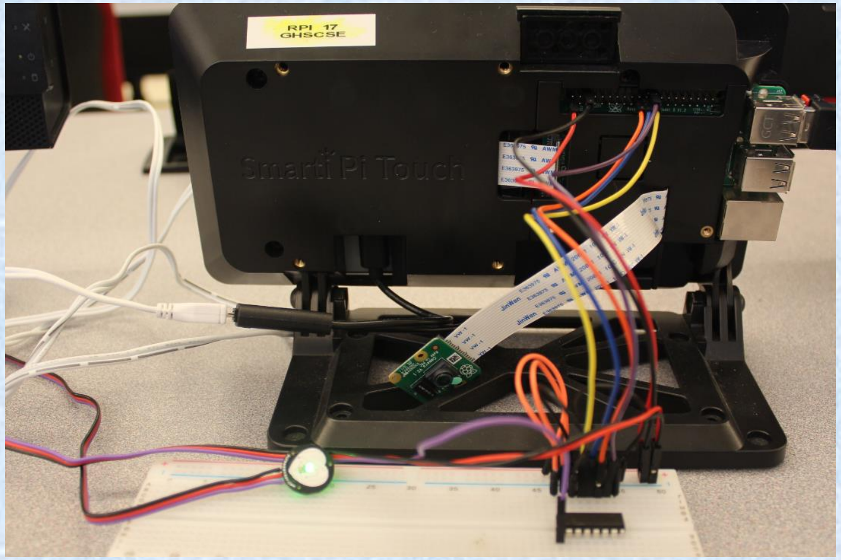
Pulse sensor

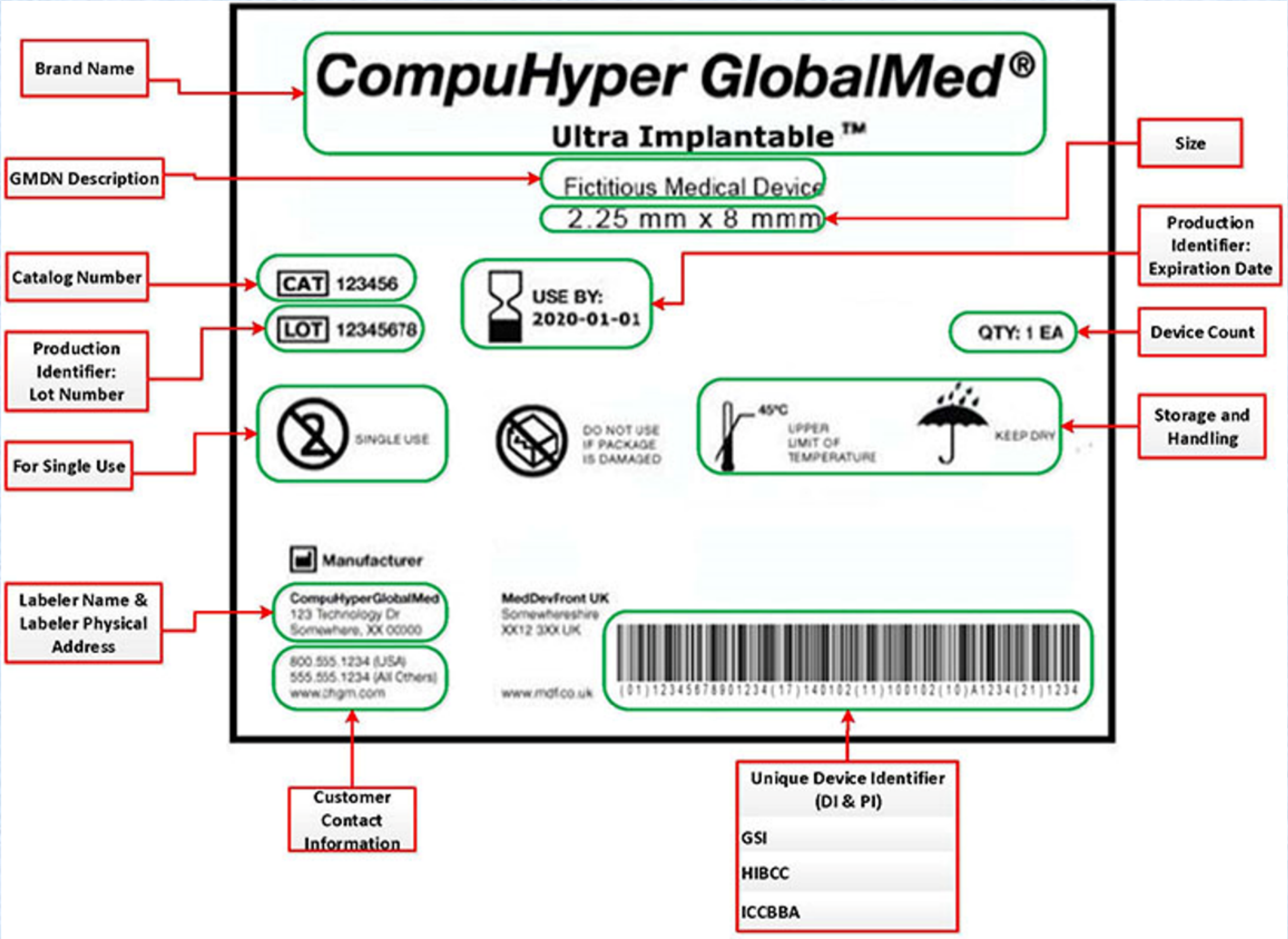


Fingerprint sensor

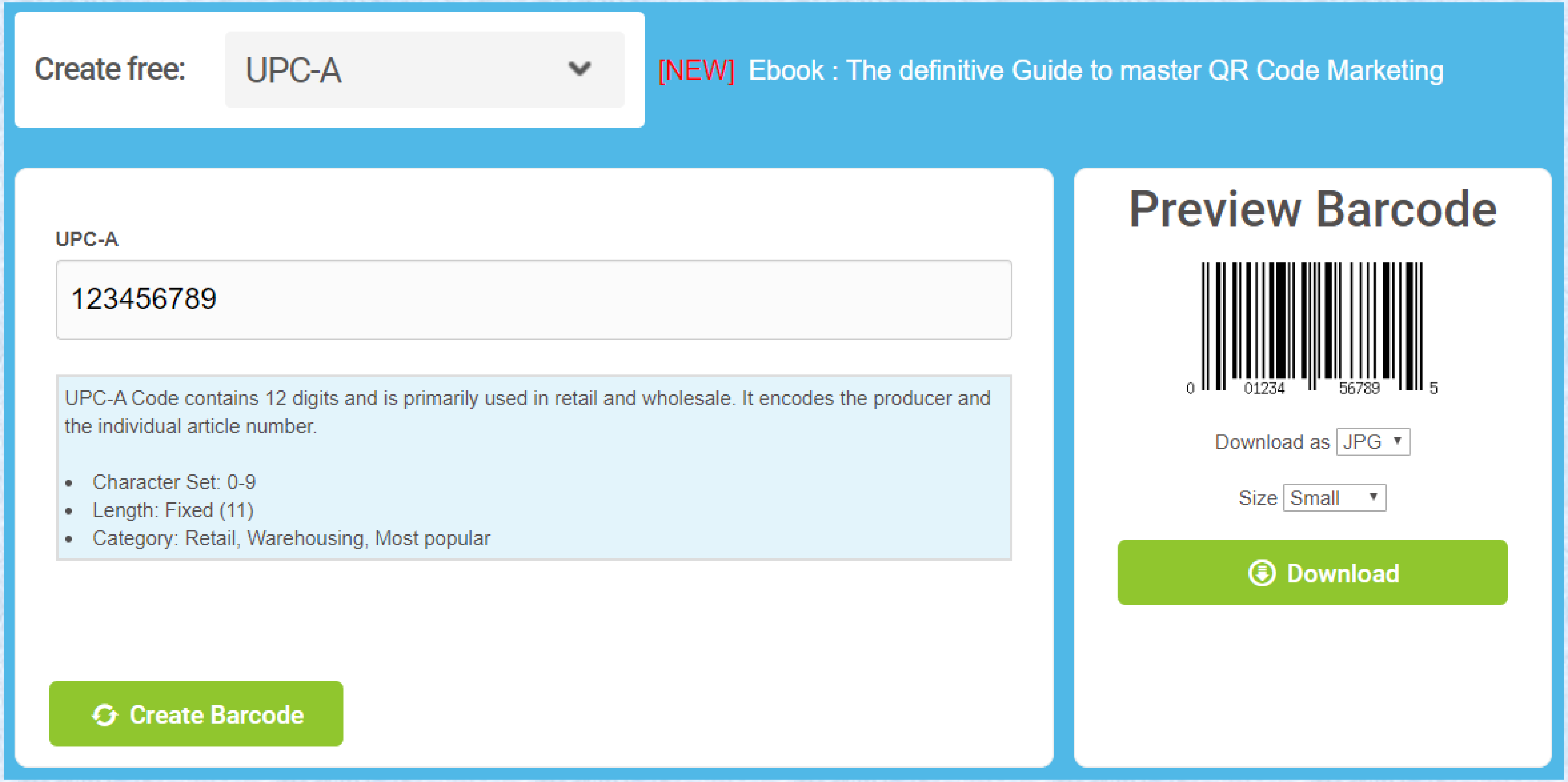


```
Template at position #235 is used: False
Template at position #236 is used: False
Template at position #237 is used: False
Template at position #238 is used: False
Template at position #239 is used: False
Template at position #240 is used: False
Template at position #241 is used: False
Template at position #242 is used: False
Template at position #243 is used: False
Template at position #244 is used: False
Template at position #245 is used: False
Template at position #246 is used: False
Template at position #247 is used: False
Template at position #248 is used: False
Template at position #249 is used: False
Template at position #250 is used: False
Template at position #251 is used: False
Template at position #252 is used: False
Template at position #253 is used: False
Template at position #254 is used: False
Template at position #255 is used: False
pi@raspberrypi:~ $ python2 /usr/share/doc/pyt
Currently used templates: 13/240
Waiting for finger...
```





The government website fda.gov provides an example of a fictitious label containing a UDI (unique device identifier).



Create free:
UPC-A
[NEW] Ebook : The definitive Guide to master QR Code Marketing

UPC-A

123456789

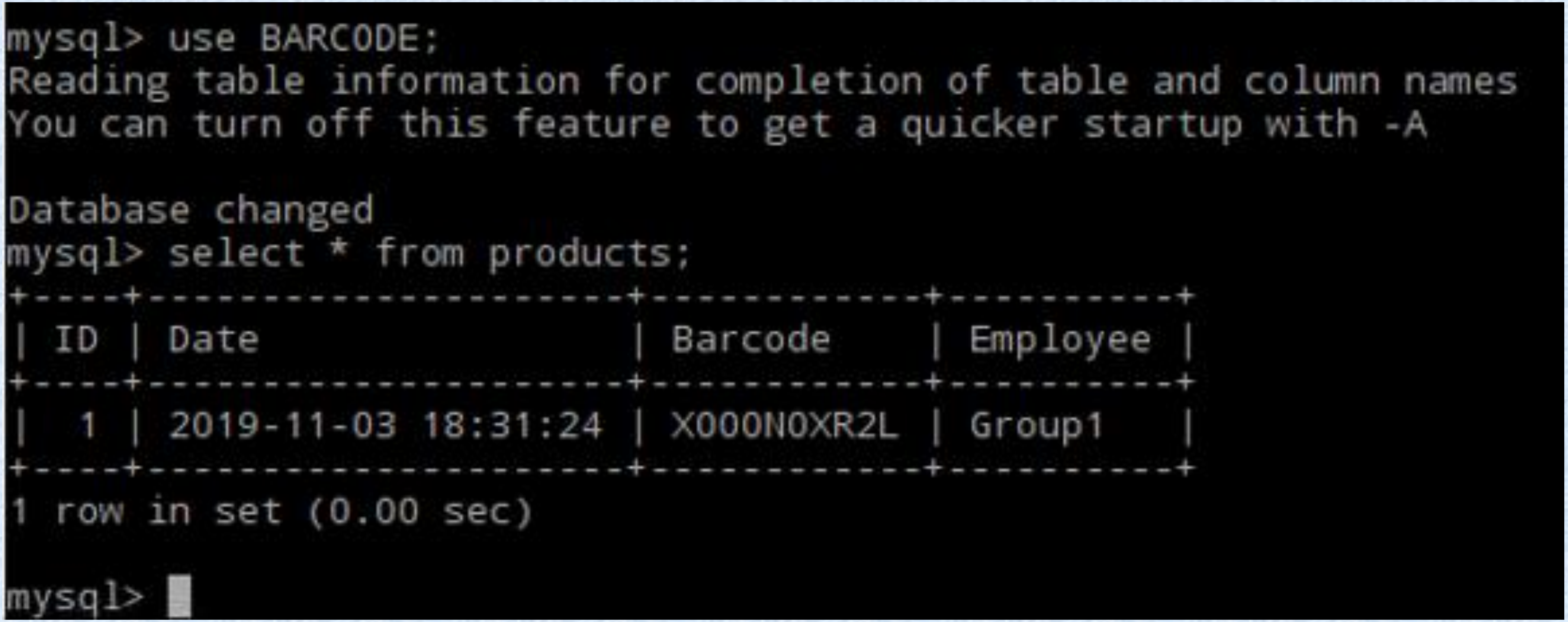
UPC-A Code contains 12 digits and is primarily used in retail and wholesale. It encodes the producer and the individual article number.

- Character Set: 0-9
- Length: Fixed (11)
- Category: Retail, Warehousing, Most popular

Download as JPG

Size Small

Creating a fictitious barcode:
https://www.barcode-generator.org/



```
mysql> use BARCODE;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select * from products;
+----+---------------------+------------+----------+
| ID | Date                | Barcode    | Employee |
+----+---------------------+------------+----------+
|  1 | 2019-11-03 18:31:24 | X000N0XR2L | Group1   |
+----+---------------------+------------+----------+
1 row in set (0.00 sec)

mysql> 
```

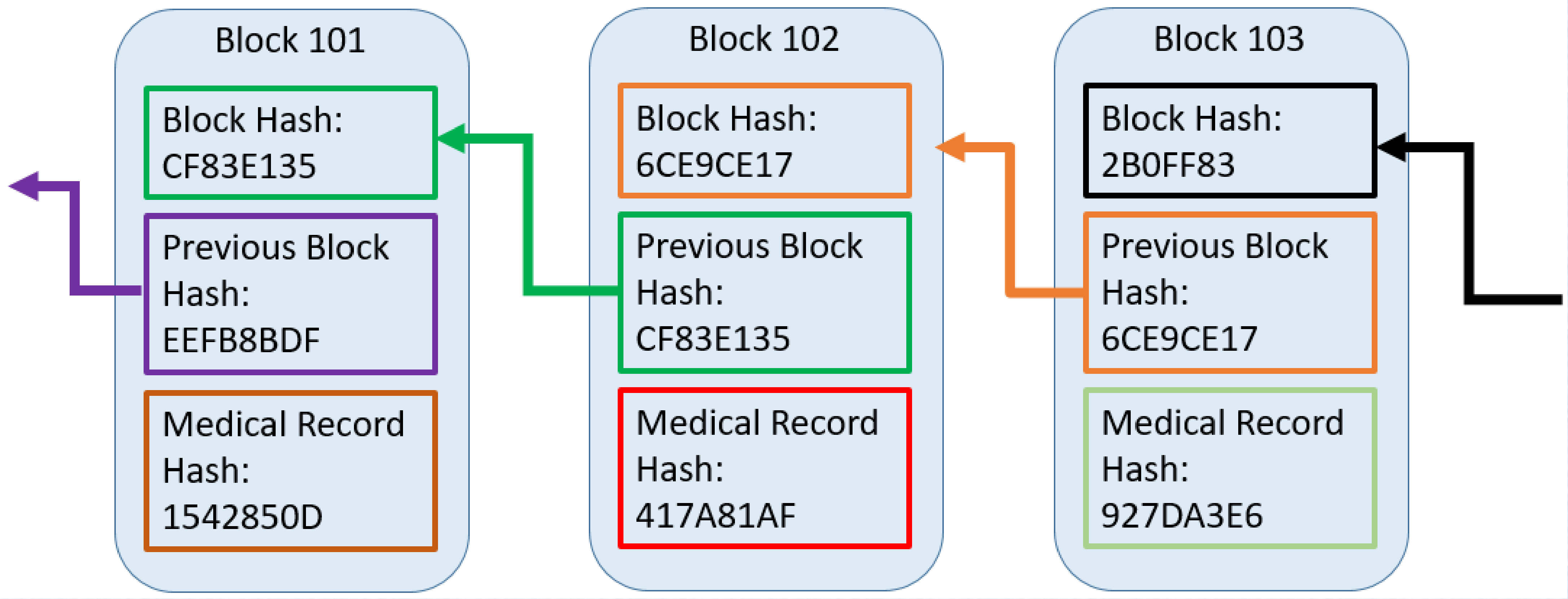
A screenshot of a Raspberry-Pi terminal session showing the successful creation of MySQL table with the scanned barcode. This view is from within MySQL, which is launched by typing ‘mysql’ at the Linux command prompt. During this launch, the user is prompted for a valid password. Only authorized users can view the data in the table. The name of the Employee is ‘Group1’ for illustrative purposes.

Potential for SQL Injection Attacks

An example of such a query is

*select * from login where username= “Bob” or 1=1;*

Alternately, a comment field can be used to conduct a SQL injection.


Block 101
Block Hash: CF83E135
Previous Block Hash: EEFB8BDF
Medical Record Hash: 1542850D
Block 102
Block Hash: 6CE9CE17
Previous Block Hash: CF83E135
Medical Record Hash: 417A81AF
Block 103
Block Hash: 2B0FF83
Previous Block Hash: 6CE9CE17
Medical Record Hash: 927DA3E6

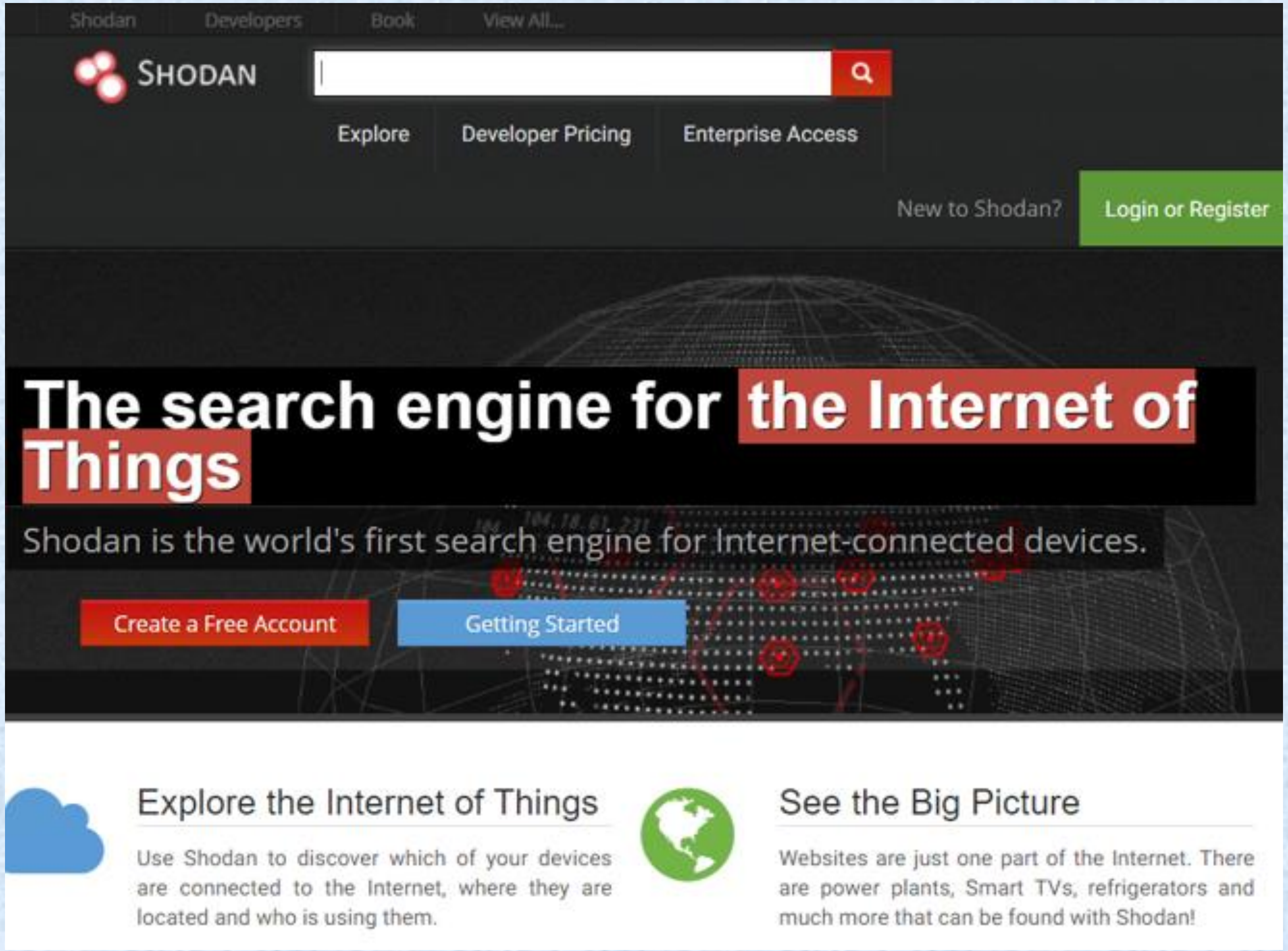
A simple depiction of a blockchain. For instance, we can consider each block to represent a medical record. This medical record could combine data related to patient vitals with biometrics collected by IoT devices.

Desirable properties of blockchains

Definition: A public, permanent, append-only distributed ledger

- Decentralization
- Persistency
- Anonymity
- Auditability

Shodan.io



The search engine for the Internet of Things

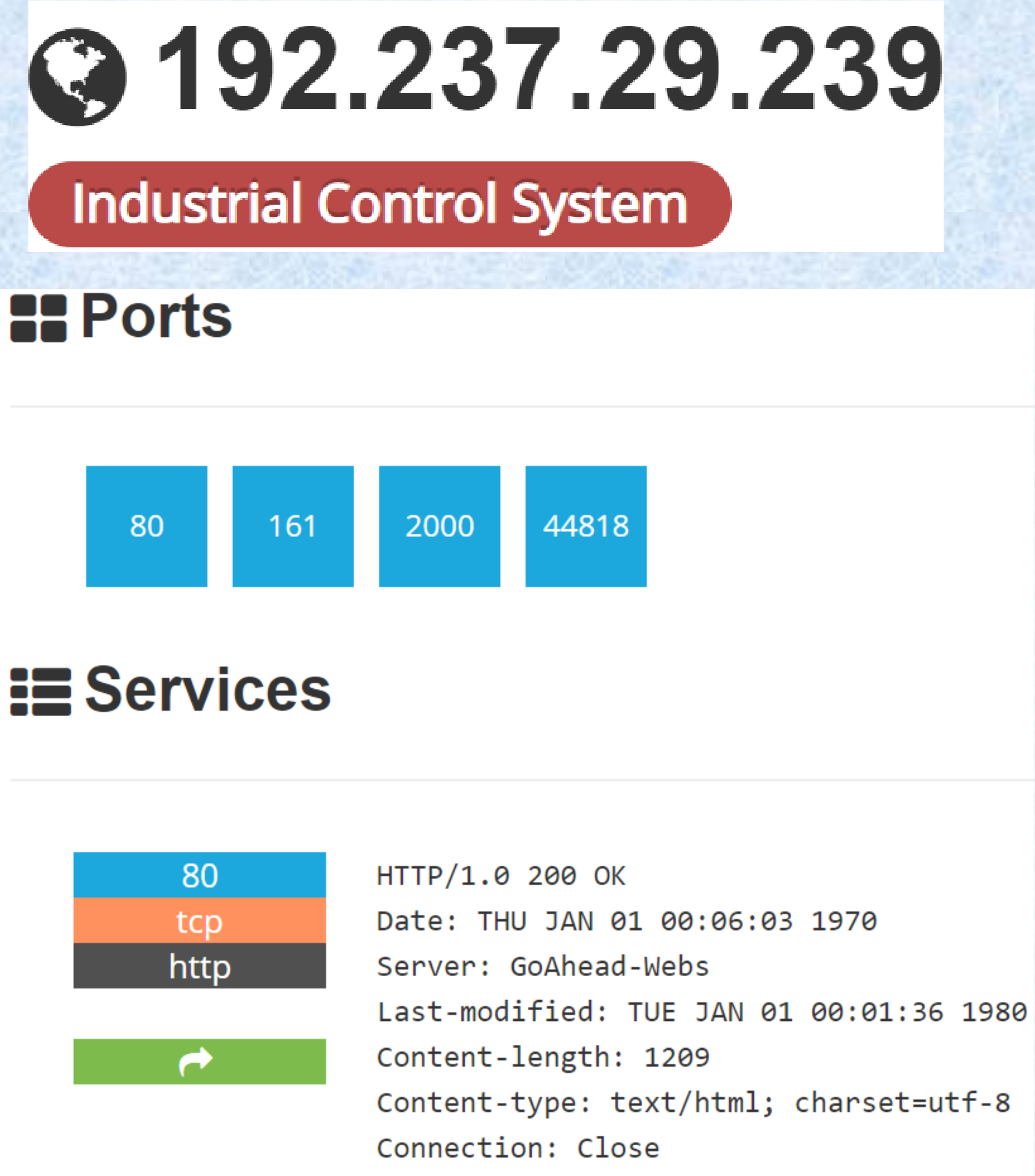
Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



192.237.29.239

Industrial Control System

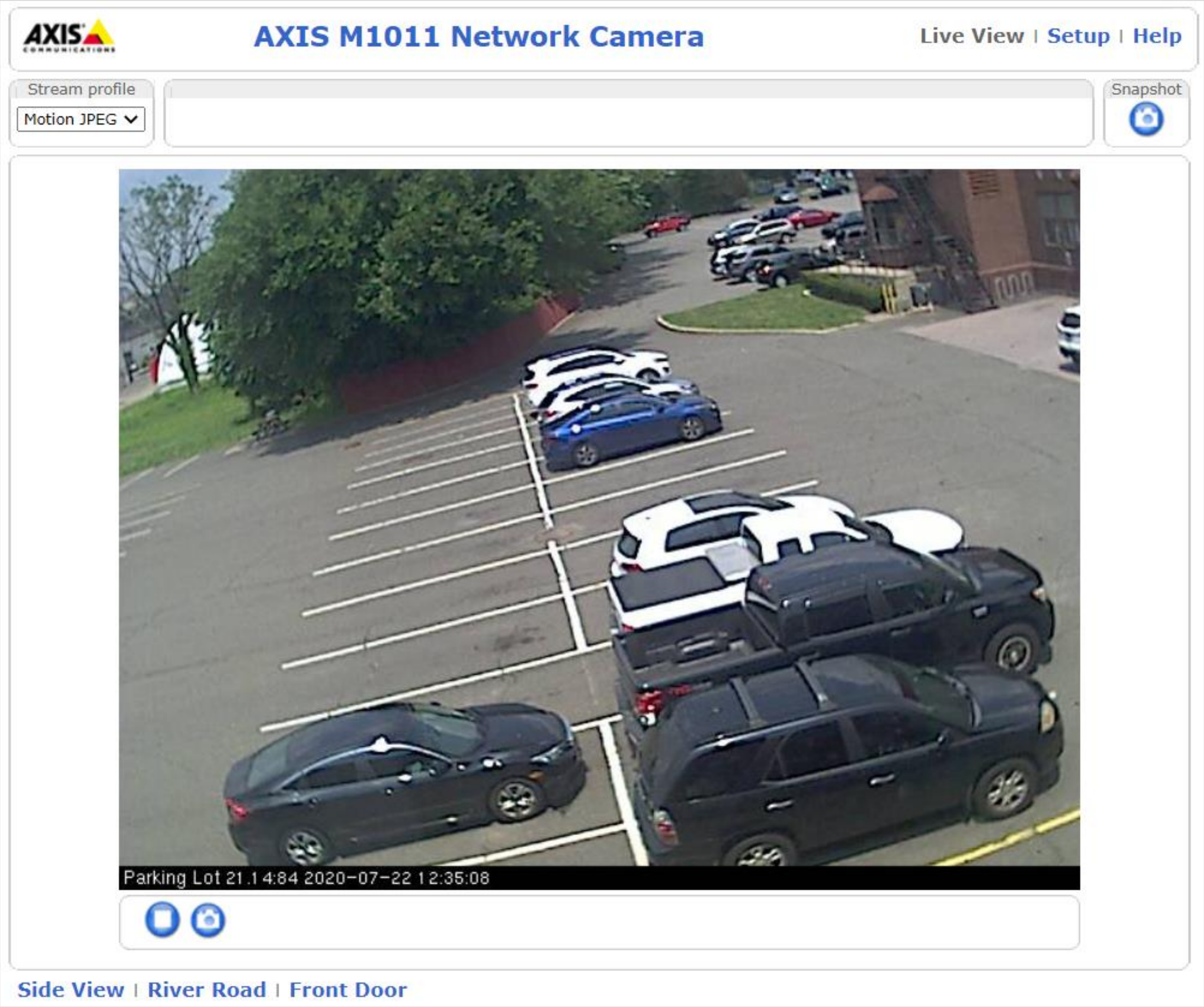
Ports

Services

```
HTTP/1.0 200 OK
Date: THU JAN 01 00:06:03 1970
Server: GoAhead-Webs
Last-modified: TUE JAN 01 00:01:36 1980
Content-length: 1209
Content-type: text/html; charset=utf-8
Connection: Close
```

The search engine Shodan allows users to search for IoT devices on the internet.

Shodan.io

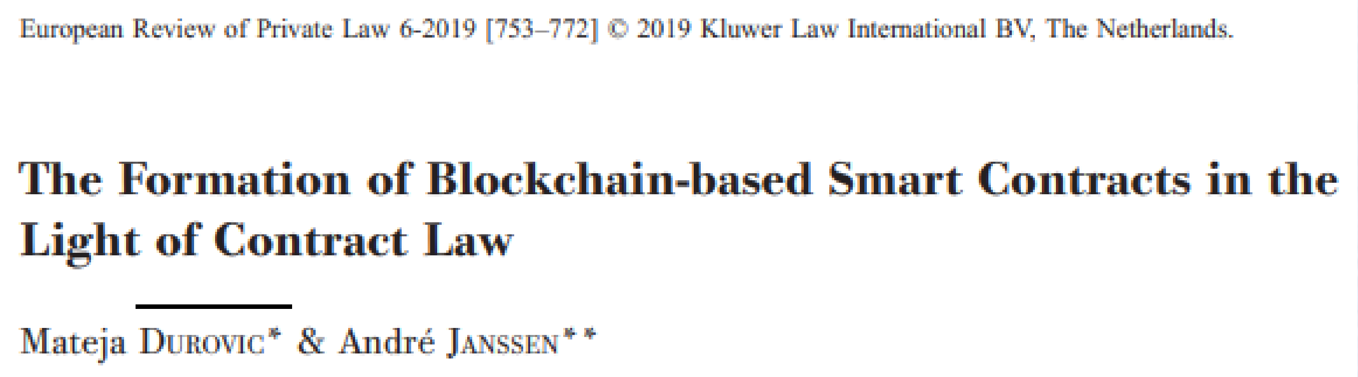


AXIS M1011 Network Camera

Stream profile: Motion JPEG

Parking Lot 21.1 4:84 2020-07-22 12:35:08

Problem with smart contracts

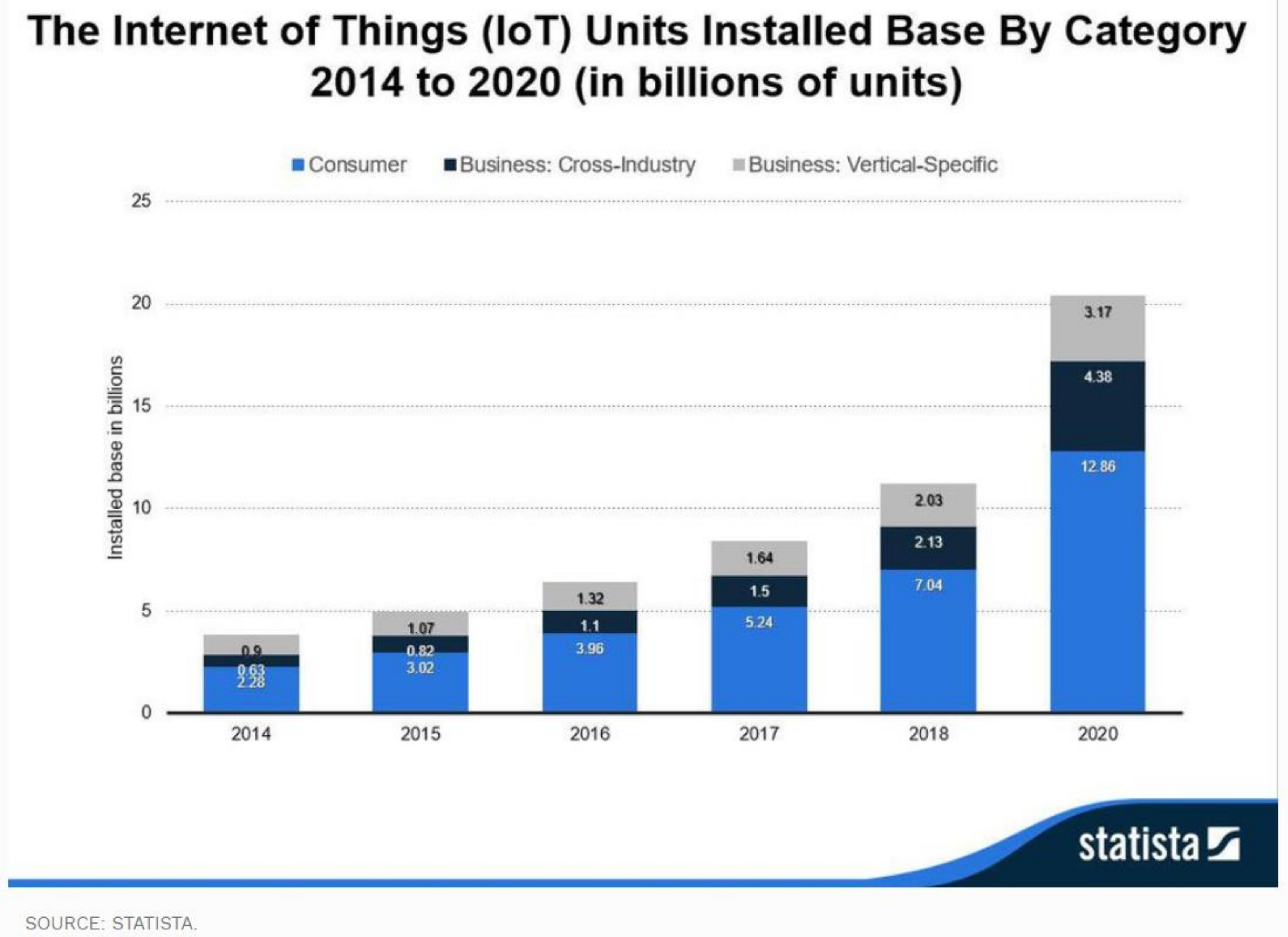


European Review of Private Law 6-2019 [753–772] © 2019 Kluwer Law International BV, The Netherlands.

The Formation of Blockchain-based Smart Contracts in the Light of Contract Law

Mateja DUROVIC* & André JANSSEN**

- They are neither smart nor contracts (ie legally enforceable)!
- 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.

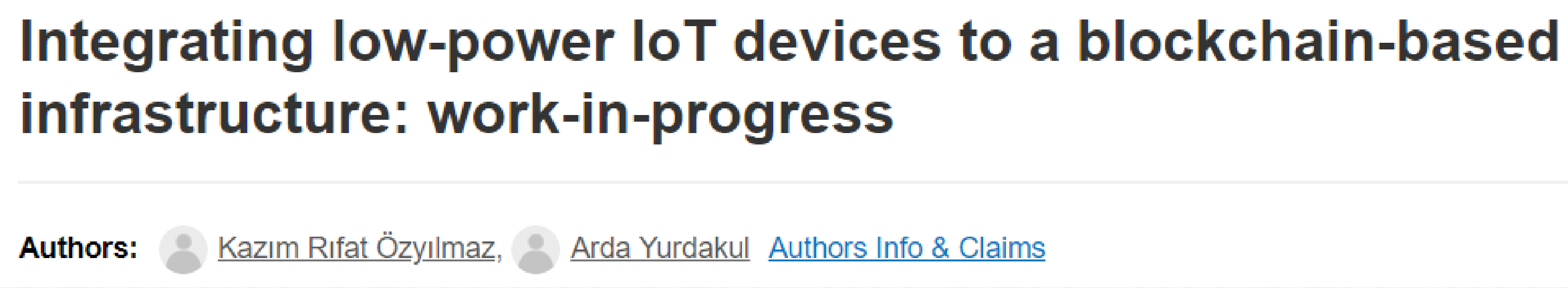


The Internet of Things (IoT) Units Installed Base By Category 2014 to 2020 (in billions of units)

SOURCE: STATISTA.

https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide

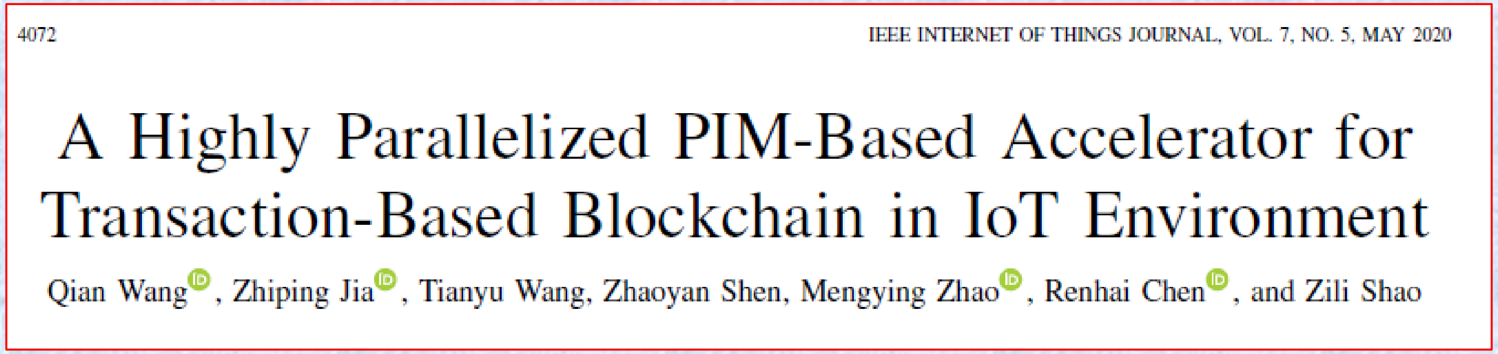
Challenge: IoT Devices lack computational power



Integrating low-power IoT devices to a blockchain-based infrastructure: work-in-progress

Authors: Kazım Rıfat Özyılmaz, Arda Yurdakul Authors Info & Claims

2017



4072 IEEE INTERNET OF THINGS JOURNAL, VOL. 7, NO. 5, MAY 2020

A Highly Parallelized PIM-Based Accelerator for Transaction-Based Blockchain in IoT Environment

Qian Wang, Zhiping Jia, Tianyu Wang, Zhaoyan Shen, Mengying Zhao, Renhai Chen, and Zili Shao

2020

electronics MDPI

Article

Design and Hardware Implementation of a Simplified DAG-Based Blockchain and New AES-CBC Algorithm for IoT Security

Sung-Won Lee and Kwee-Bo Sim *

Department of Electrical and Electronics Engineering, Chung-Ang University, Seoul 06974, Korea; sungwon8912@cau.ac.kr
* Correspondence: kbsim@cau.ac.kr; Tel.: +82-10-8997-1256

2021

Steady progress

Enablers of IoT + Blockchain applications

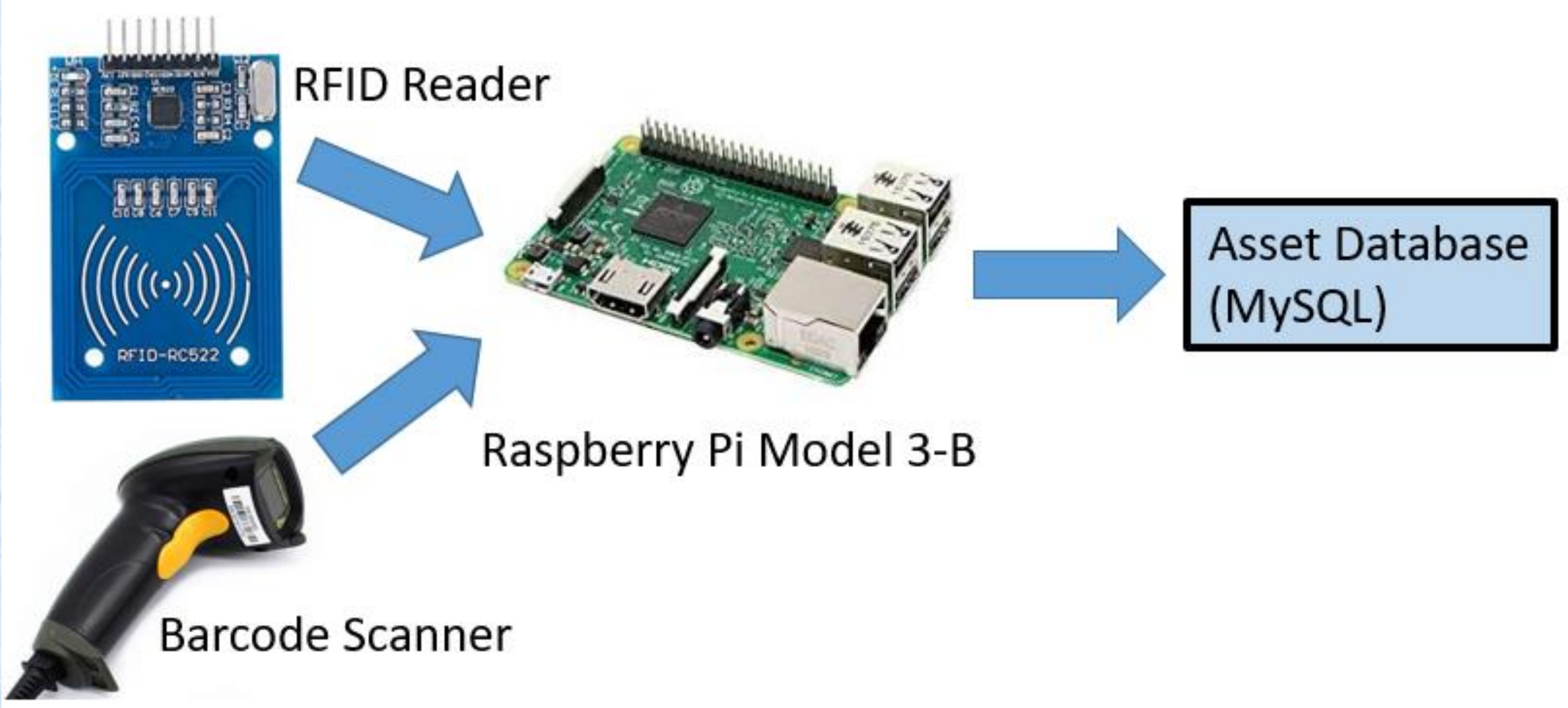
- Adoption of 5G networks and beyond (6G)
- Faster hardware acceleration
  - Custom ASICs, modules for SHA256 computation
- Cloud computing
- Web services
  - Amazon Web Services (AWS) offers blockchain as a fully managed service

EMERGING APPLICATIONS: 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.

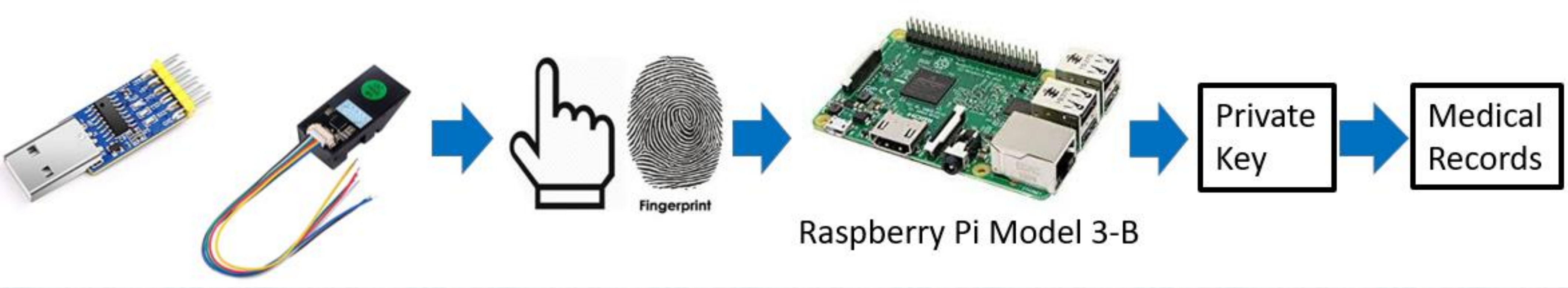
EMERGING APPLICATIONS: FOCUS APPLICATION #1: HEALTHCARE



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

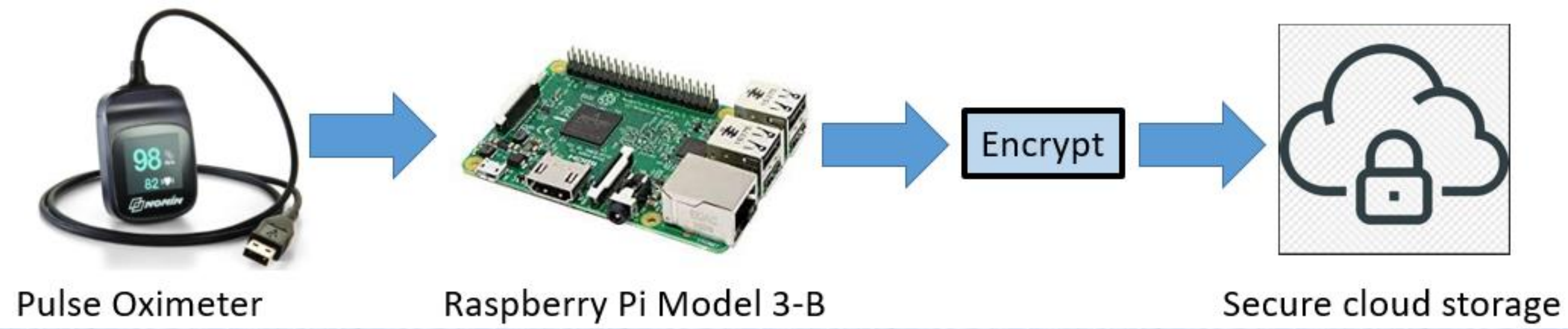
Using patient biometrics for identification

- Currently, most hospitals in the US identify patients by their name birthdate.
- This is causing increasing problems as multiple patients may have the same name and birthdate.
- The Wall Street Journal recently reported that in a Texas healthcare system, “there are now 2,833 Maria Garcias, with 528 of them having the same date of birth.”



Using sensors to measure patient vitals

- 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. 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.

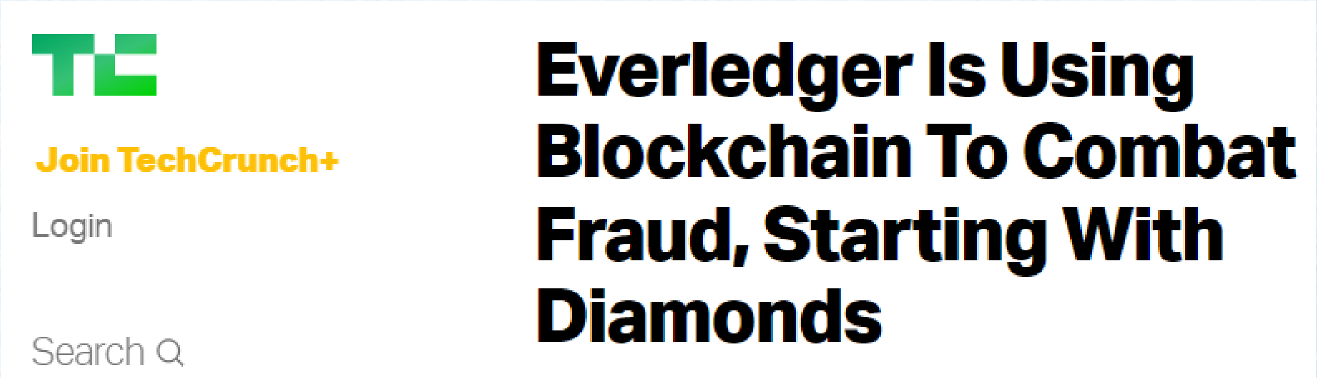


EMERGING APPLICATIONS:

FOCUS APPLICATION #2: SUPPLY CHAINS

Food supply chains

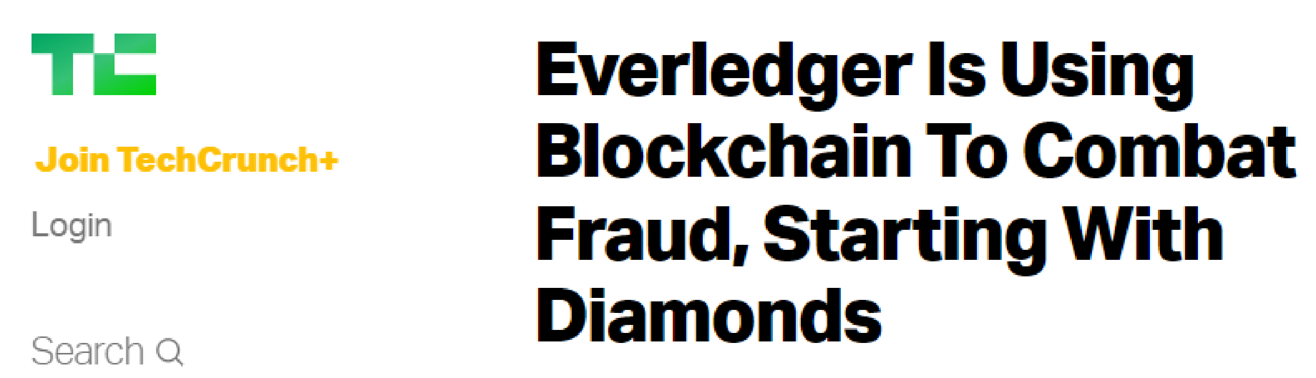
- Wastage of around 50% of products
- Containers must have the right temperature
  - Too cold is not good
  - Too hot is not good
- Suppliers are unaware of this problem
- Should be able to enforce contracts
  - Temperature stays within a certain range
- Solution: Use IoT sensors, RFID tags, sensor networks, blockchain
- Smart system: only adds significant temperature variations to the blockchain
  - Avoids need to continuously store data
  - Tamper resistant



Everledger Is Using Blockchain To Combat Fraud, Starting With Diamonds

- 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.
- Create a set of forty physical features 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.
- Not possible with diamonds, but with pharmaceutical pills/packaging

https://techcrunch.com/2015/06/29/everledger/

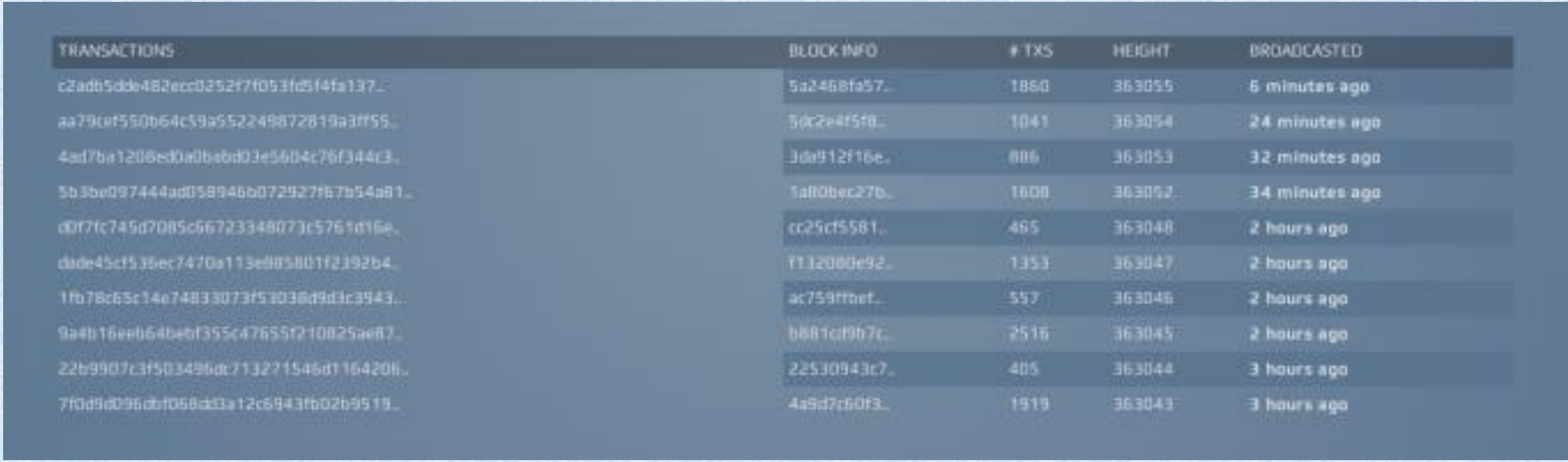


Join TechCrunch+

Login

Search

Everledger Is Using Blockchain To Combat Fraud, Starting With Diamonds



TRANSACTIONS	BLOCK INFO	# TXS	HEIGHT	BROADCASTED
c2adb5dde482ecc0252f7f053fd5f4fa137...	5a2468fa57...	1860	363055	6 minutes ago
aa79cef550b64c59a55224987281 9a3ff55...	5dc2e4f5f8...	1041	363054	24 minutes ago
4ad7ba1206ed0a0babd03e5604c76f344c3...	3da912f16e...	886	363053	32 minutes ago
5b3be097444ad0589466072927f67b54a81...	1a80bec27b...	1608	363052	34 minutes ago
d0f7fc745d7085c66723348073c5761d16e...	cc25cf5581...	465	363048	2 hours ago
dade45cf536ec7470a113e885801f2392b4...	f132080e92...	1353	363047	2 hours ago
1fb78c65c14e74833073f53038d9d3c3943...	ac759ffbef...	557	363046	2 hours ago
9a4b16eeb64bebf355c47655f210825ae87...	b881cd9b7c...	2516	363045	2 hours ago
22b9907c3f503496dc713271546d116420b...	22530943c7...	405	363044	3 hours ago
7f0d9d096dbf068dd3a12c6943fb02b9519...	4a9d7c60f3...	1919	363043	3 hours ago

https://techcrunch.com/2015/06/29/everledger/

National Security Agency (NSA)

Supply Chain Risk Management (SCRM)

19 October 2022

By **Dorian Pappas**

Chief Governance Operations

Agenda

- SCRM 101
  - What is SCRM?
  - What is the Threat
- SCRM Solutions
  - Tools
  - Tactics
  - Techniques

SCRM 101

What is information and communication technology (ICT)?

- The term ICT refers to technology used for data and information retrieval, storage, processing, transfer, security, and communications

- ICT and its components include microelectronics, computing systems, networks, software, and mobile devices that are used extensively in defense systems

Our Dependence on ICT

- DoD's military, business, and intelligence operations, including communications and command and control, rely heavily on commercial ICT
- Networked systems, devices, and platforms depend on ICT components to enable an ever-increasing number of capabilities that support DoD's missions

SCRM Background

- Commercial IT functionality has penetrated nearly every aspect of DoD Mission Critical Functionality
  - Dramatically varying quality, reliability and trustworthiness
- IT communications connects nearly all DoD IT functionality together and with the functionality of the rest of the world including our adversaries
- IT Supply Chain is global, no longer under US and is increasingly not trusted
  - Competitors and adversaries actively participating in the supplier chain

A Condition to Manage

- Because everything is connected today, one ICT component in a system or network can have an impact on one system or on multiple systems

- Therefore, risk must be considered for each ICT component before it is purchased or integrated into a system
  - The more critical the mission, the system, and the component, the more diligent we must be in conducting risk management

Risk

- Programmatic Risk is to cost/schedule/performance
- IA/Cyber risk is to confidentiality / integrity / availability (CIA)
- Operational Risk is to mission performance / accomplishment
- There are multiple and diverse risk owners in SCRM
  - Program Manager (PM)
  - Authorizing Official (AO)
  - Type Commander (TYCOM)
  - Combatant Commander
  - Commanding Officer (CO)
  - User/Operator

Supply Chain Risk Management (SCRM)

- SCRM traditionally refers to managing risks in the manufacturing and delivery supply chains
- SCRM is:
  - The process of identifying critical components and functions
  - Identifying supply chain threats, vulnerabilities, and risks
  - Determining likelihood (susceptibility) and the impact of those risks
  - Developing strategies in response
- ICT supply chain exploitation risks should be assessed at **each stage of the life cycle**

SCRM

- SCRM is:
  - All about securing the supply chain for ICT components from exploitation
  - A component of the Navy CYBERSAFE Initiative
  - Know as Trusted Systems and Networks (TSN) in DoD

- SCRM is **not** about "just in time" logistics
  - Though there is a logistics component based in contracting, supply, and delivery

Vulnerabilities of ICT components

- Software and hardware are increasingly complex and interdependent
- Manufacturers use components from unknown sources
- Software developers create software from code created by third-party and unknown sources
- All phases of supply chains are at risk for cyber attack or manipulation
- ICT components are susceptible to both intentional and unintentional threats

(open source)
executable
(open source)
program
(custom)
black
box
(proprietary)
GUI
Graphical
User Interface
(open source)
(proprietary)

Threats to the Supply Chain

- Supply chain risk considers the opportunity that an adversary may compromise a component or system along its supply chain
- An adversary may:
  - Sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system
  - So as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.
- Risks include information exfiltration, system disruption, and compromised system integrity
- Counterfeits can affect the mission, though their purpose is typically financial
- Malicious embedded code on hardware and software threatens system confidentiality, integrity, and availability (CIA)

Supply Chain Attacks

- U.S. dependence on foreign-sourced and ICT creates advantages and risks
  - Nearly every aspect of mission critical functionality relies on ICT
  - Networks connect ICT functionality with the rest of the world, including adversaries
  - ICT supply chain is no longer under U.S. control and increasingly not trusted
- Successful supply chain attacks require sophisticated adversaries
  - Employ full spectrum offensive capabilities (insiders, surreptitious entry, etc.)
  - Deep knowledge of latent vulnerabilities; use systems approach to identify targets
  - Access to front companies or “weak link” suppliers
  - Distinct from counterfeiting in motivation, utilize similar pathways
- High-value targets difficult to defend against determined Nation-State adversary

What Does the Supply Chain Attack Look Like?

Counterfeit Material Case

- **Owner and employee of Florida-based compan indicted in connection with sales of counterfei high tech devices destined to the U.S. military and other industries**
  - WASHINGTON - A 10-count indictment was unsealed in U.S. District Court for the District of Columbia charging Shannon L. Wren, 42, and Stephanie A. McCloskey, 38, with conspiracy, trafficking in counterfeit goods, and mail fraud. The indictment alleges that Wren, McCloskey and others imported counterfeit integrated circuits from China and Hong Kong and sold them to the U.S. Navy, defense contractors and others, marketing some of these products as" military-grade."
  - Stephanie McCloskey, former Administrative Manager of VisionTech, was sentenced on 25 October 2011 for her role in a conspiracy to distribute counterfeit integrated circuits. She was sentenced to 38 months incarceration, 3 years of supervised release, and asset forfeiture of $166,141.23, which represents the salaries she earned at VisionTech. A restitution order will follow, which could be as much as $578,062.23.

How Does Grey Market Attack Happen?

Received in developing country

Shipping from/to U.S.

Resold

Removed from boards and sorted

Refurbished and remarked

Repackaged

Hardware

“Breakthrough Silicon Scanning Discovers Backdoor in Military ”

Hardware

Common Development Practice:

During a two week evaluation of the Actel/Microsemi ProASIC3 (PA3) A3P250 silicon chip, an undocumented backdoor was discovered. Originally, the backdoor was thought to have been inserted by malicious actors during the manufacturing process in China. However, it was eventually confirmed that the **backdoor was a built-in debugging interface inserted by the developer**. This is a common development practice used for many chips, because it is too costly to make customized versions without the interface.

Risk:

The backdoor leaves systems vulnerable to Trojans, property theft, new backdoors, and reprogramming without the user’s knowledge. It also permits the possibility of a large scale Stuxnet-type attack. Since the backdoor is built into the hardware, rather than the firmware, simply issuing a patch will not fix it, and adding software level protection will be ineffective because the underlying hardware can be accessed to circumvent any software countermeasures. Instead, the user must accept the risk or all the hardware must be replaced, either of which could be extremely expensive.

Operational Impact:

The chip is a “COTS” product used in military products, but there is some dispute as to how widespread the chip is used.

- http://www.cl.cam.ac.uk/~sps32/sec_news.html
- http://www.techspot.com/news/48817-china-not-responsible-for-us-military-chip-backdoor.html

"Chinese Hackers Target Logistics and Shipping Firms With Poisoned Inventory Scanners"

Hardware

INCIDENT:

In a cyberattack campaign dubbed "ZombieZero," a popular brand of Chinese manufactured inventory scanners that contained preloaded malware stole sensitive information from shipping and logistics companies. According to TrapX Security, an unnamed Chinese manufacturer implanted malware into its handheld terminal scanners and in software updates available for download on its support website. They delivered the infected devices to customers where the scanners launched an automated attack that sent inventory information to botnets in China, and downloaded additional malware that infiltrated corporate servers and targeted sensitive financial and customer information

IMPACT:

The Chinese manufacturer sells handheld scanners to companies around the world. The exact amount of affected companies is unclear, but the manufacturer recently delivered infected scanners to 7 logistics and shipping companies and 1 large robotics manufacturing firm. One affected company was running 16 infected scanners that compromised 9 of its corporate servers. According to TrapX, the attackers successfully stole all financial and customer data, which can provide the attackers complete situational awareness and visibility into the company's operations.

MITIGATION:

The attack was discovered when a TrapX solution was deployed in the victim company's environment as part of a proof-of-concept. The solution immediately detected the attack, reported its anatomy and performed a complete automated forensic analysis.

http://www.darkreading.com/attacks-breaches/chinese-hackers-target-logistics-and-shipping-firms-with-poisoned-inventory-scanners/d/d-id/1297182
http://www.scmagazineuk.com/china-accused-of-global-zero-day-attack-on-shipping-firms/article/360406/
http://www.trapx.com/wp-content/uploads/2014/07/TrapX_ZOMBIE_Report_Final.pdf

Software

"Counterfeit Versions of Windows with Preinstalled Malware Sold in China"

Software

INCIDENT:

As part of an investigation into the sale of **counterfeit software**, Microsoft's digital crimes unit purchased brand new computers from different cities in China. The investigators discovered that of the computers were running forged versions of Windows and that 20% of the computers were pre-infected with viruses including the aggressive botnet virus Nitol.

IMPACT:

Microsoft detected nearly 4,000 Nitol infections, which likely represents only a subset of the number of infected computers. The Nitol virus is capable of performing DDOS attacks, spreading through removable and network devices, and acting as a backdoor by allowing an attacker to run additional malware.

Although Microsoft did not explicitly address this in its filing, experts say 3322.org has long been associated with malware used in highly targeted attacks aimed at stealing corporate and government secrets from U.S. and other Western firms.

MITIGATION:

Microsoft received permission from a United States court to take down the network of Nitol-infected computers and successfully sinkholed the virus' command and control domain, 3322.org, and any other subdomains linked to malware. The takedown was part of a legal campaign called Project MARS (Microsoft Active Response for Security), which takes the lead in combating digital crime by obtaining court orders to seize web domains and computers without notifying the owners of the property.

- http://www.bbc.co.uk/news/technology-19585433
- http://krebsonsecurity.com/2012/09/microsoft-disrupts-nitol-botnet-in-piracy-sweep/
- http://www.theguardian.com/technology/2012/sep/14/malware-installed-computers-factories-microsoft
- http://www.theregister.co.uk/2012/09/13/botnet_takedown/

" Home Depot Hack Linked to Compromised Supplier, Login Credentials, and Malware"

Software

INCIDENT:

In November 2014, Home Depot announced that criminals used a third-party vendor's username and password to enter the perimeter of its network in September 2014. From there, hackers acquired "elevated rights" that allowed them to navigate portions of Home Depot's network and to deploy custom-built malware on the retailer's self-checkout systems in the U.S. and Canada, compromising millions of customer data.

The malware used in the attack was designed to evade detection by anti-virus software, according to Home Depot. Although Home Depot has not identified the supplier linked to the breach, the revelation highlighted the importance of information security throughout the supply chain.

IMPACT:

Home Depot revealed that some 53 million customer e-mail addresses were stolen in the attack, in addition to the compromise of 56 million payment cards.

Those customers who have had their e-mail addresses compromised should be on heightened alert for phishing attacks, says Shirley Inscoe, analyst at Aite Group.

Home Depot estimates it will spend $62 million in fiscal 2014 for breach-related costs, including investigating the incident, providing credit monitoring services to its customers, increasing call center staffing, and paying legal and professional services. The company expects its insurance to cover about $26 million of that expense.

MITIGATION:

The company is notifying affected customers in the U.S. and Canada. Home Depot is warning customers to be on guard against phishing scams.

The company also has completed a major payment security project that provides enhanced encryption of payment data at the point of sale. The project required writing tens of thousands of lines of new software code and deploying nearly 85,000 new PIN pads to stores.
Rollout of enhanced encryption to 180 Canadian stores will be completed by early 2015. U.S. stores will have EMV in place by the end of this year.

All individuals affected by the breach will receive free identity theft protection services, including credit monitoring, for one year, Home Depot says.

- http://www.computerweekly.com/news/2240234281/Home-Depot-traces-credit-card-data-hack-to-supplier-compromise
- http://www.bankinfosecurity.com/target-home-depot-breaches-lessons-a-7544/op-1
- http://www.databreachtoday.com/home-depot-53-million-e-mails-stolen-a-7537?webSyncID=1612ec2c-3c8b-85ba-87a0-33b952bb87ca&sessionGUID=478e7423-6501-0104-a32a-86d53cbd0ace

Services

“Outsourcing New Software Poses Cyber Security Risk”

Services

INCIDENT:

A U.S. critical infrastructure software developer, named Bob, secretly outsourced his job of writing computer programs to software engineers at a consulting firm in China. In order for the third-party contractor to complete his work, he physically mailed his RSA token to China so that they could log-in under his credentials during the workday. This created the appearance that he was working an average 9 to 5 work day. The incident was discovered once a cybersecurity team was consulted to investigate an unknown intruder from Shenyang, China that was using Bob’s credentials to establish VPN connections to their network on a daily basis.

IMPACT:

During the outsourcing, the unnamed company Bob was working for was left vulnerable to having its computer network compromised, possibly in very severe ways that interfered with company operations or jeopardized the public. An attacker that is part of an organization as an outsource contractor – writing code, or building the chip – they are, in effect, insiders with all kinds of advantages that enable them to cause the company and its customers all kinds of problems.

MITIGATION:

A thorough security review must be conducted by organizations in order to identify issues that are being introduced into their networks. Businesses need to have capabilities in place to manage and monitor vendors. A 2008 survey titled “Offshoring Research Network” indicated that US software companies’ primary concerns of outsourcing consist of “data security” and “lack of intellectual property protection.”

- http://www.csmonitor.com/USA/2013/0130/Tale-of-Bob-Does-outsourcing-new-software-pose-cyber-security-risk-video
- http://www.computerworld.com/s/article/9235926/_Bob_outsources_tech_job_to_China_watches_cat_videos_at_work?taxonomyId=17&pageNumber=1
- http://www.bbc.co.uk/news/technology-21043693

SCRM Solutions

So, what can be done to address SCRM?

How is supply chain risk managed during the Operations and Sustainment phase of the life cycle?

- Maintain up-to-date security profiles
- Install software patches in a timely fashion
- Include identity and access management requirements
- Monitor and periodically (or continuously, if appropriate) re-evaluate changes in risk, suppliers, operational environment, and usage
- Track acquired ICT to ensure appropriate use

What can be done to manage supply chain risk during the Disposal phase?

- ICT items must be deactivated, disassembled, and removed from systems and system elements
- DoD policies dictate destruction or retention of hardware, software, and data to reduce the risk of revealing system information that might enable an attacker to penetrate a system; illegally distribute licensed software; or release sensitive system information to an unauthorized organization or individuals, enabling reverse engineering

Hardware Assurance

The level of confidence that a hardware component (ICT) is genuine and comes from a trusted source

NSA has tools available to ensure the authenticity of an ICT product

Products delivered by a trusted foundry

Software Assurance

The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner.

Ensure that the processes, procedures, and products used to produce and sustain the software conform to all requirements and standards specified to govern those processes, procedures, and products.

Ensure that the software-intensive systems we produce are more secure.

Numerous commercial tools and methods are available for SWA

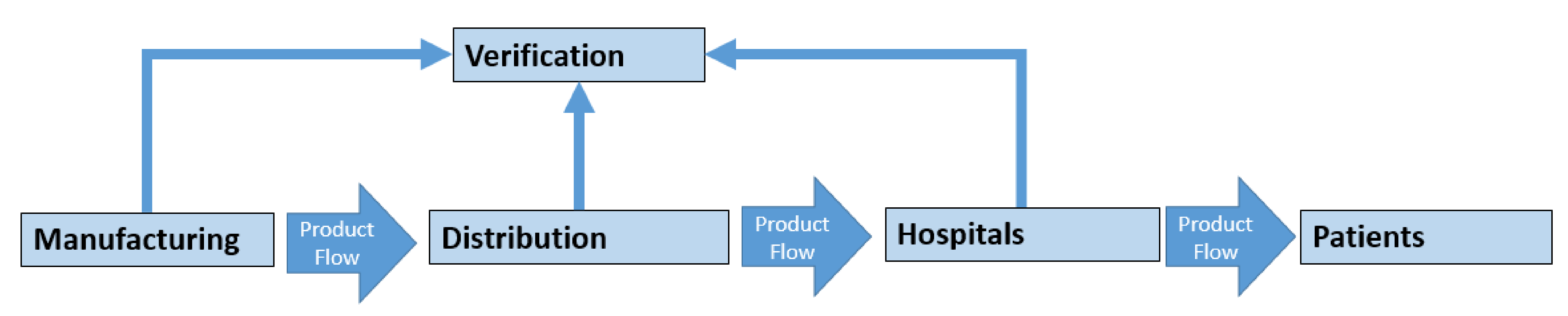
Business Intelligence (BI)

A BI is a detailed analysis of any entities involved in your supply chain

Typically, a BI includes an analysis of:

- Company Leadership
- Marking and Labeling
- Cyber Security
- Regional Stability
- Quality Assurance
- Financial Risk
- Physical Security
- Insider Threats
- Manufacturing and R&D
- Supply Chain Concerns

Tackling the problem of falsified medicines in the UK



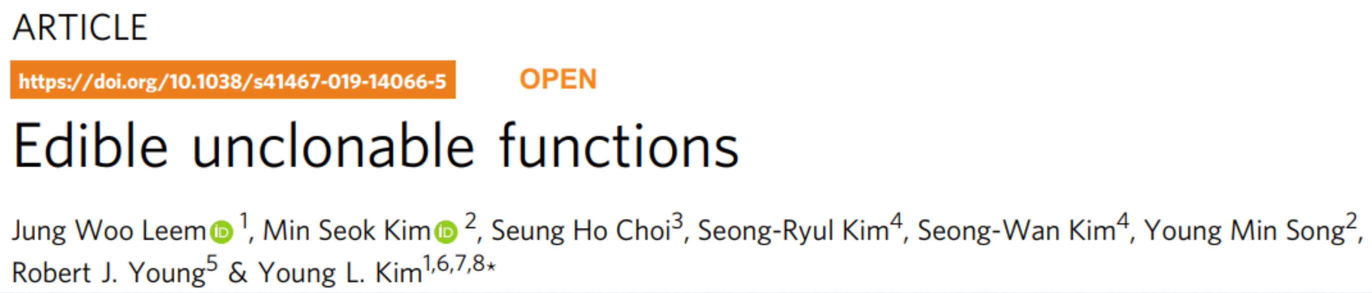
Proposed product flow in a pharmaceutical supply chain. The end-to-end verification prevents the entry of counterfeits and illegal products.

This could be an enabling technology 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

prescriber.co.uk

Futuristic pill technologies

nature COMMUNICATIONS



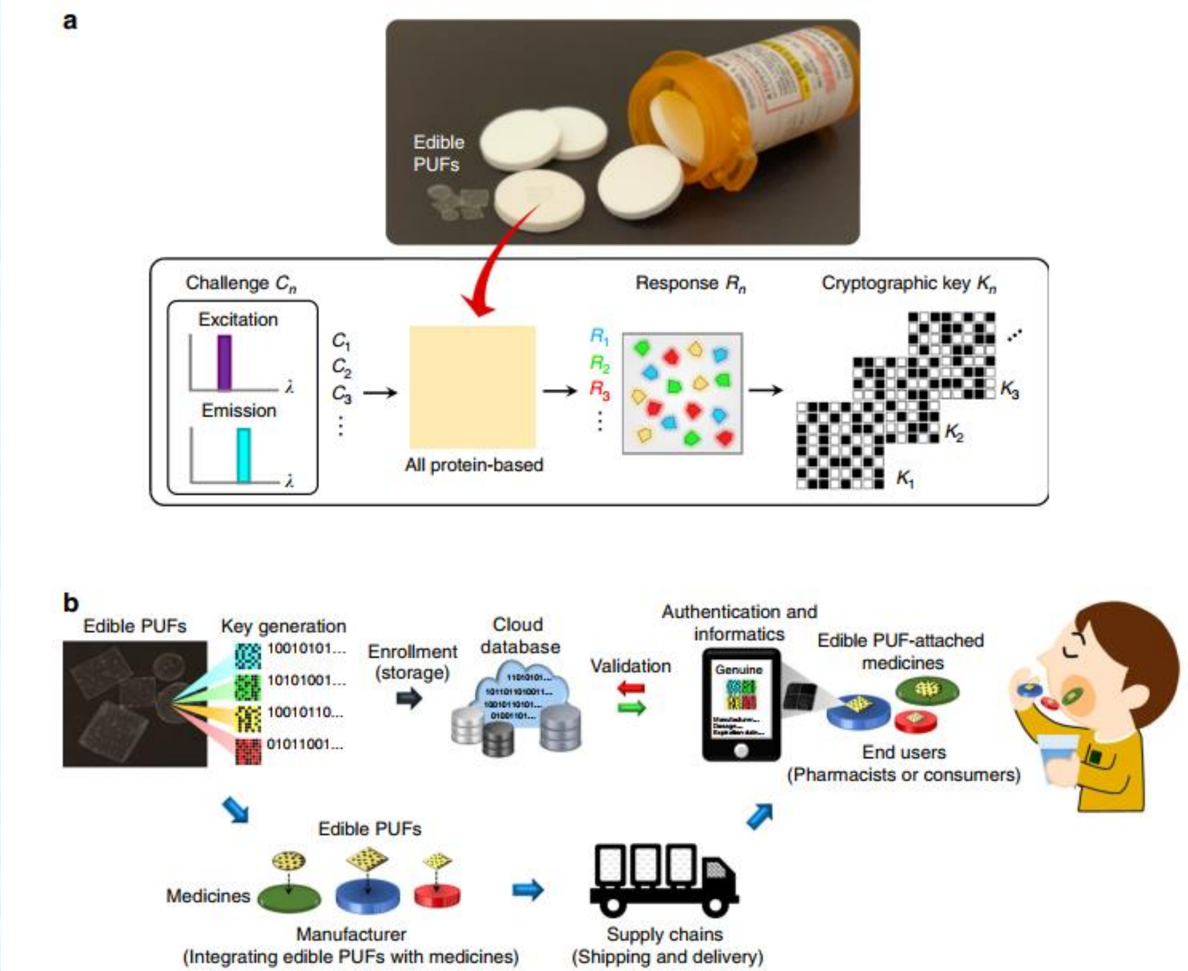
ARTICLE

https://doi.org/10.1038/s41467-019-14066-5 OPEN

Edible unclonable functions

Jung Woo Leem[1], Min Seok Kim[2], Seung Ho Choi[3], Seong-Ryul Kim[4], Seong-Wan Kim[4], Young Min Song[2], Robert J. Young[5] & Young L. Kim[1,6,7,8]*

2020



Use fluorescent proteins to create unique, edible ID on each pill

PUF: Physically unclonable function

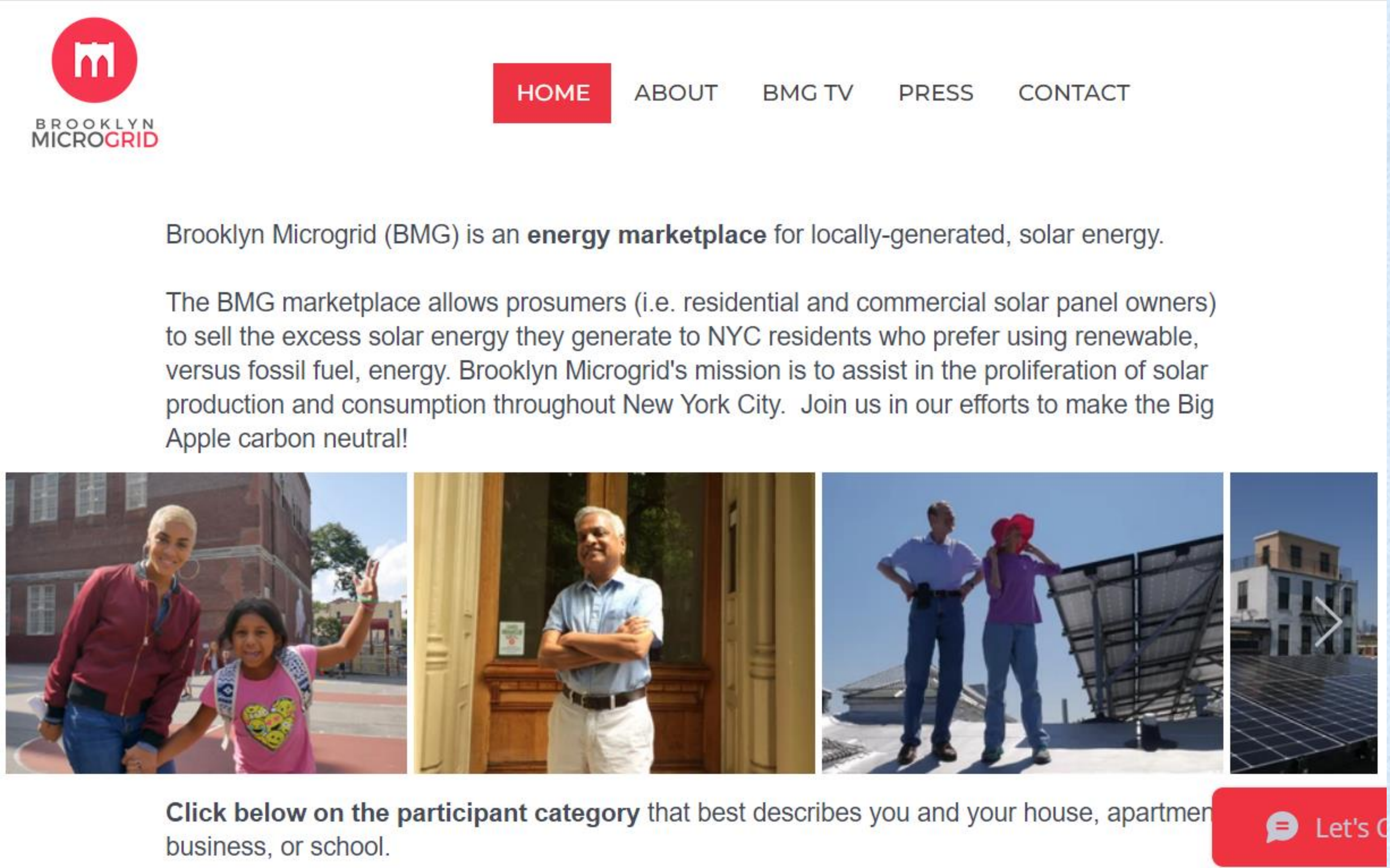
FOCUS APPLICATION #3: SMART ENERGY GRIDS

- There is considerable interest in green and renewable energy sources today, including bio-fuels, hydroelectric, solar, and wind energy.
- 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.
- 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

SMART ENERGY GRIDS

- 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.
- 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.
- Such peer-to-peer energy producing and trading systems are growing in the world, with installations in the USA, Germany and Australia.
- Hence, the availability of IoT-blockchain solutions can have significant socio-economic impact, and result in profits that stay within local communities.

https://www.brooklyn.energy/

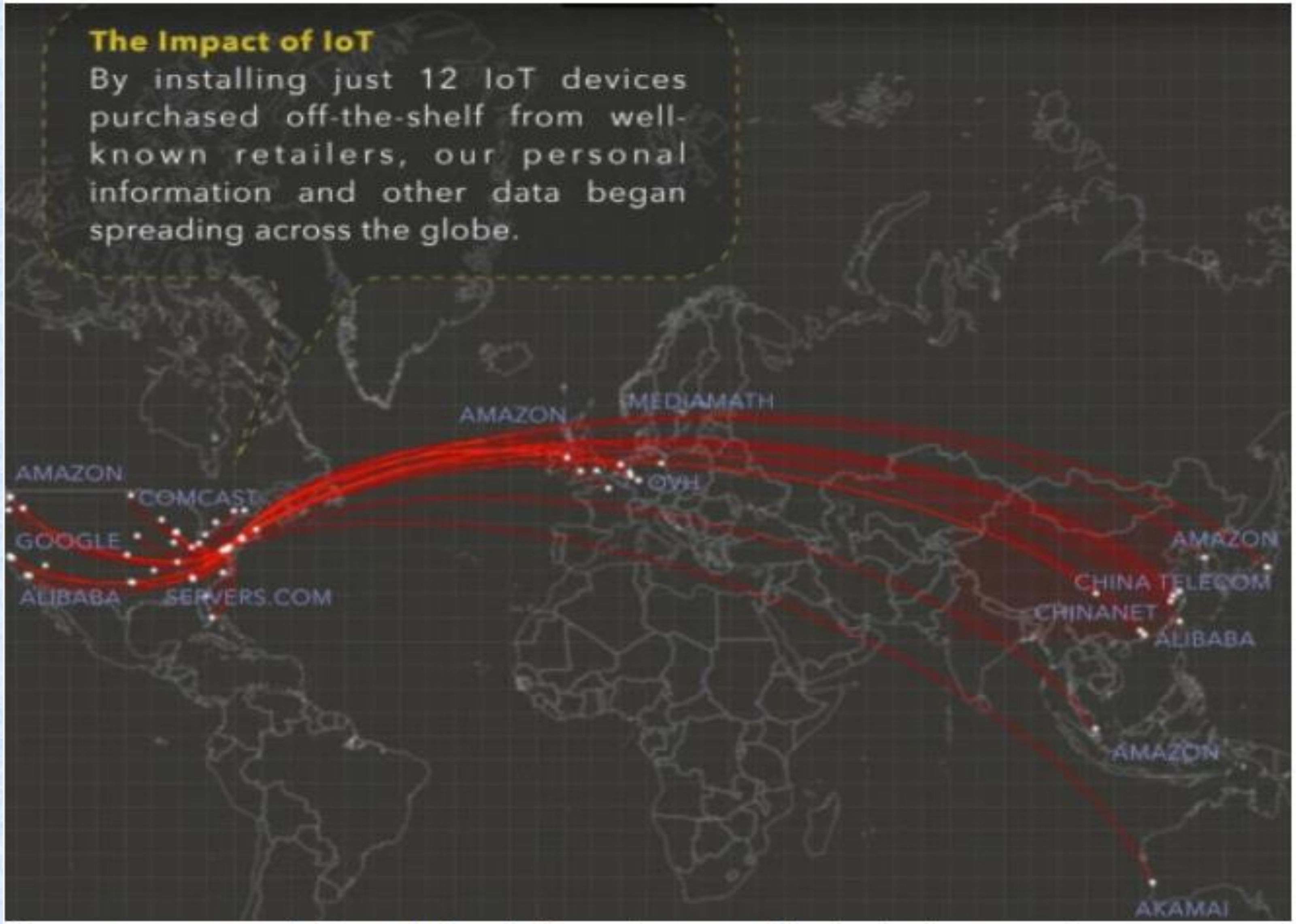


Brooklyn Microgrid (BMG) is an **energy marketplace** for locally-generated, solar energy.

The BMG marketplace allows prosumers (i.e. residential and commercial solar panel owners) to sell the excess solar energy they generate to NYC residents who prefer using renewable, versus fossil fuel, energy. Brooklyn Microgrid's mission is to assist in the proliferation of solar production and consumption throughout New York City. Join us in our efforts to make the Big Apple carbon neutral!

Click below on the participant category that best describes you and your house, apartmen business, or school.

Cybersecurity considerations



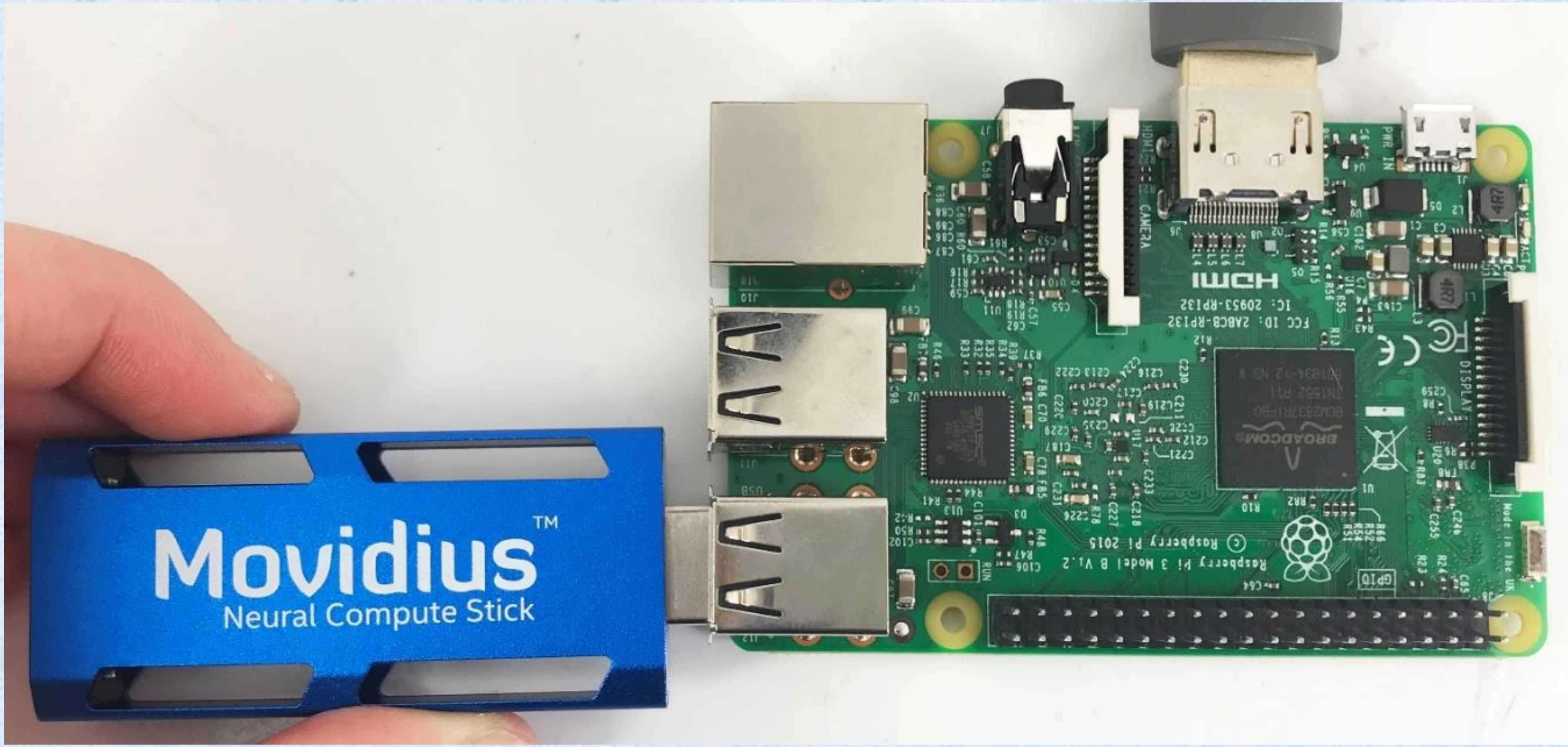
The Impact of IoT

By installing just 12 IoT devices purchased off-the-shelf from well-known retailers, our personal information and other data began spreading across the globe.

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

Image Credit: Pepper IoT

Computation and storage

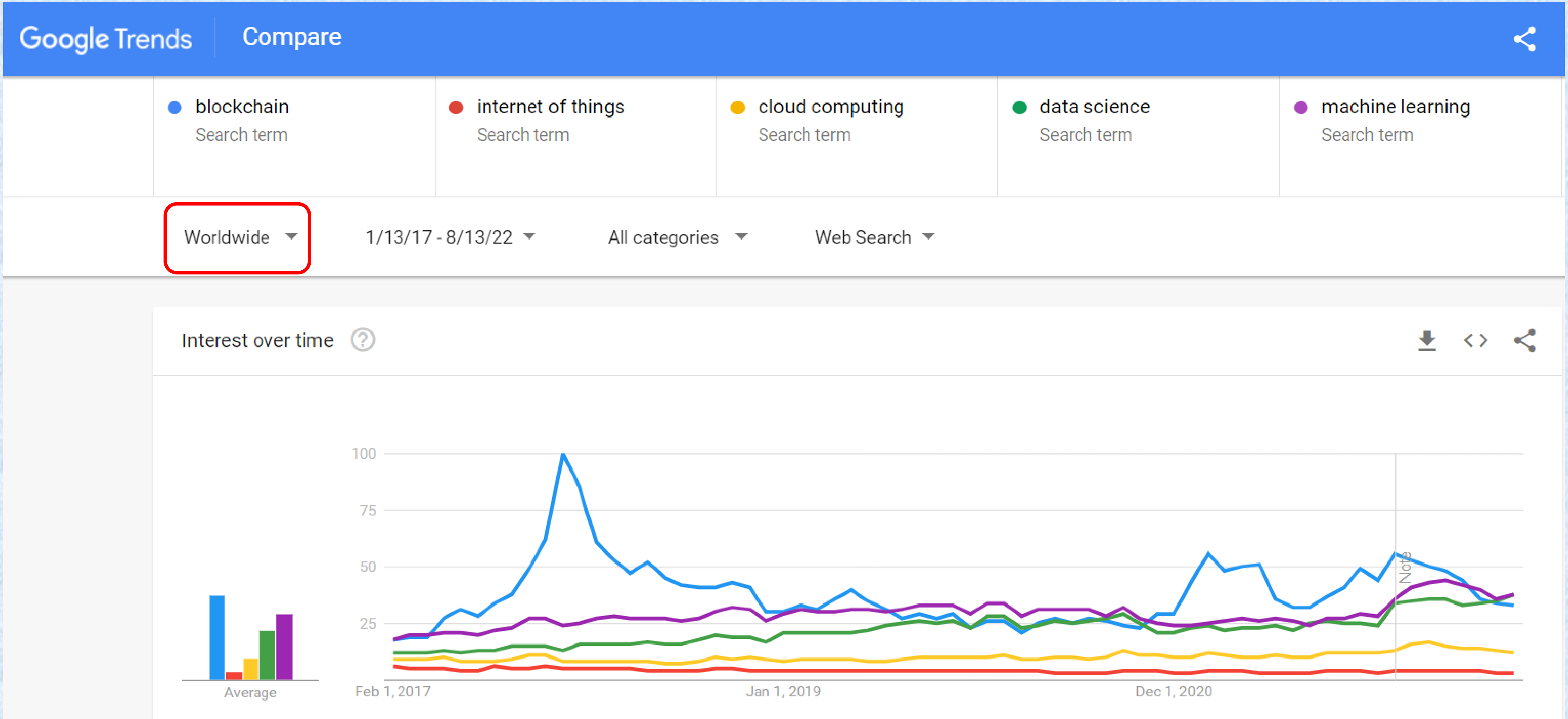


The Movidius neural compute stick is a low-power and small form factor device that can implement deep neural network algorithms for signal processing and image recognition. Here, a Movidius compute stick costing $75 it is shown attached to a USB port of a Raspberry Pi Model 3-B that costs $35.

Edge of network intelligence: Smart cities

- Edge-of-the-network intelligence is being utilized in the array-of-things project at the Argonne National Laboratory (Chicago)
- cameras at traffic intersections only count the number of pedestrians without storing pictures of individual pedestrians.

5-year analysis of trends in search terms



Google Trends Compare

● blockchain
Search term

● internet of things
Search term

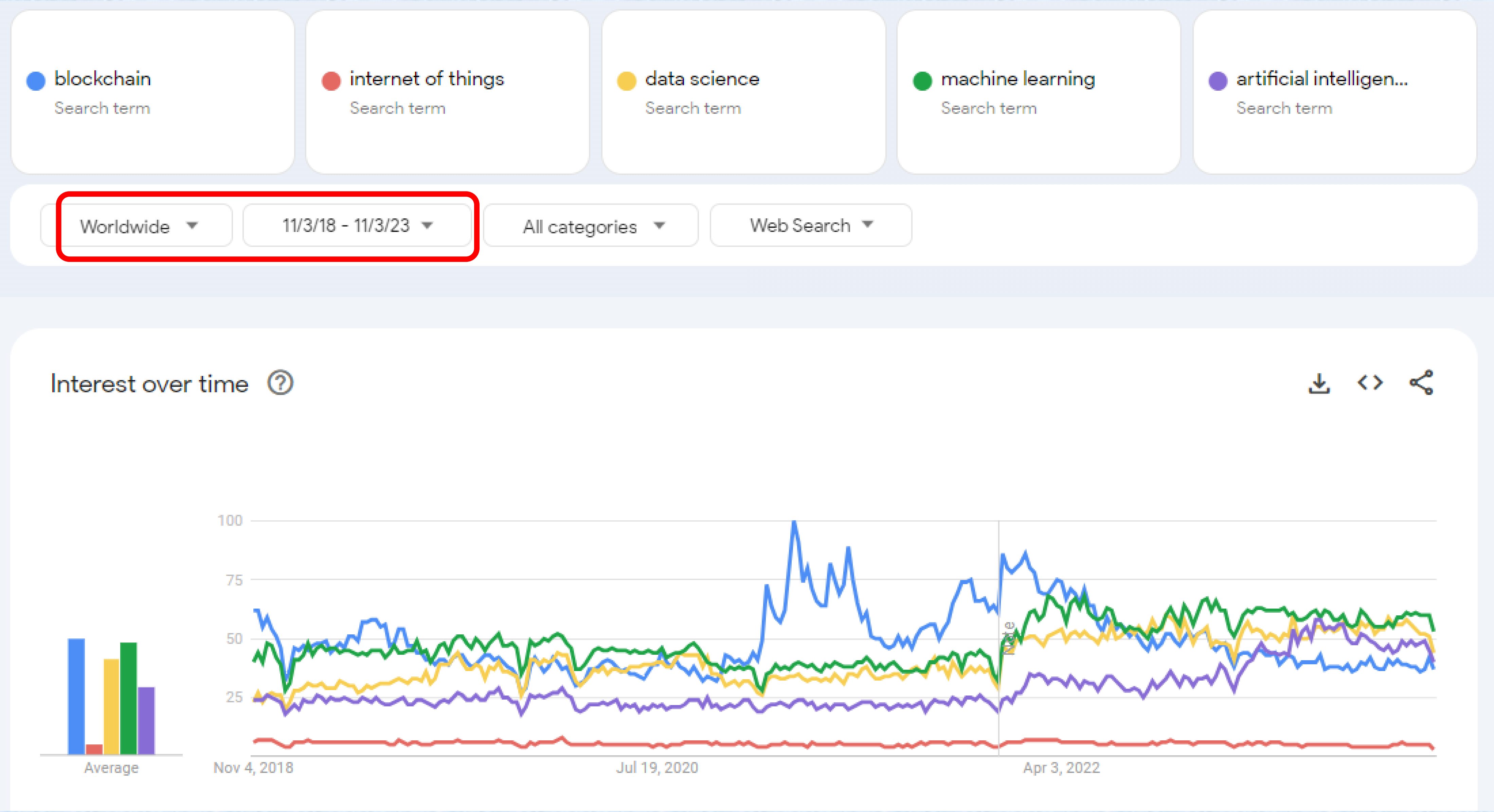
● cloud computing
Search term

● data science
Search term

● machine learning
Search term

Worldwide ▾ 1/13/17 - 8/13/22 ▾ All categories ▾ Web Search ▾

Interest over time



● blockchain
Search term

● internet of things
Search term

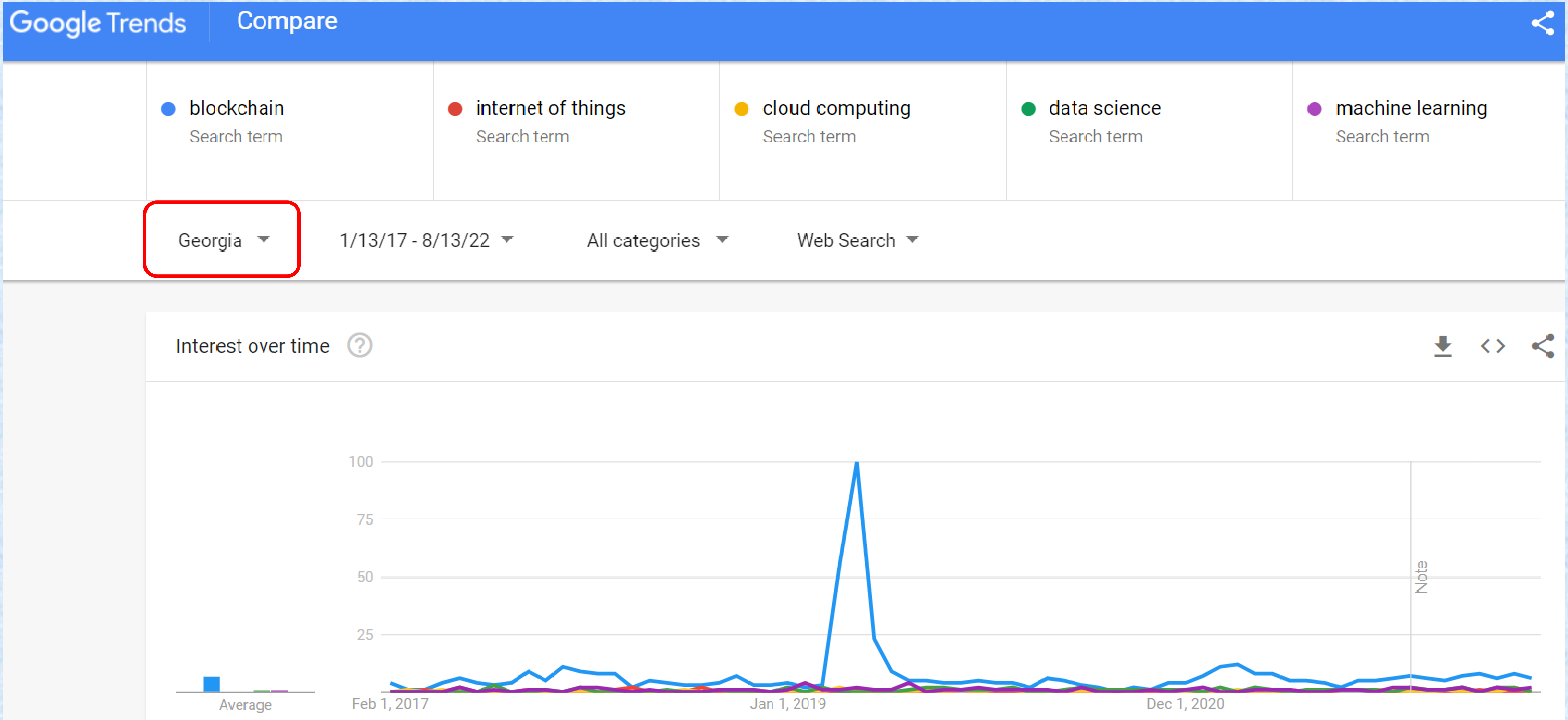
● data science
Search term

● machine learning
Search term

● artificial intelligen...
Search term

Worldwide ▾ | 11/3/18 - 11/3/23 ▾ | All categories ▾ | Web Search ▾

Interest over time



● blockchain
Search term

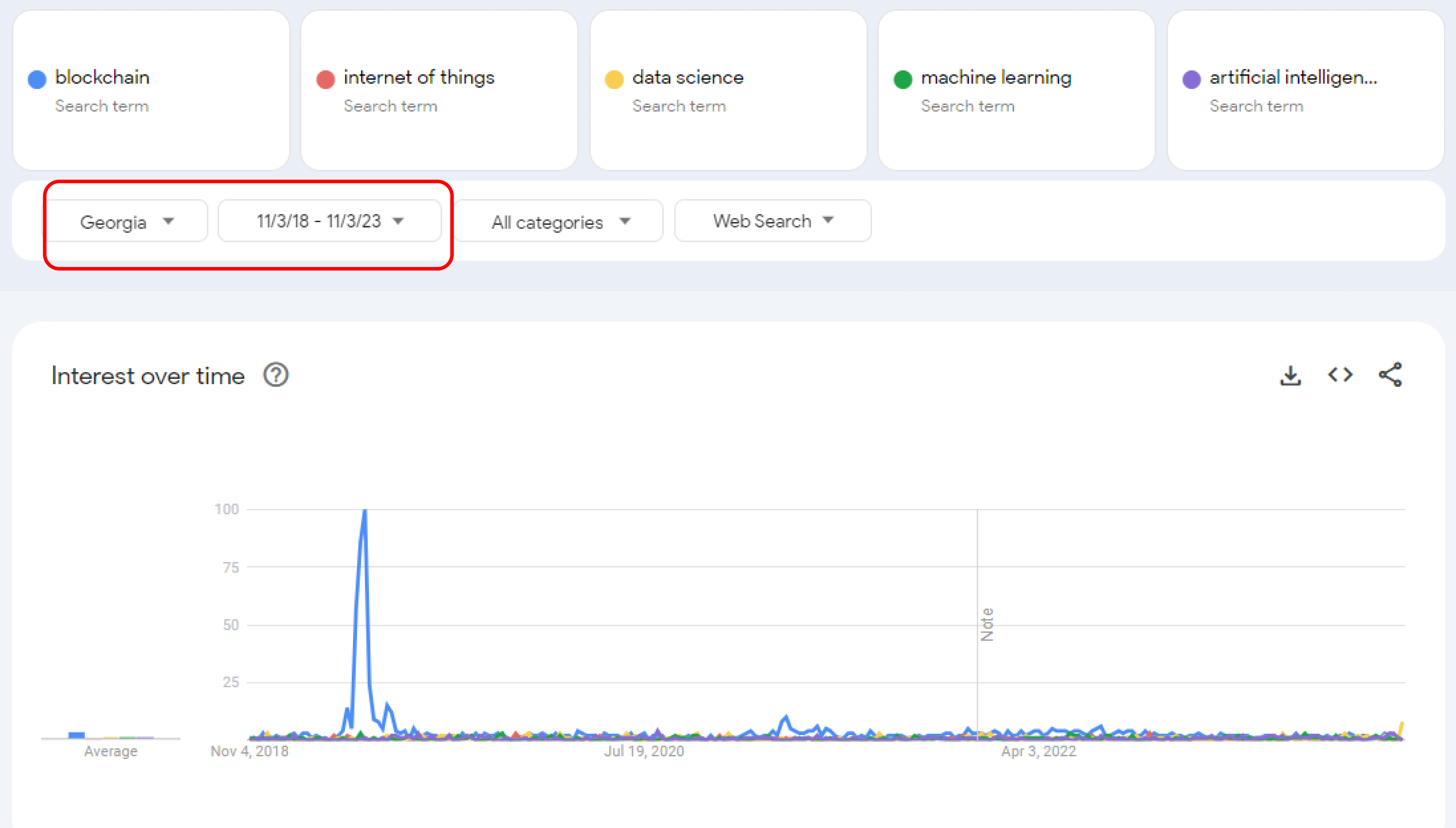
● internet of things
Search term

● cloud computing
Search term

● data science
Search term

● machine learning
Search term

Georgia ▼ 1/13/17 - 8/13/22 ▼ All categories ▼ Web Search ▼



● blockchain
Search term

● internet of things
Search term

● data science
Search term

● machine learning
Search term

● artificial intelligen...
Search term

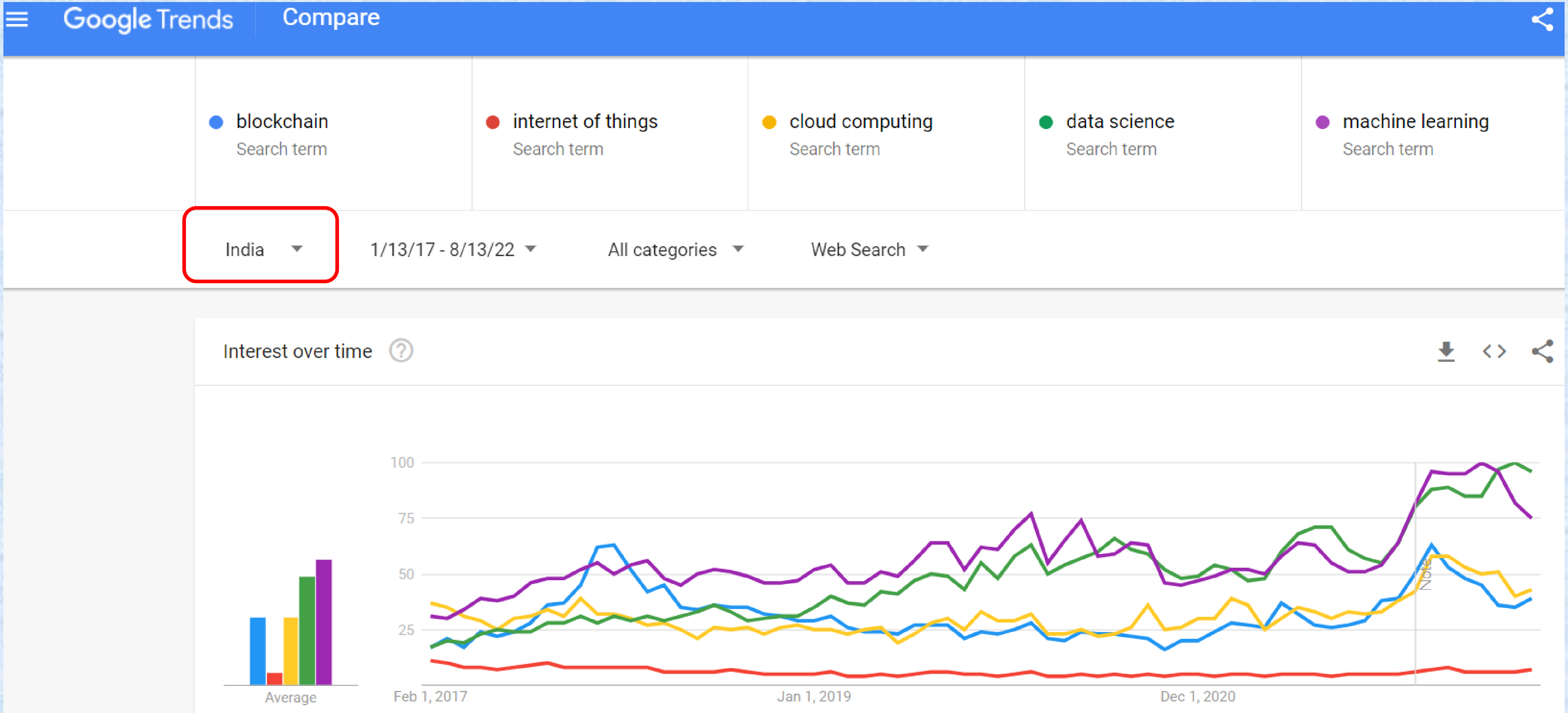
Georgia ▼

11/3/18 - 11/3/23 ▼

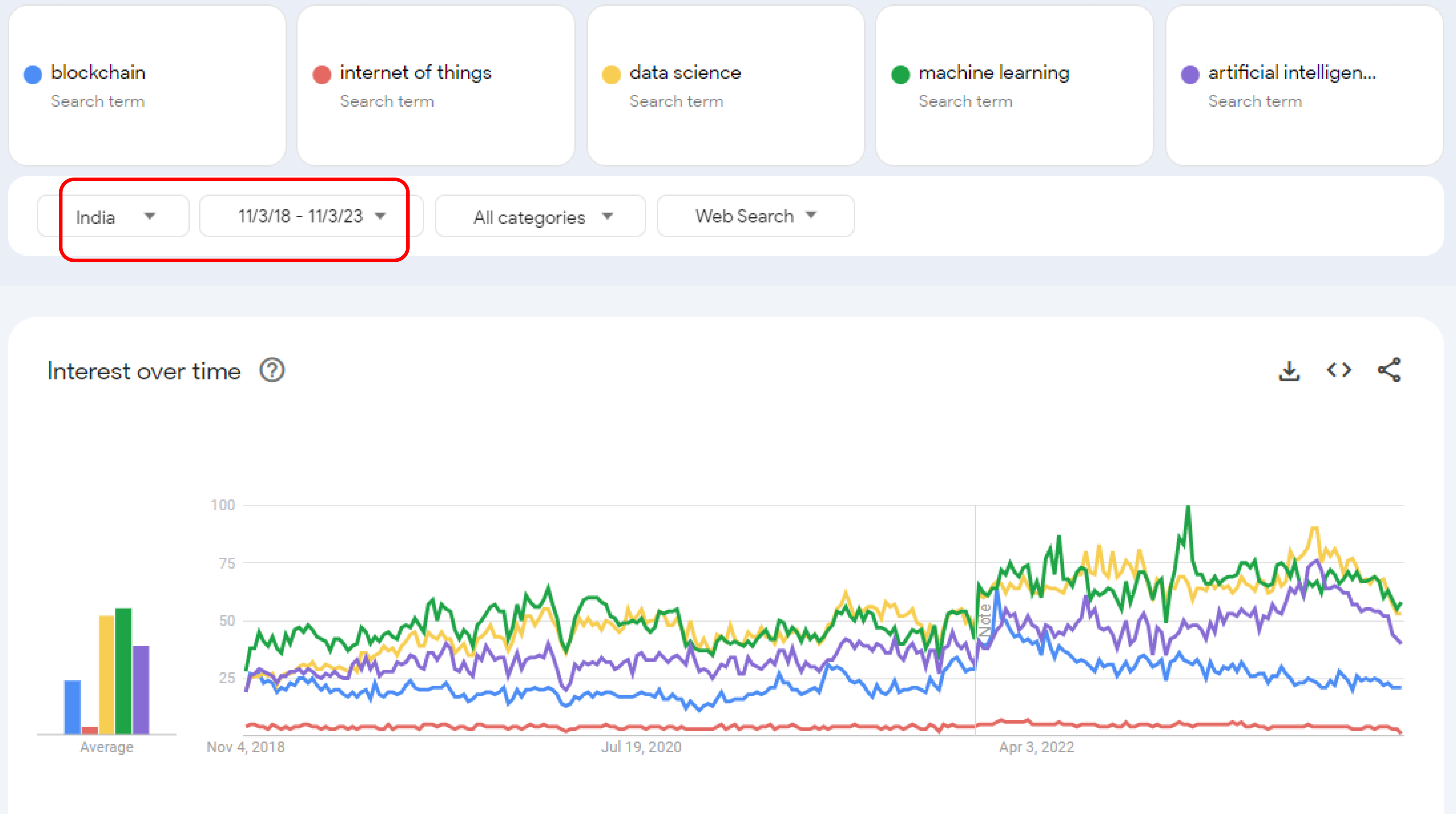
All categories ▼

Web Search ▼

Interest over time



High demand in India for skills in data science/machine learning. Many multi-national companies have huge operations in India



● blockchain
Search term

● internet of things
Search term

● data science
Search term

● machine learning
Search term

● artificial intelligen...
Search term

India ▼

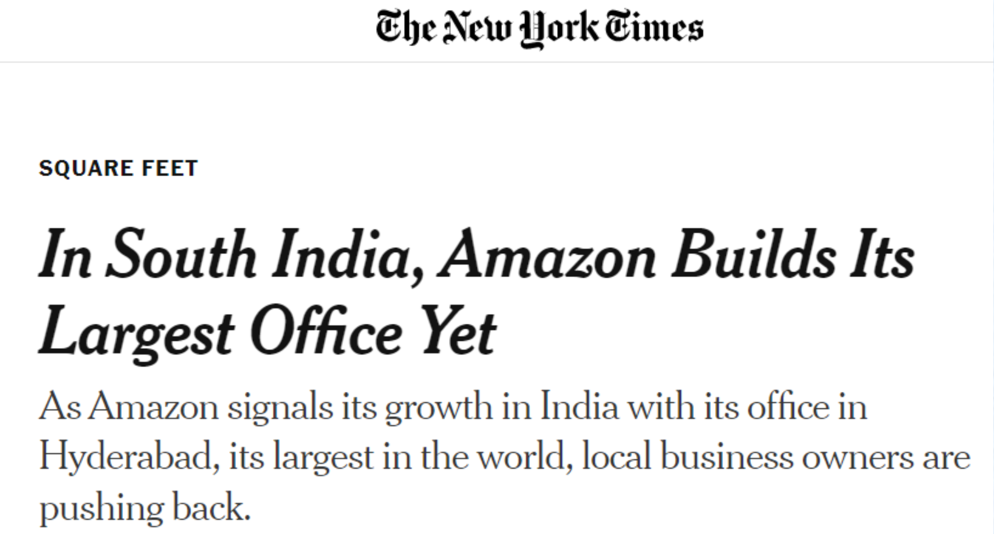
11/3/18 - 11/3/23 ▼

All categories ▼

Web Search ▼

Interest over time

Geopolitical factors can dictate what fields of technology are popular in a given region



The New York Times

SQUARE FEET

In South India, Amazon Builds Its Largest Office Yet

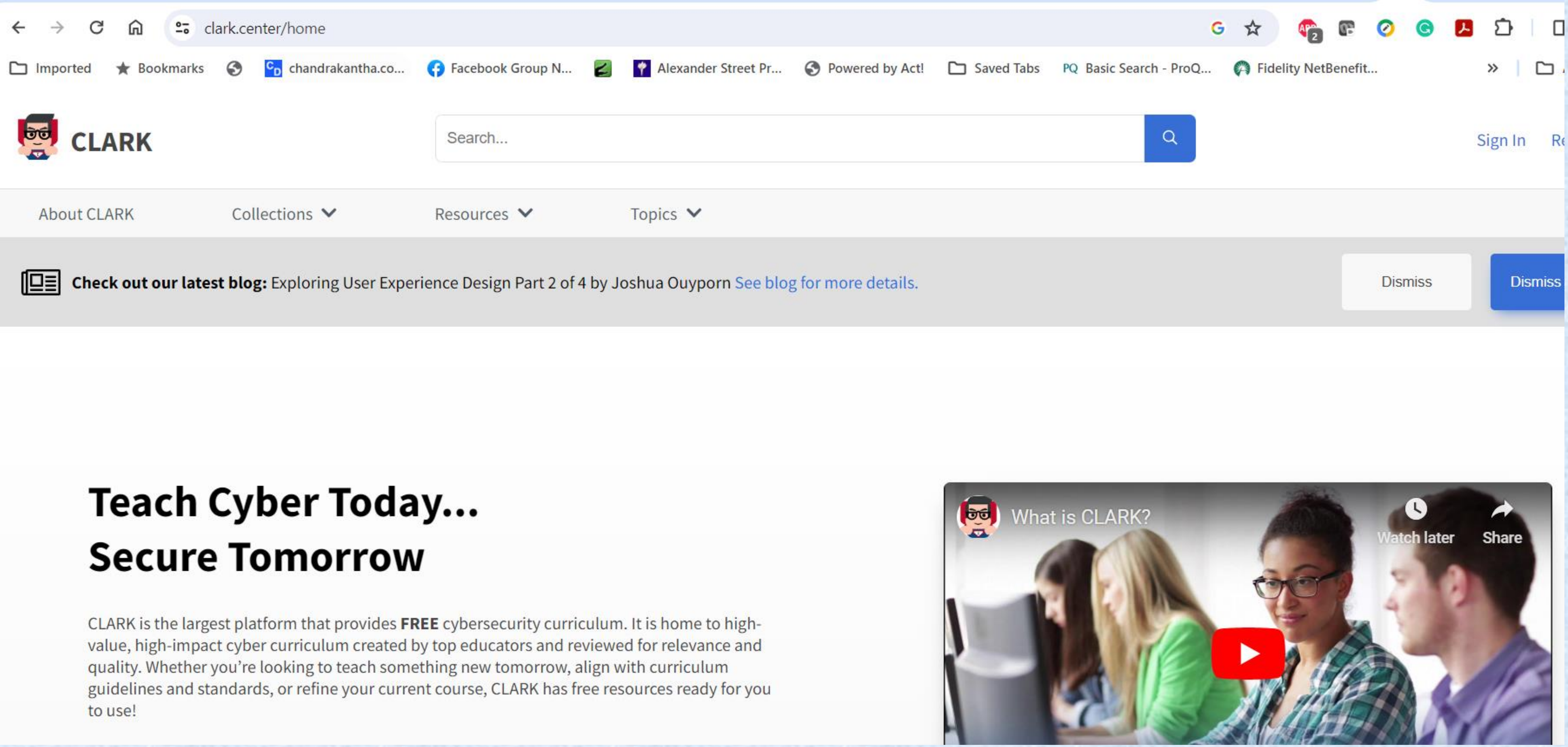
As Amazon signals its growth in India with its office in Hyderabad, its largest in the world, local business owners are pushing back.

Aug 2020

Amazon's new office in Hyderabad, India, is 1.8 million square feet. The office and its campus are equal to nearly 65 football fields. Amazon India Blog

clark.center: the largest repository of free cybersecurity related courseware, funded by the National Security Agency, USA

https://youtu.be/wXlZZjq0lDo

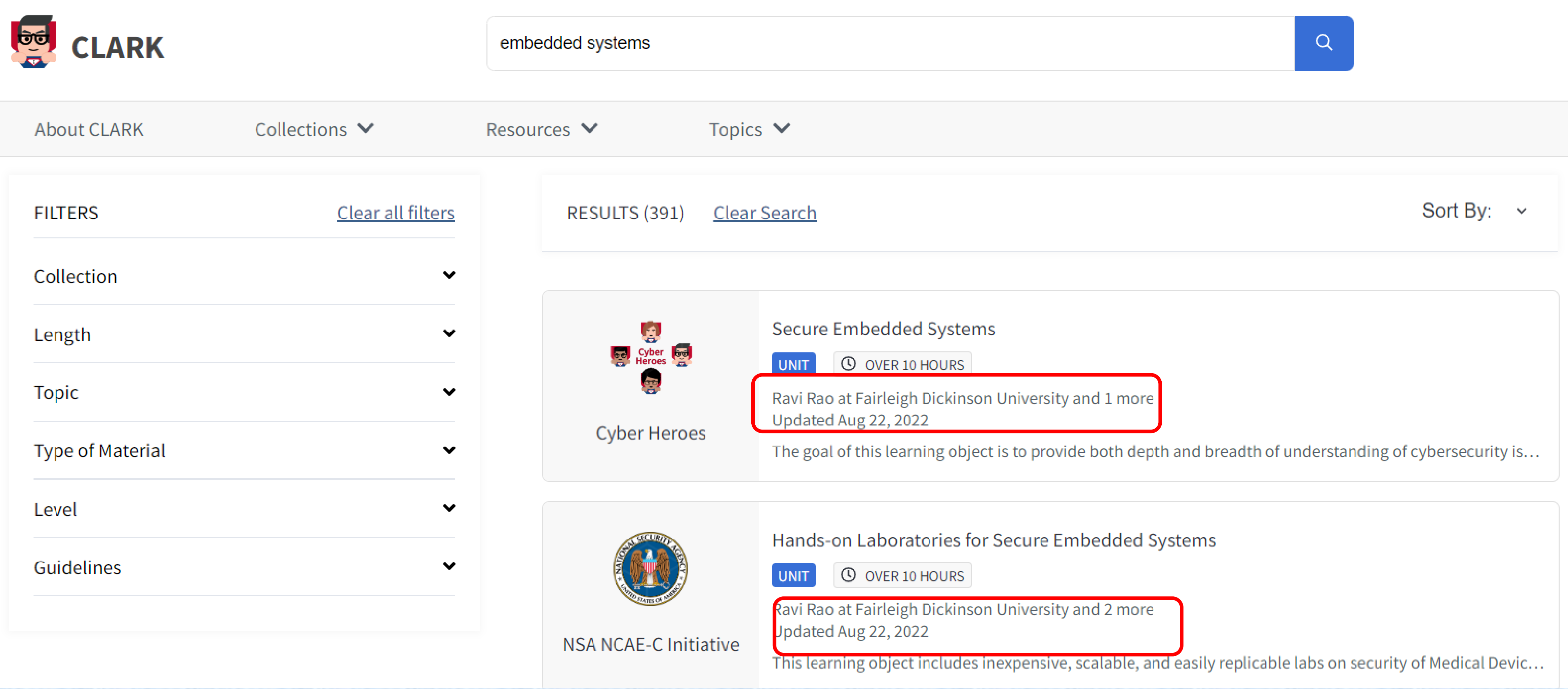


Check out our latest blog: Exploring User Experience Design Part 2 of 4 by Joshua Ouyporn See blog for more details.

Teach Cyber Today...
Secure Tomorrow

CLARK is the largest platform that provides **FREE** cybersecurity curriculum. It is home to high-value, high-impact cyber curriculum created by top educators and reviewed for relevance and quality. Whether you're looking to teach something new tomorrow, align with curriculum guidelines and standards, or refine your current course, CLARK has free resources ready for you to use!

Search for Embedded Systems at clark.center. You will see courses developed by Ravi Rao



FILTERS Clear all filters

Collection

Length

Topic

Type of Material

Level

Guidelines

RESULTS (391) Clear Search

Sort By:

Cyber Heroes

Secure Embedded Systems

UNIT OVER 10 HOURS

Ravi Rao at Fairleigh Dickinson University and 1 more
Updated Aug 22, 2022

The goal of this learning object is to provide both depth and breadth of understanding of cybersecurity is...

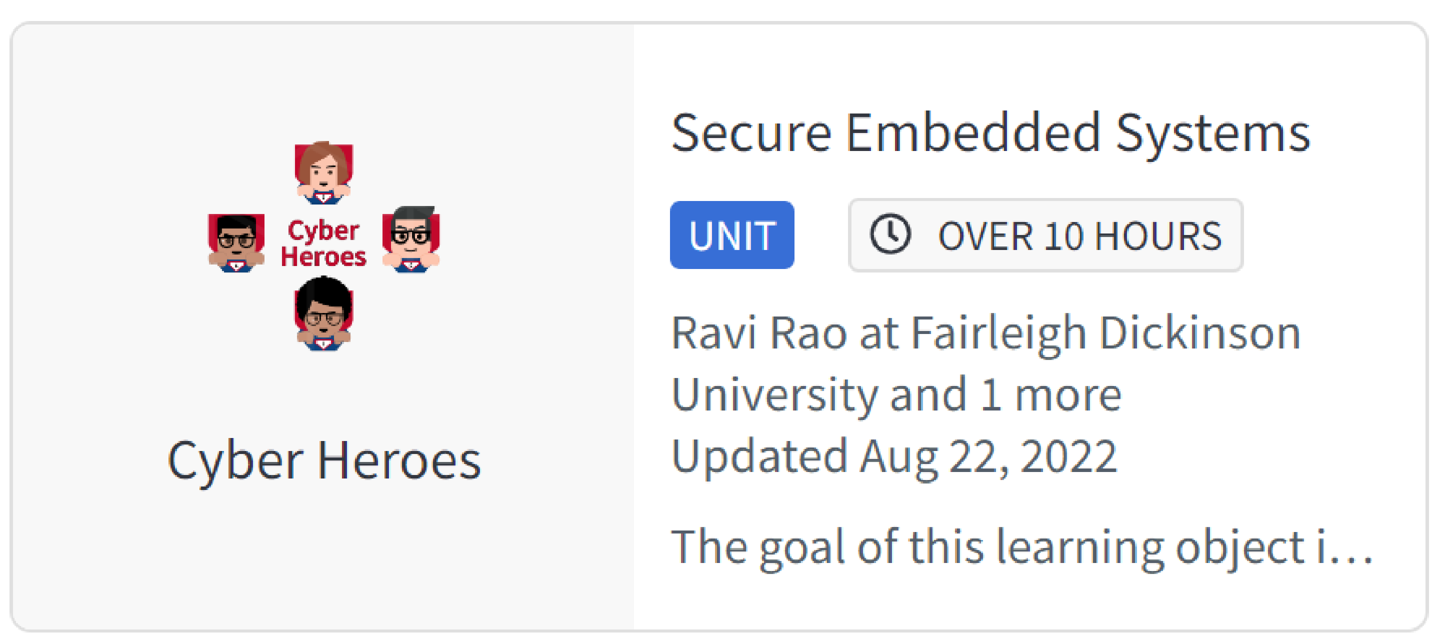
NSA NCAE-C Initiative

Hands-on Laboratories for Secure Embedded Systems

UNIT OVER 10 HOURS

Ravi Rao at Fairleigh Dickinson University and 2 more
Updated Aug 22, 2022

This learning object includes inexpensive, scalable, and easily replicable labs on security of Medical Devic...



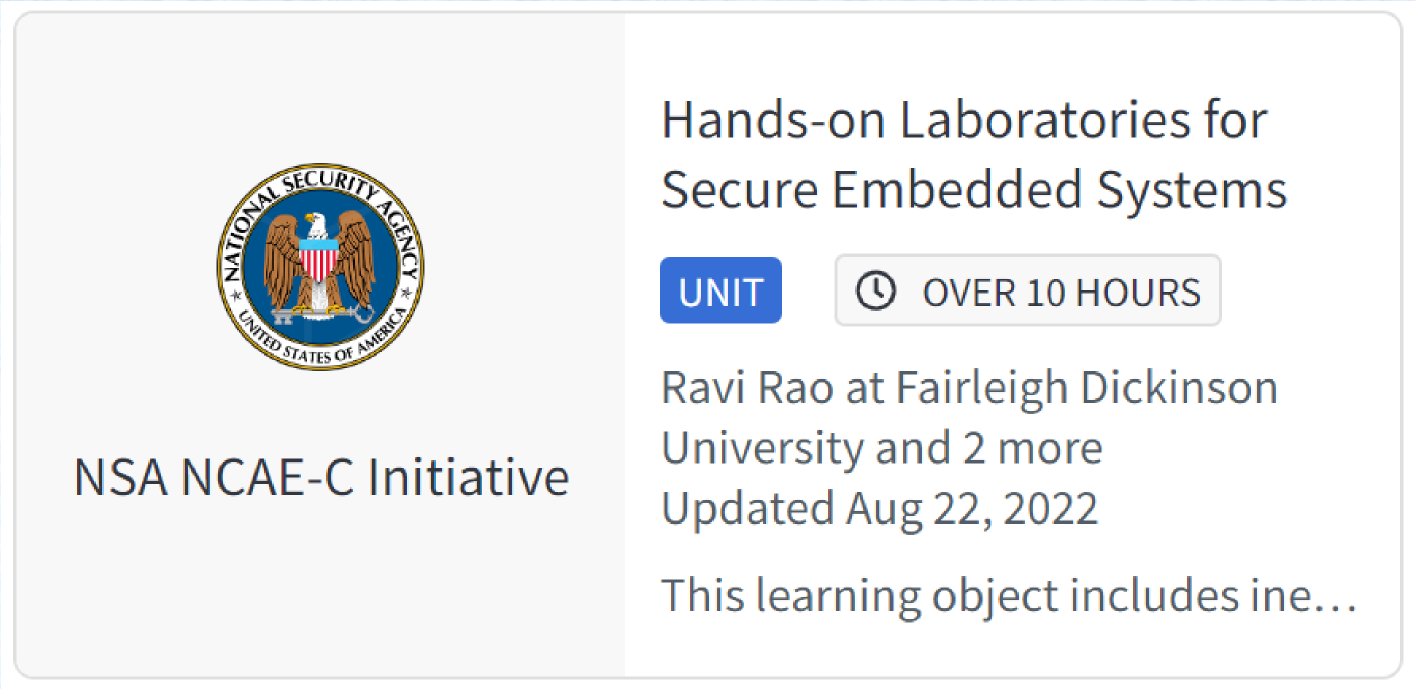
Cyber Heroes

Secure Embedded Systems

UNIT ◷ OVER 10 HOURS

Ravi Rao at Fairleigh Dickinson University and 1 more
Updated Aug 22, 2022

The goal of this learning object i…



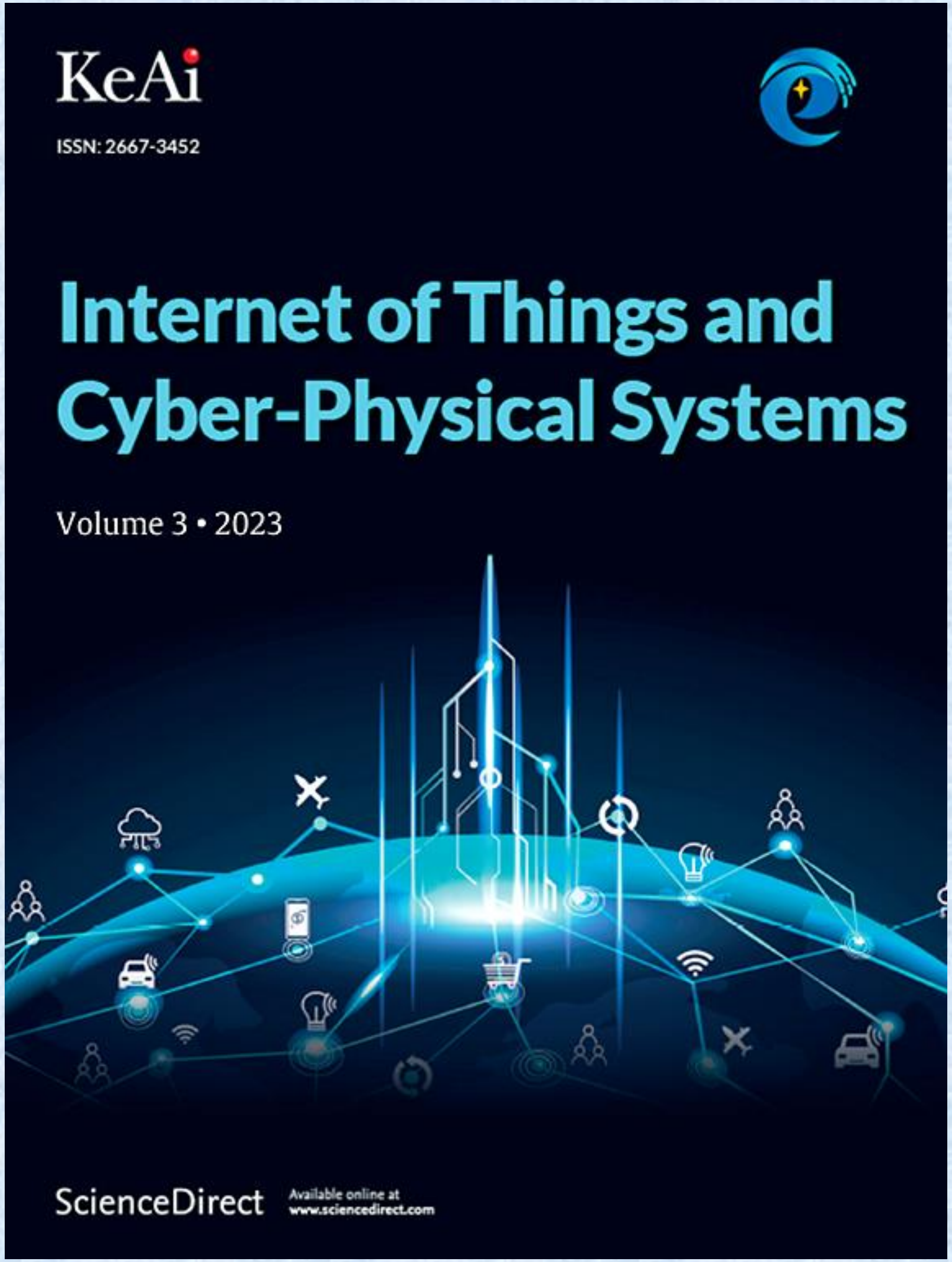
NSA NCAE-C Initiative

Hands-on Laboratories for Secure Embedded Systems

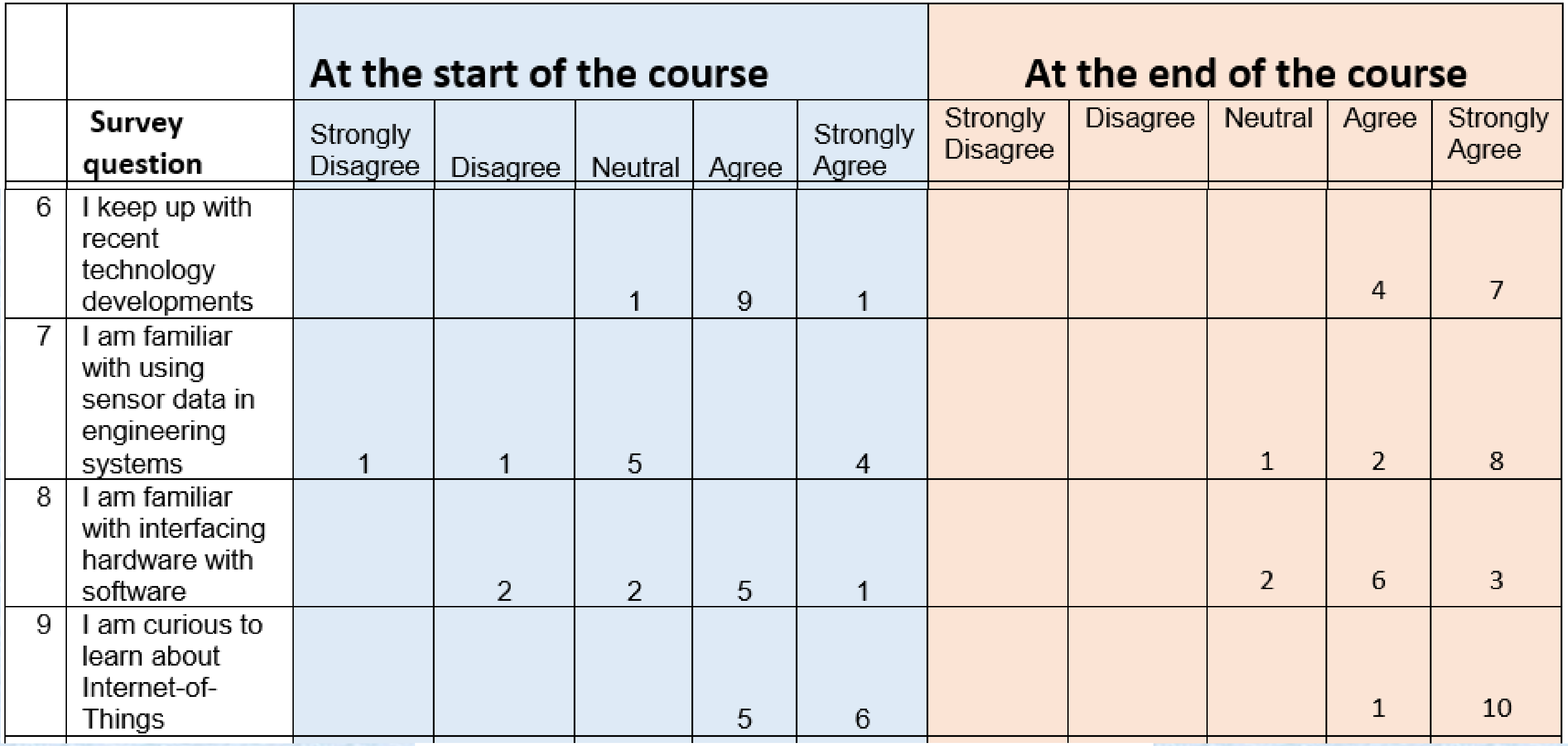
UNIT ◷ OVER 10 HOURS

Ravi Rao at Fairleigh Dickinson University and 2 more
Updated Aug 22, 2022

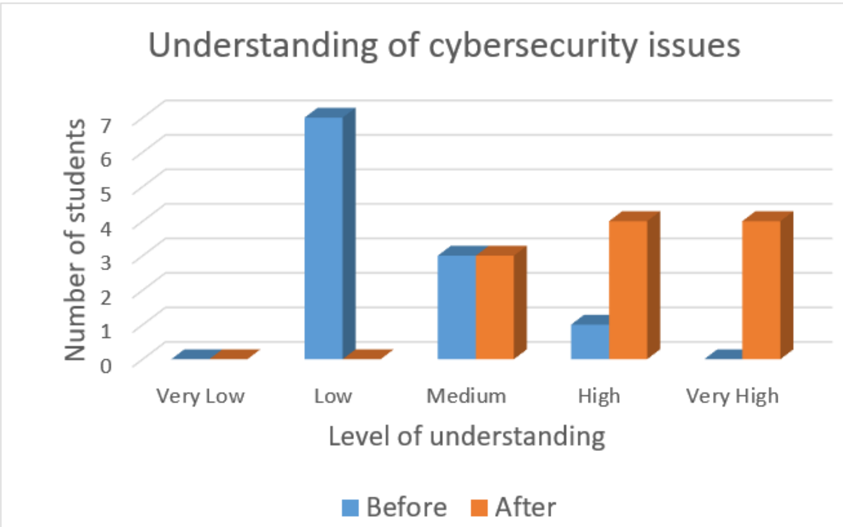
This learning object includes ine…


KeAi
ISSN: 2667-3452
Internet of Things and Cyber-Physical Systems
Volume 3 • 2023
ScienceDirect
Available online at www.sciencedirect.com

A.R. Rao, A. Elias-Medina, “Designing an internet-of-things laboratory to improve student understanding of secure IoT systems”, Journal of Internet of Things and Cyber-physical Systems, Elsevier Publishers, to appear in November 2023.



		At the start of the course					At the end of the course				
	Survey question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
6	I keep up with recent technology developments			1	9	1				4	7
7	I am familiar with using sensor data in engineering systems	1	1	5		4			1	2	8
8	I am familiar with interfacing hardware with software		2	2	5	1			2	6	3
9	I am curious to learn about Internet-of-Things				5	6				1	10



Conclusions

- Internet-of-things, blockchain, and cybersecurity are important areas for future research
- Adoption of blockchain is dependent on the ecosystem
  - Enough customers need to use it
  - Proper infrastructure needs to be built
  - Cost savings should be obvious to companies
- Futuristic scenarios can motivate students to enter these fields
- Hand-on labs based on the Raspberry-Pi ecosystem are an effective way to teach students to build embedded/IoT applications