THE ACADEMY OF SCIENCES OF TURKMENISTAN
OGUZ HAN ENGINEERING AND TECHNOLOGY
UNIVERSITY OF TURKMENISTAN

Cyberphysical Systems Faculty

Nano and Biomedical Electronics Department

Blockchain based Cybersecurity in IoT Systems and Smart Home

GRADUATION THESIS

Prepared by: Muhammetberdi Jepbarov

Supervised by: Ogulnazik Atajanova

Ashgabat – 2022

Contents

ABSTRACT

Blockchain is a distributed ledger technology that became popular as the foundational block of the Bitcoin cryptocurrency. Over the past few years it has seen a rapid growth, both in terms of research and commercial usage. Due to its decentralized nature and its inherent use of cryptography, Blockchain provides an elegant solution to the Byzantine Generals Problem and is thus a good candidate for use in areas that require a decentralized consensus among untrusted peers, eliminating the need for a central authority. Internet of Things is a technology paradigm where a multitude of small devices, including sensors, actuators and RFID tags, are interconnected via a common communications medium to enable a whole new range of tasks and applications. However, existing IoT installations are often vulnerable and prone to security and privacy concerns. This paper studies the use of Blockchain to strengthen the security of IoT networks through a resilient, decentralized mechanism for the connected home that enhances the network self-defense by safeguarding critical security-related data. This mechanism is developed as part of the Safe-Guarding Home IoT Environments with Personalized Real-time Risk Control (GHOST) project.

INTRODUCTION

The Internet of Things (IoT) connects people, places, and products, and in so doing, it offers opportunities for value creation and capture. Sophisticated chips, sensors, and actuators are embedded into physical items, each transmitting data to the IoT network. The analytics capabilities of the IoT use this data to convert insights into action, impacting business processes and leading to new ways of working. However, there are still a number of technical and security concerns that remain unaddressed.

Security is a major concern with IoT that has hindered its large-scale deployment. IoT devices often suffer with security vulnerabilities that make them an easy target for Distributed Denial of Service (DDoS) attacks. In DDoS attacks, multiple compromised computer systems bombard a target such as a central server with a huge volume of simultaneous data requests, thereby causing a denial of service for users of the targeted system. A number of DDoS attacks in recent years have caused disruption for organizations and individuals. Unsecured IoT devices provide an easy target for cyber-criminals to exploit the weak security protection to hack them into launching DDoS attacks.

Another issue with current IoT networks is that of scalability. As the number of devices connected through an IoT network grows, current centralized systems to authenticate, authorize and connect different nodes in a network will turn into a bottleneck. This would necessitate huge investments into servers that can handle the large amount of information exchange, and the entire network can go down if the server becomes unavailable.

According to Gartner's Forecast, Internet of Things endpoints are expected to grow at a compound annual growth rate of 32 per cent from 2016 through 2021, reaching an installed base of 25.1 billion units. With IoT devices expected to be such an integral part of our daily lives in the coming years, it is imperative that organizations invest in addressing the above security and scalability challenges.

CHAPTER I SHORT REVIEW OF A PROJECT

1.1 Introduction to IoT

The IoT (Internet of Things) technology has a wide practical use all over the world nowadays. Every electronic device has the control options, like wired, radio, Bluetooth, wi-fi network and internet. And the last one is the most interesting and it gives ability for a wide range of applications, starting from simple online smart sockets to complex systems that rely on each other and work together, as it is shown in Industry4.0 made robots, factory automation systems, drones, etc. The IoT has several different approaches and solutions, like Lora-WAN, MQTT, API.

Building an IoT Smart Home system from scratch gives the wide range of development abilities. The aim is to create a progressive programming interface, where anyone could integrate additional device and make use of the API to control it or get sensor data from it [13], [19].

The main components, that were dedicated to connect to a network, store and share states, send actions to control any electronic device, are:

- Microcomputer with a Linux operation system (example: RaspberryPi, OrangePi, or any other computer)

- ESP8266, NodeMCU for connecting circuits to Wi-Fi

- Arduino for controlling electronics.

1.2 Server-side application

The project is based on communication and data collection between devices and server. Basic schematic is an interconnected network with an access of IoT device and database server.

Programming languages used:
- C++
- Python

The aim of the server-side app:
- Creation a bridge between devices
- Saving the data and states
- Securing the actions and communication
- Creation the base API for client-side apps

- Synch between cloud data and local data

Server-side handles a database with a relation-constructed structured data, and webserver written on Python language, handling all data and working on all main operations of connection, requests handling, data saving, redirecting, securing, hashing of information between devices and client-side applications [12], [17].

API created and documented to easily create client-side applications, for any platforms as Android, iOS, or create web-client on JavaScript. At the same time, webserver API is built for expanding the quantity and organizing of IoT devices. Each device written, has its own secure key, and "device type" property makes selection of usage type of this device and it's working technique [13], [16].

The interface of handling requests and storing the database of all devices and sensors can be written in any programming language for backend development.

Examples of languages and frameworks:

- JavaScript. Frameworks: Express, Next
- Python. Frameworks: Flask, Django, FastApi
- Go. Frameworks: Gin, Gorilla
- C#. ASP
- PHP. Laravel
- Ruby.
- Rust.
- And many others.

Using relational database will be very helpful for further development, and surely it will contain a one to many and many to many relationship templates.

Authentication layer is covered by User table. API should use one of the standards of Authentication for client-side security.

Device table will store each of our ESP8266 modules, this table contain a detailed info of a controller and it's IP address in a network. When connected, a RaspberryPi acts like the same IoT device in whole system, sharing and transferring info across the web to our modules [17], [20],

The state of our electronic devices is stored in Device and Pin tables. The Pin table will be connected with device using one-to-many relationship. A lot more tables could be added for expanding features and security of the IoT application.

Afterwards the URL routes should be created. These routes will handle request a work on it, by storing data or running an action dedicated to that data.

The sample Device controlling route will look like following:

"/device/" methods: GET, POST

When "Get" request is done, the API will retrieve information about state of device, and "Post" will be used to update info on server and database, and send action to an IoT device.

Retrieving and sending data is done, but how about ESP8266 controllers?

Arduino Library of ESP8266 has a wide range of libraries so we will use it. Each microprocessor will store a data and share it with a main cloud, so it could be programmed as a mini-server for itself and for devices around. Creating a route "/control/" will handle the states that were send from API server and control our device.

For a lamp or wall socket devices, it requires to send "true" and "false" (1 & 0) values to it. For more complex devices, like a temperature controlling systems (coolers, heaters) it requires to send structured arguments in URL or in body of the request.

Now, when the API set and device and client-side application connected to it, changing state will update the microcontroller and therefore will manage the electric circuit.

In the whole overview, separate electronic devices, that running ESP8266 or any other controller, are connected to main hub, that handles local database and system of a Smart Home. Furthermore, this hub can be connected to a remote cloud server, to update its own states through internet connection.

How about security?

In every data exchanging and remote controlling systems, it is required to have a security layer.

As for client-side application, the security is done by "Basic" and "Bearer" authentication, as known as JWT tokens, with added SSL encryption of cloud server [18], [20].

What about electronic devices, they have secret keys that are registered on system using QR codes that are unique and attached to device. They also validate time, connection with Home system. Therefore, another more complex level of security could be added. Smart home systems and IoT is still adopting, more complex tasks and projects are developing on it, with added Artificial Intelligence and Blockchain.

1.3 Smart Home using IoT

Smart technologies are becoming popular nowadays and the automation has come to use in home appliances. Sensors and controllers being used to make life easier and solve problems and do routine tasks. The system that works in this version of Smart Home uses the ESP8266 microcontrollers and RaspberryPi as a server and database computer.

A smart home is a modern building management system that allows you to optimize and manage all the events that take place inside the building.
The Smart Home system manages and connects electronic devices. Coordinates their work. It also helps to make the most of their opportunities. Even when we are away from home, we can remotely control home appliances over the Internet with the help of a computer or cell phone. It is possible to monitor the condition of the house, the amount of water used in the house or the amount of electricity used.

In emergencies, for example, the Smart House not only warns us about water and gas leaks, but also interrupts the flow of electricity, gas or water to the home [13], [22].

The main features of the Smart Home system are:

- Turn on / off lights with the help of a motion sensor;
- Show homeowners "as if" at home (periodically / accidentally turn on / off lights in different rooms);
- Various design and remote control of interior lighting;
- Remote control of the lighting system / lights with the help of a smartphone or tablet;
- Automatic control of natural lighting (curtains, automatic opening / closing of curtains according to room lighting)
- Changing the lighting mode in the room (morning, afternoon, evening, night, reading, cinema (switching off the lights with the TV or projector turned on, closing the curtains and blinds));

- Automatic opening / closing of doors / windows (by phone, fingerprint);
- Receive a warning that all doors / windows are closed / open (sms, mms, call, beep);
- Closing windows (wind / rain) according to the weather;
- Receive alerts when the security system is turned on or off (sms, mms, call, beep);
- Take pictures or videos from the cameras when a signal arrives from the motion sensor, intercom, and turn on the lights around the corresponding sensor;
- Internet video surveillance (indoor equipment, events);
- Home water and gas leaks, smoke emissions, electrical wiring warnings (sms, mms, call, sound signal);
- Get information on the amount of electricity, gas, water consumed in the house;
- Remote shutdown of incoming electricity, gas, water.

Lamp. Keep the temperature and humidity in the rooms to a certain extent;

Maximum energy saving mode when homeowners are not at home;

Automatic on / off fans and air vents (remote control, automatic depending on the concentration of carbon dioxide in the house);

Automatic activation and deactivation of the irrigator after a certain period of time depending on the humidity level of the fireplace (lawn).

- Controlling TVs, projectors, loudspeakers in different rooms with the help of smartphones (on / off / volume up);

Automatic switching off of the lights if there is no movement for some time after the lights in the kitchen are turned on;

IR Remote control of all electrical appliances in the kitchen;

Automatic operation of the ventilation device when the electric or gas stove starts operating;

Remote control of water heater operation (e.g. in energy-saving mode).

Nearly every aspect of life where technology has entered the domestic space (lightbulbs, dishwashers and so on) has seen the introduction of a smart home alternative:

Smart TVs connect to the internet to access content through applications, such as on-demand video and music. Some smart TVs also include voice or gesture recognition.

In addition to being able to be controlled remotely and customized, smart lighting systems, such as Hue from Philips Lighting Holding B.V., can detect when

occupants are in the room and adjust lighting as needed. Smart lightbulbs can also regulate themselves based on daylight availability.

Smart thermostats, such as Nest from Nest Labs Inc., come with integrated Wi-Fi, allowing users to schedule, monitor and remotely control home temperatures. These devices also learn homeowners' behaviors and automatically modify settings to provide residents with maximum comfort and efficiency. Smart thermostats can also report energy use and remind users to change filters, among other things.

Using smart locks and garage-door openers, users can grant or deny access to visitors. Smart locks can also detect when residents are near and unlock the doors for them.

With smart security cameras, residents can monitor their homes when they are away or on vacation. Smart motion sensors are also able to identify the difference between residents, visitors, pets and burglars, and can notify authorities if suspicious behavior is detected.

Pet care can be automated with connected feeders. Houseplants and lawns can be watered by way of connected timers.

Kitchen appliances of all sorts are available, including smart coffee makers that can brew a fresh cup automatically at a programmed time; smart refrigerators that keep track of expiration dates, make shopping lists or even create recipes based on ingredients currently on hand; slower cookers and toasters; and, in the laundry room, washing machines and dryers.

Household system monitors may, for example, sense an electric surge and turn off appliances or sense water failures or freezing pipes and turn off the water so the basement doesn't flood, for example.

1.3.1 Independent system

The first task was to create an independent or weakly depended system. Devices in the Smart Home are already built separately as the modules that people can connect or disconnect any time they wish. This technology adds not only flexibility in Smart Home setup, but the chance to buy more additional devices if needed or select only needed device for cheaper price. This is also a good building base for newly developed devices in the future. The server app is ready, developers and engineers can create their own device and embed it to this system.

1.3.2 API for Client-side application

The Server-side code has the authentication system and possibility to develop any Client-side application based on it. It can be anything, Mobile (Android/iOS), Web (React, Vue, Angular), desktop, etc. Developers can view the documentation and make requests to specific web URL's to get required information or to manage the smart devices.

1.3.3 Synchronization with the Cloud app

The Third required mode was to synchronize the state of devices with the Cloud application. That is why all Smart Home systems are required to have Internet connection, so they could get the state updates when user manages the devices through the Internet. And it's also needed to register sensor and meter values in the main system, to monitor safety and prevent damages and danger cases.

If the Smart Home system doesn't have the Internet connection, it will continue working in the local web build using routers and repeaters. But in that case, there's a solution that is described later.

1.3.4 Flexible architecture

The option of having a flexible architecture opens all doors of creativity and imagination of building and deploying the system. System can be deployed directly from one flat to Internet, or from flat (flats) to the basement main computer, then to the district main computer through fiber optics, then to the Internet. This type of architecture will help us developing a decentralized system later using Blockchain and encryption.

1.3.5 About upgrading it into Blockchain

This system is already successfully deployed in 4 different places. Usually one of the problems was lack of Internet connection. That is why the idea of linking systems together, creating independent nodes and securing the transfer became one of the main tasks of project.

It should work as the Internet, independent nodes could work or crash, but system will still stay online and available. If one of the networks of Internet disconnects, the whole Internet doesn't crash and keeps working.

The idea is the following. Everyone who buy a Smart Home system, agrees to become a network node, that'll receive status updates and transfer other node updates of other Smart Home systems through it. For each transfer of data through the user's system, user will gain points or coins as a transfer commission. If the user doesn't have an Internet connection to synchronize the state updates, the Smart Home user probably might need to have some points too. It means, that the internet connected computer will cover their payment for internet by points of the System that he'll able to sell or exchange with other users of the System. Also, the transfer stations, without a Smart Home system itself could be deployed too, if a user wants to become a node and provide other systems with the required connection. Sure, it's not the best idea of managing the transfer and giving points, but one of the possible solutions.

To become a node and to transfer data, there are a lot of variants and solutions. It could be an ordinary LAN cable (if the distance is short), fiber optics, Lora-WAN network, etc. If the data is transferred through other nodes, it should be crypted and secured from data modification. Here comes the use of Blockchain.

Figure 1.1 Smart Home System

1.4 Components, modules and devices, embedded on Smart Home

1.4.1 Fingerprint door lock authentication

Legacy version of door lock used the Adafruit fingerprint sensor, that is connected to Arduino or ESP8266 to transfer data and handle authentication. Newer version is combined with a ready device that is reconfigured to send authentication requests to the Smart Home system.

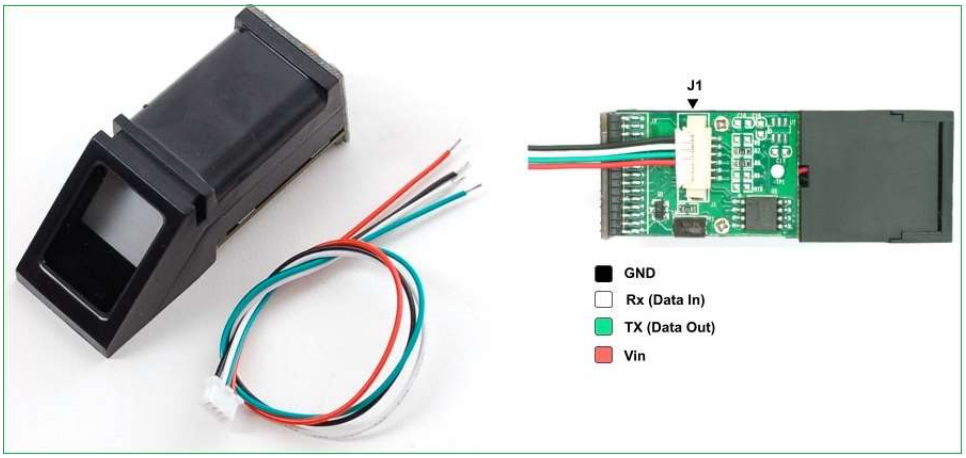

Figure 1.2 Adafruit Fingerprint

1.4.2 ESP8266

In the Arduino world, this circuit is a great solution for IoT tasks. It works the same as the Arduino and it can be easily compiled with Arduino code. But additionally, it can create an access point Wi-Fi or connect to a Wi-Fi, transfer data, handle basic API requests and act as an independent web server [17].

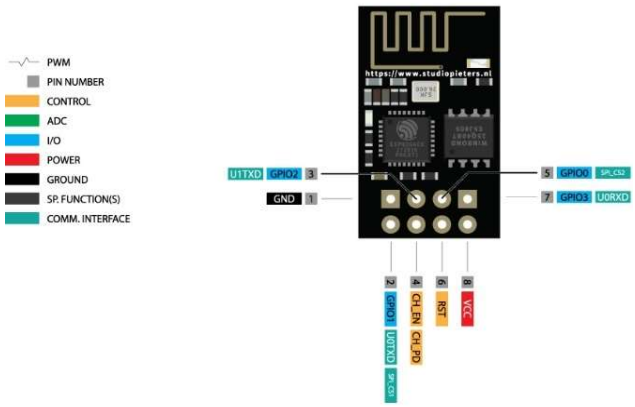

Figure 1.3 ESP8266 microcontroller

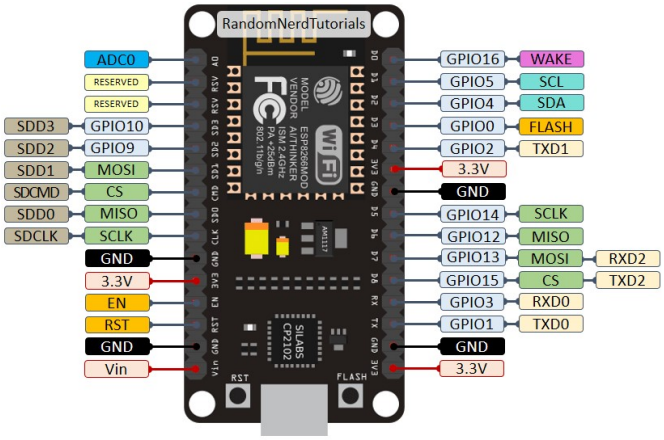

Figure 1.4 NodeMCU ESP8266 microcontroller

1.4.3 RaspberryPi

To deploy the Server-side application, any microcomputer device could be used. One of them is RaspberryPi.

Raspberry Pi is the name of a series of single-board computers made by the Raspberry Pi Foundation, a UK charity that aims to educate people in computing and create easier access to computing education.

Figure 1.5 RaspberryPi

All over the world, people use the Raspberry Pi to learn programming skills, build hardware projects, do home automation, implement Kubernetes clusters and Edge computing, and even use them in industrial applications.

The Raspberry Pi is a very cheap computer that runs Linux, but it also provides a set of GPIO (general purpose input/output) pins, allowing you to control electronic components for physical computing and explore the Internet of Things.

The Raspberry Pi Foundation works to put the power of computing and digital making into the hands of people all over the world. It does this by providing low-cost, high-performance computers that people use to learn, solve problems, and have fun. It provides outreach and education to help more people access computing and digital making it develops free resources to help people learn about computing and making things with computers and also trains educators who can guide other people to learn.

The Raspberry Pi operates in the open source ecosystem: it runs Linux (a variety of distributions), and its main supported operating system, Pi OS, is open source and runs a suite of open source software. The Raspberry Pi Foundation contributes to the Linux kernel and various other open source projects as well as releasing much of its own software as open source.

Some people buy a Raspberry Pi to learn to code, and people who can already code use the Pi to learn to code electronics for physical projects. The Raspberry Pi can open opportunities for you to create your own home automation projects, which is popular among people in the open source community because it puts you in control, rather than using a proprietary closed system.

1.4.4 Other devices, reconfigured to use in the system

Here is the example of a stove of a Siemens company that is reconfigured electronically to use in hybrid mode. It could be managed using the IoT system and through the mobile app, and it also can be used in manual mode.

Figure 1.7 Siemens stove

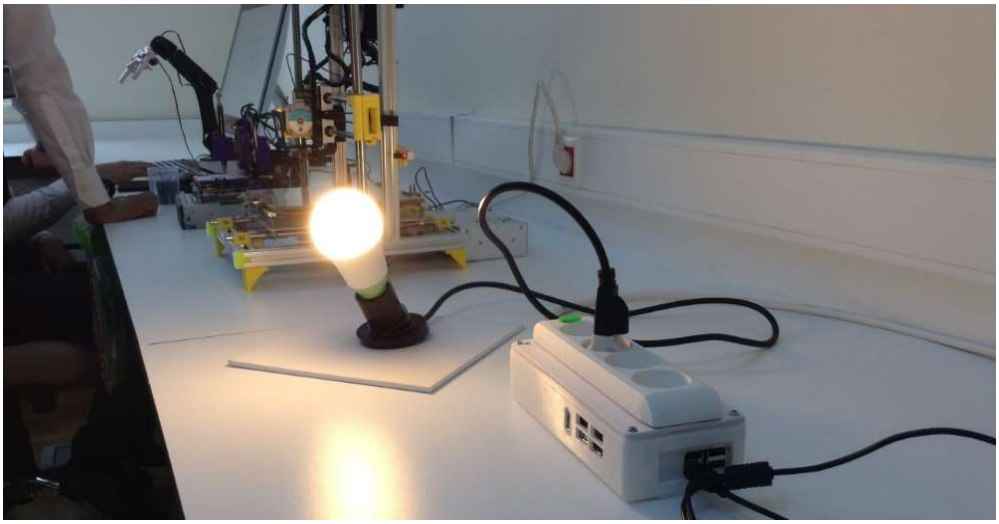

Figure 1.6 Multi-socket device build on RaspberryPi

1.4.5 Ordinary Switch Circuit

To update the state of electric devices, ESP8266 with the circuit is connected. Each GPIO update of ESP8266 occurs, the relays and transistors will manage the higher voltage electricity afterwards.

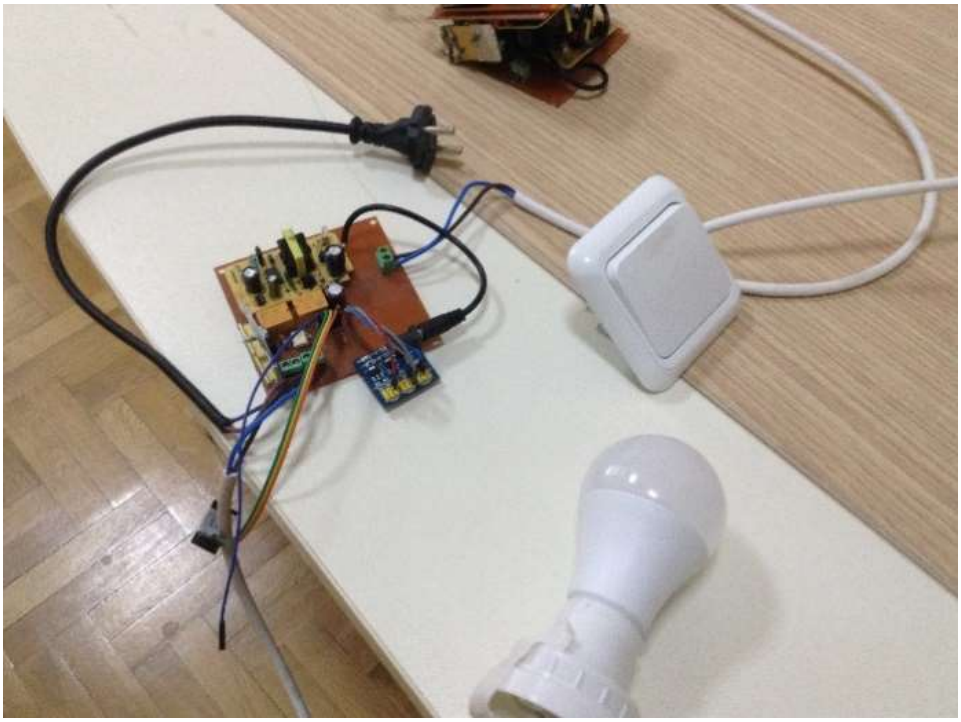

Figure 1.8 Simple switch and lamp circuit

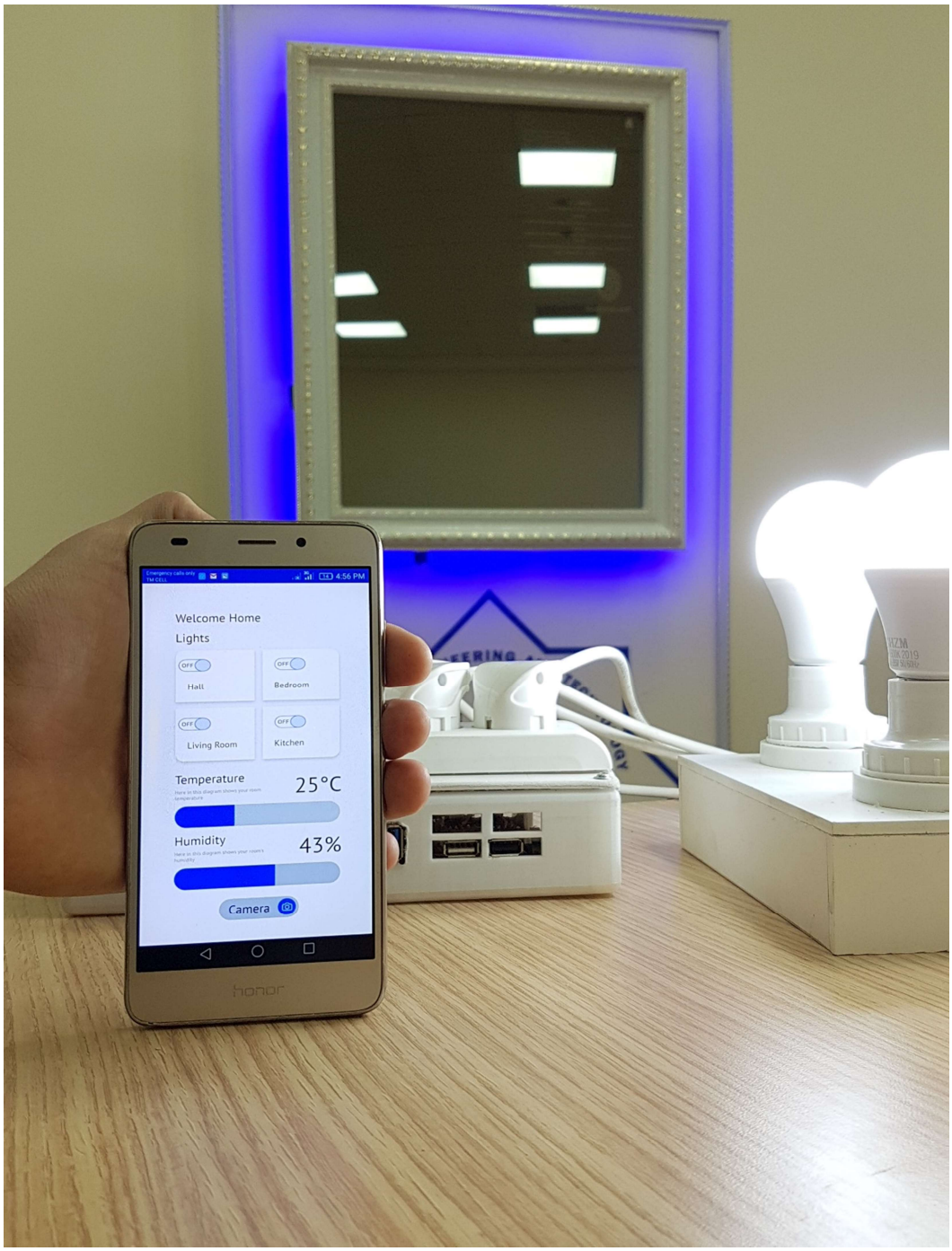

Figure 1.9 Mobile App with a Smart Socket Device

CHAPTER II BLOCKCHAIN BASED CYBERSECURITY

2.1 Introduction of IoT security risks

The Internet of Things (IoT) connects people, places, and products, and in so doing, it offers opportunities for value creation and capture. Sophisticated chips, sensors, and actuators are embedded into physical items, each transmitting data to the IoT network. The analytics capabilities of the IoT use this data to convert insights into action, impacting business processes and leading to new ways of working. However, there are still a number of technical and security concerns that remain unaddressed [1], [22].

Security is a major concern with IoT that has hindered its large-scale deployment. IoT devices often suffer with security vulnerabilities that make them an easy target for Distributed Denial of Service (DDoS) attacks. In DDoS attacks, multiple compromised computer systems bombard a target such as a central server with a huge volume of simultaneous data requests, thereby causing a denial of service for users of the targeted system. A number of DDoS attacks in recent years have caused disruption for organizations and individuals. Unsecured IoT devices provide an easy target for cyber-criminals to exploit the weak security protection to hack them into launching DDoS attacks.

Another issue with current IoT networks is that of scalability. As the number of devices connected through an IoT network grows, current centralized systems to authenticate, authorize and connect different nodes in a network will turn into a bottleneck. This would necessitate huge investments into servers that can handle the large amount of information exchange, and the entire network can go down if the server becomes unavailable.

According to Gartner's Forecast, Internet of Things endpoints are expected to grow at a compound annual growth rate of 32 per cent from 2016 through 2021, reaching an installed base of 25.1 billion units. With IoT devices expected to be such an integral part of our daily lives in the coming years, it is imperative that organizations invest in addressing the above security and scalability challenges [2].

Another breakthrough technology, Blockchain or distributed ledger technology (DLT), has the potential to help address some of the IoT security and scalability challenges. Blockchain is an ‘information game changer’ due to its unique capabilities and benefits. At its core, a Blockchain system consists of a distributed digital ledger, shared between participants in the system, that resides on the Internet: transactions or events are validated and recorded in the ledger and

cannot subsequently be amended or removed. It provides a way for information to be recorded and shared by a community of users. Within this community, selected members maintain their copy of the ledger and must validate any new transactions collectively through a consensus process before they are accepted on to the ledger. For more detailed information on Blockchain technology, please refer to Deloitte's previous publication The Blockchain (R)evolution.

2.2 Solving IoT security and scalability challenges with Blockchain

The IoT network can process data transactions across multiple devices that are owned and administered by different organizations , making it difficult to pinpoint the source of any data leakages in case of an attack by cyber-criminals. Additionally, the IoT generates a vast amount of data, and with multiple stakeholders involved, the ownership of the data is not always clear. Blockchain can help alleviate the security and scalability concerns associated with IoT in the following ways:

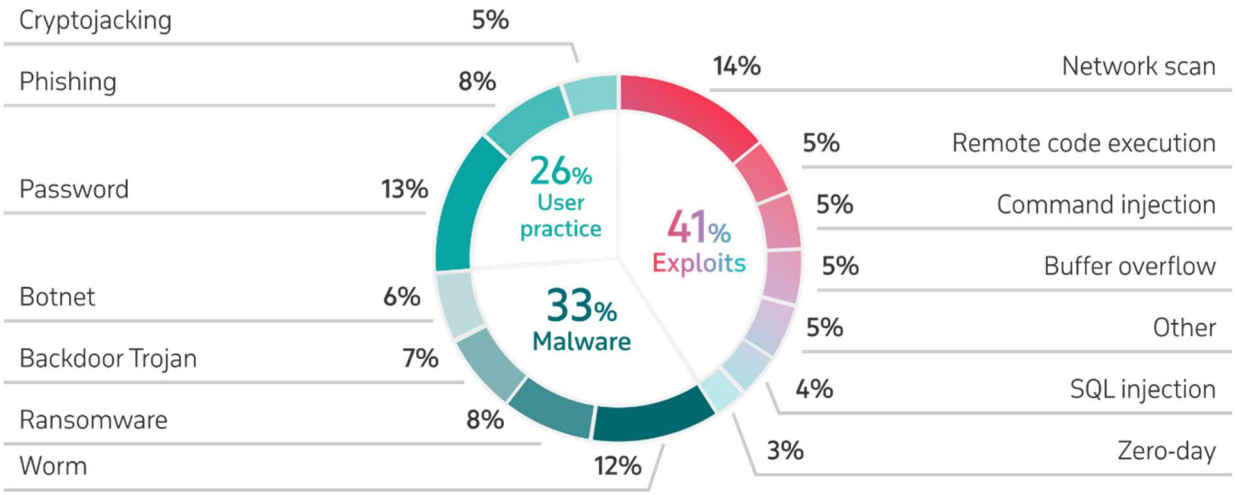

Figure 2.1 Breakdown of top IoT threads

The distributed ledger in a Blockchain system is tamper-proof and this removes the need for trust among the involved parties. No single organization has control over the vast amount of data generated by IoT devices.

Using Blockchain to store IoT data would add another layer of security that hackers would need to bypass in order to get access to the network. Blockchain provides a much more robust level of encryption that makes it virtually impossible to overwrite existing data records [1], [2], [21].

Blockchain provides transparency, by allowing anyone who is authorized to access the network to track the transactions that happened in the past. This can provide a reliable way to identify a specific source of any data leakages and take quick remedial action.

Blockchain can enable fast processing of transactions and coordination among billions of connected devices. As the number of interconnected devices grows, the distributed ledger technology provides a viable solution to support the processing of the large number of transactions.

By providing a way to enable trust among the stakeholders, Blockchain can allow IoT companies to reduce their costs by eliminating the processing overheads related to IoT gateways (for e.g. traditional protocol, hardware, or communication overhead costs) [3].

Smart contracts, an agreement between two parties that is stored in the Blockchain, can further allow the execution of contractual arrangements among stakeholders based on certain criteria being fulfilled. For example, smart contracts can authorize payments automatically, without any need for human intervention, when the conditions for providing a service have been fulfilled.

2.3 Some current Blockchain-IoT players and their use cases

The technology behind sensors and smart chips is evolving rapidly, making them increasingly portable and applicable for real-time interactions with Blockchain ledgers. The combination of Blockchain and IoT has broad potential for the creation of a marketplace of services between devices, and gives companies the opportunity to create value from collected data. The growing number of emerging Blockchain protocols, partnerships and IoT device providers already indicates that there is a good fit for Blockchain in the IoT sector.

Some current Blockchain-IoT players and their use cases are described briefly below. (Please note that the partnerships and companies mentioned in this article should not be considered as endorsements by Deloitte.)

- Chain of Things (CoT) is a consortium of technologists and leading Blockchain companies. It investigates the best possible use cases where a combination of Blockchain and IoT can offer significant benefits to industrial, environmental, and humanitarian applications. So far, CoT has built Maru, an integrated Blockchain and IoT hardware solution to solve issues with identity,

security, and interoperability. There are three developed use cases named Chain of Security, Chain of Solar and Chain of Shipping [4], [23].

- IOTA is a protocol for fast transaction settlement and data integrity, with a Tangle ledger that eliminates the need for expensive mining (validation of transactions). IOTA is a promising infrastructure for IoT devices that need to process large amounts of micro data. Features of the Tangle ledger, which is the distributed ledger that supports IOTA, are machine-to-machine communication, fee-less micropayments, and quantum resistant data. IOTA has built a sensor data marketplace and is entering the market for data-driven insights, supported by more than 20 global corporations.

- Riddle&Code provides cryptographic tagging solutions for Blockchains in smart logistics and supply chain management. Working on the integration between IoT devices and distributed ledger networks, Riddle&Code offers a combined, patented hardware and software solution that enables secure and trusted interaction with machines in the IoT age by giving machines and any physical device a 'trusted digital identity'. This technology breaks through the physical/digital divide to strike a balance between the demand for paper documentation and the advantages that Blockchain technology has to offer.

- Modum.io combines IoT sensors with Blockchain technology, providing data integrity for transactions involving physical products. The modum sensors record environmental conditions, such as temperature, that goods are subject to while in transit. When the goods arrive at the next transit point or end customer, the sensor data is verified against predetermined conditions in a smart contract on the Blockchain. The contract validates that the conditions meet all of the requirements set out by the sender, their clients, or a regulator and triggers various actions such as notifications to sender and receiver, payment, or release of goods [3].

2.4 Considerations for the adoption of Blockchain and IoT technologies

As explain previously, a fundamental problem with current IoT systems is their security architecture, with a centralized client-server model managed by a central authority which makes it susceptible to a single point of failure. Blockchain addresses this problem by decentralizing decision-making to a consensus-based shared network of devices. However, when designing the architecture for IoT

devices in conjunction with a Blockchain ledger, there are three main challenges to consider:

1. Scalability.

   One of the crucial difficulties still faced by IoT is one of scale - how to handle the massive amounts of data collected by a large network of sensors and potentially lower transaction processing speeds or latencies. Defining a clear data model beforehand can save time and prevent difficulties when bringing the solution into production.

2. Network privacy and transaction confidentiality.

   The privacy of transaction history in the shared ledger for a network of IoT devices cannot be easily granted on public Blockchains. That is because transaction pattern analysis can be applied to make inferences about the identities of users or devices behind public keys. Organizations should investigate their privacy requirements to see whether hybrid or private Blockchains might suit their requirements better.

3. Sensors.

   The reliability of IoT sensors could potentially be undermined by interfering with the correct measurement of the criteria that need to be met to execute a transaction. Measures to ensure the integrity of IoT devices such that they cannot be altered by external interventions are key to securing a safe environment for data recording and transactions.

Blockchain and IoT are both emerging technologies with great potential, but still lacking widespread adoption due to technical and security concerns. Several companies in the market are already working on use cases combining the two technologies, as together they offer a way to minimize the security and accompanying business risks [5], [24]

2.5 Advantages of IoT

This technology entails new business models and, therefore, new revenue models. IoT brings incredible opportunities for companies to offer real-time sensor data and information services. It is efficient for automating business and manufacturing processes, as well as remotely controlling operations, conserving resources and optimizing supply chains.

The Internet of Things boosts the productivity and effectiveness of the workforce in many ways because beyond automating routine tasks, it also accelerates the process of decision-making and communications.

With IoT, companies can offer an enhanced experience to customers: in addition to being useful, the products and services related to it have attractive physical and digital characteristics, and they can also be customized.

2.6 Areas where Internet of Things applied

The impact of IoT is evident in a wide range of businesses. For example, the way products were made changed with the use of the Internet of Things (IoT) along with Machine to Machine (M2M) communication, boosting automation. This technology is capable of preventing or foreseeing failures and even making work safety reliable.

The use of the IoT also has many important applications in the field of transport. Intelligent transport systems for both people and goods use IoT sensors. This includes trains, planes, ships and vehicles. The aim is to increase engine performance, manage the supply chain and handle logistics and security.

Car manufacturing and technology companies use the Internet of Things. How? Intelligent vehicles help drivers anticipate maintenance problems, accidents, find parking spaces, etc. [5], [24].

2.7 IoT Safety

As for the safety of IoT, it is based on the technology that protects both the connected equipment and the IoT itself. The «Things» have a unique identifier that automatically passes data over the network; but if they are not protected, they run the risk of being targeted for vulnerabilities. For this reason, measures have been introduced to ensure the safety of networks and the devices connected to them.

Although there is no single standard, the GSM Association, the Industrial Internet Consortium, IoT Security Foundation and other institutions released frameworks. In addition, in the US, the FBI warned about vulnerabilities and offered protection recommendations; Congress has also pointed out measures that manufacturers must respect, and the Senate passed the IoT Innovation and Growth Development Act.

Also, the General Data Protection Regulation covers privacy in the European Union, which extends to devices that work with IoT; in the state of California, they certified the privacy of information that covers all connected devices sold in the country, with their respective security requirements [3], [6].

2.8 Internet of Things Safety Challenges

While there are many ways to secure IoT devices, it will always be a challenge, especially since some designers and manufacturers focus on selling fast rather than ensuring safety from the start.

The things you need to pay close attention to are:

- Passwords that are already encrypted, because even if they are changed frequently, they must be strong enough not resist infiltration.

- The availability of security features such as advanced encryption, because it is common that there are some resource constraints.

- Providing upgrades or patches, however costly it may be to the manufacturer, is necessary for security.

- Legacy assets connectivity, those that were basically not designed for connectivity.

- Agreeing on a single framework of protection rather than specific standards, because this would make security less difficult and interoperability more reliable.

- Educating customers or users to apply their own methods of precaution, to avoid any breach in security [5], [23].

2.9 Internet of Things IoT Challenges

Many companies have already embraced this technology, which makes their infrastructure more complex. In the telecommunications sector, the IoT focus is on 5G networks that support the millions of connected devices. The idea is to meet the problem of temporary delays, high speed and low power consumption. Public institutions such as the government also use IoT to implement numerous services, such as lighting, security, traffic, etc.

The implementation of the Internet of Things leads to a hyper-connected world over which we must have control and in which security is a permanent

challenge. For this reason, it relies on programming codes that address such a problem [6].

2.10 Security problems of the IOT

The Internet of Things (IoT) presents a series of unknowns for users, ranging from privacy to security. The growth of the Internet of Things (IoT) is continuous and there are an increasing number of devices in daily use connected to the network. The same happens in industries, where there is a trend towards the interconnection of autonomous and intelligent factories.

Technology is moving towards hyper-connectivity in platforms, networks, applications and devices, but all of this requires protection measures, proportionate to the intelligence of the devices and their behavior.

IoT has to think beyond usability and apply sufficient focus on things like:

- Software protection.
- Implementation of practices against vulnerabilities.
- Ensuring the authenticity and integrity of future patches.

The 10 most common security problems of IOT in this domain and their possible solutions:

1. Ecosystem Complexity

Since it should not look like a compendium of stand-alone devices, IoT becomes tangled in its complexity. IoT should to be understood as a rich, broad and diverse ecosystem that integrates people, communications and interfaces.

Although it simplifies life and industrial production, the application of the concept is not simple, as there are many components in its ecosystem. These range from sensors (devices), networks (bridges, routers, WiFi technology, LiFi, etc.) technological standards (protocols: network, communication and data) and regulations (confidentiality and security) [7].

2. Limited capacities in devices

Many IoT devices come with inherent limitations in power, processing and memory. As a consequence, they are not always managed with the advanced security patterns the need, which is why they are at greater risk of being attacked

or succumbing to defects. That's why the architecture of the equipment has to be scalable because it's a way to offer security.

3. Limited experience

As technologies related to the Internet of Things are in many cases still relatively new, we do not have a background of previous threats to let us know about failures in protection. There are not many cybersecurity experts specializing in IoT. A few basic rules are barely available.

4. Threats and attacks

There are computer programs specially designed to attack IoT devices and the ecosystem itself. These are threats called malware. They perform unwanted actions without the user's consent, causing damage and data theft. Exploit Sequences are other code-based abuses that take advantage of fragile points to access the system, hitting the infrastructure with a high to severe impact, depending on the assets affected. Among other threats, we can also mention information modification, message reproduction, network failure, system or device failures, data filtering and device modification [7].

Often, manufacturers strive to reduce the development and launch cycle of products, prioritizing time to market and the volume of sales and without stopping to consider fundamental factors in the design phase, such as access control or encryption of information, among many others

5. Privacy

When we accept any contract without reading or understanding the clauses it contains, and in truth we all do sometimes, the privacy of our information is at risk. The number of people who click «accept» without understanding or even reading the terms when using applications or devices to work with the Internet of Things is extremely high.

Manufacturers, eager to stay one step ahead of the competition, do not always apply enough diligence towards auditing their equipment sufficiently, and often do not dedicate sufficient resources to ensure that those who embrace these devices within their lives can be fully confident.

6. Reduced costs

In order to reduce costs, manufacturing companies could limit security investment. The result can be equipment that can never provide adequate protection. The end user would always be at risk. Reducing costs in hardware as

well as in development in this context can be a terrible mistake. The user is the one who ends up paying.

7. Lack of clarity in responsibilities

Regarding safety in IoT devices, there are three key players: manufacturer, service provider and user. In the event of a cyber-attack, the assignment of responsibilities is not entirely clear and can lead to conflicts. Another important aspect is how security would be managed when a component is shared between several parties.

8. Lack of rigor in data processing

At the heart of most security problem's in IoT is that the user is often unaware of how the data they transmit via sensor devices will be used, because conventional methods of consent are of poor quality, i.e. they do not specify the subsequent handling of personal information. Such information could reach third parties, and the user will not be aware of this.

9. Safety versus efficiency

The speed with which IoT devices are to be manufactured limits safeguard considerations, and the budget is likely to have an impact, which means the company would emphasize usability rather than security.

10. Limitation of anonymity

It's linked to a lack of rigor in data processing. Sometimes we assume that anonymity is guaranteed in any service we use, but it really is not. In IoT, to guarantee this, it is necessary to optimize the techniques of access control, encryption, design privacy, safeguarding the location and any basic aspect to avoid any undesired intervention [7].

CHAPTER III BLOCKCHAIN IN THE INTERNET OF THINGS

Fundamentally, the data stored in a Blockchain should have consisted of the following characteristics:

- Immutable
- Distributed
- Persistent (no loss of data)
- Not hackable

A Blockchain is an open-source application that is shared between thousands of computers. These computers follow a set of rules in order to track money that has been sent from accounts tied to the Blockchain software. These qualities are mandatory in order to maintain the Blockchain's integrity and the network security within which the transactions occur.

Security of Internet of Things (IoT) devices is an ongoing problem. The largely unregulated IoT market leaves plenty of room for device hacking. When considering applications such as smart homes and smart cars, this lack of security can be a real concern. A hacker, for example, could take over a self-driving car with someone in it, or make purchases based on access levels given to an IoT system. With all of the data that is collected and passed between IoT devices, strong security is a must.

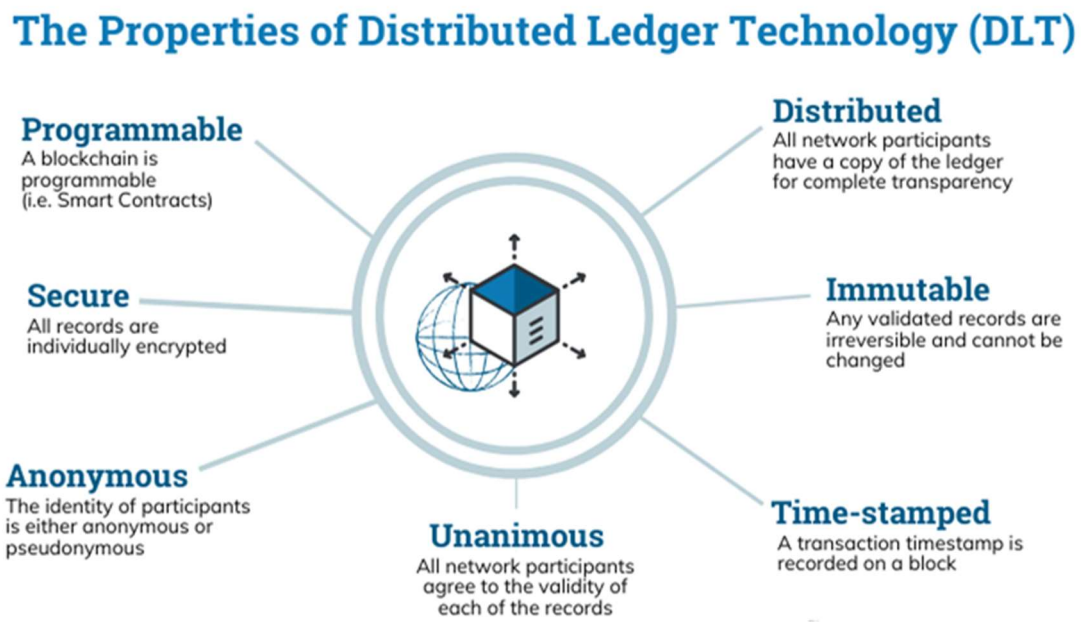

Figure 3.1 The Properties of Distributed Ledger Technology (DLT)

While there are many security recommendations for IoT devices, such as biometrics and two-factor authorization, one potential solution is Blockchain IoT security. Blockchain, which is most familiar for bitcoin and Ethereum, offers an intriguing solution for IoT security. Blockchain contains strong protections against data tampering, locking access to Internet of Things devices, and allowing compromised devices in an IoT network to be shut down. Hyundai has recently backed a Blockchain start-up that is specifically designed for IoT security. Called HDAC (Hyundai Digital Access Currency), this innovative approach creates a permissioned private network [10].

If there is to be Blockchain IoT security, however, there are issues to be overcome. For one, Blockchain mining requires a large amount of processing power. Many IoT devices lack the power needed. Current Blockchains are vulnerable if a group of miners controls more than 50% of the network's mining hash rate. The global distribution of nodes in a typical Blockchain makes this very difficult. But a home IoT Blockchain's processing power might be more easily hacked [9].

3.1 Basic Blockchain security

Blockchain technology produces a structure of data with inherent security qualities. It's based on principles of cryptography, decentralization and consensus, which ensure trust in transactions. In most Blockchains or distributed ledger technologies (DLT), the data is structured into blocks and each block contains a transaction or bundle of transactions. Each new block connects to all the blocks before it in a cryptographic chain in such a way that it's nearly impossible to tamper with. All transactions within the blocks are validated and agreed upon by a consensus mechanism, ensuring that each transaction is true and correct.

Blockchain technology enables decentralization through the participation of members across a distributed network. There is no single point of failure and a single user cannot change the record of transactions. However, Blockchain technologies differ in some critical security aspects [8].

Blockchain networks can differ in who can participate and who has access to the data. Networks are typically labeled as either public or private, which describes who is allowed to participate, and permissioned or without permission, which describes how participants gain access to the network.

3.2 Public and private Blockchains

Public Blockchain networks typically allow anyone to join and for participants to remain anonymous. A public Blockchain uses internet-connected computers to validate transactions and achieve consensus. Bitcoin is probably the most well-known example of a public Blockchain, and it achieves consensus through "bitcoin mining» Computers on the bitcoin network, or «miners» try to solve a complex cryptographic problem to create proof of work and thereby validate the transaction. Outside of public keys, there are few identity and access controls in this type of network [9].

Private Blockchains use identity to confirm membership and access privileges and typically only permit known organizations to join. Together, the organizations form a private, members-only "business network» A private Blockchain in a permissioned network achieves consensus through a process called "selective endorsement» where known users verify the transactions. Only members with special access and permissions can maintain the transaction ledger. This network type requires more identity and access controls.

When building a Blockchain application, it’s critical to assess which type of network will best suit your business goals. Private and permissioned networks can be tightly controlled and preferable for compliance and regulatory reasons. However, public and without permission networks can achieve greater decentralization and distribution.

- Phishing attacks

Phishing is a scamming attempt to attain a user's credentials. Fraudsters send wallet key owners emails designed to look as though they're coming from a legitimate source. The emails ask users for their credentials using fake hyperlinks. Having access to a user's credentials and other sensitive information can result in losses for the user and the Blockchain network.

- Routing attacks

Blockchains rely on real-time, large data transfers. Hackers can intercept data as it's transferring to internet service providers. In a routing attack, Blockchain participants typically can't see the threat, so everything looks normal. However, behind the scenes, fraudsters have extracted confidential data or currencies.

- Sybil attacks

In a Sybil attack, hackers create and use many false network identities to flood the network and crash the system. Sybil refers to a famous book character diagnosed with a multiple identity disorder.

- 51% attacks

Mining requires a vast amount of computing power, especially for large-scale public Blockchains. But if a miner, or a group of miners, could rally enough resources, they could attain more than 50% of a Blockchain network's mining power. Having more than 50% of the power means having control over the ledger and the ability to manipulate it [8], [9].

Note: Private Blockchains are not vulnerable to 51% attacks.

3.3 Blockchain security for the enterprise

When building an enterprise Blockchain application, it’s important to consider security at all layers of the technology stack, and how to manage governance and permissions for the network. A comprehensive security strategy for an enterprise Blockchain solution includes using traditional security controls and technology-unique controls. Some of the security controls specific to enterprise Blockchain solutions include:

- Identity and access management
- Key management
- Data privacy
- Secure communication
- Smart contract security

3.4 Transaction endorsement

Employ experts to help you design a compliant and secure solution and help you achieve your business goals. Look for a production-grade platform for building Blockchain solutions that can be deployed in the technology environment of your choosing, whether that is on-premises or your preferred cloud vendor.

3.5 Blockchain security tips and best practices

When designing a Blockchain solution, consider these key questions:

1. What is the governance model for participating organizations or members?
2. What data will be captured in each block?
3. What are the relevant regulatory requirements, and how can they be met?
4. How are the details of identity managed? Are block payloads encrypted? How are the keys managed and revoked?
5. What is the disaster recovery plan for the Blockchain participants?
6. What is the minimal security posture for Blockchain clients for participation?

When establishing a private Blockchain, ensure that it's deployed in a secure, resilient infrastructure. Poor underlying technology choices for business needs and processes can lead to data security risks through their vulnerabilities.

Consider business and governance risks. Business risks include financial implications, reputational factors and compliance risks. Governance risks emanate primarily from Blockchain solutions' decentralized nature, and they require strong controls on decision criteria, governing policies, identity and access management.

Blockchain security is about understanding Blockchain network risks and managing them. The plan to implement security to these controls makes up a Blockchain security model. Create a Blockchain security model to ensure that all measures are in place to adequately secure your Blockchain solutions.

To implement a Blockchain solution security model, administrators must develop a risk model that can address all business, governance, technology and process risks. Next, they must evaluate the threats to the Blockchain solution and create a threat model [8].

Then, administrators must define the security controls that mitigate the risks and threats based on the following three categories:

1. Enforce security controls that are unique to Blockchain
2. Apply conventional security controls
3. Enforce business controls for Blockchain

IBM Blockchain services and consulting can help you design and activate a Blockchain network that addresses governance, business value and technology needs while assuring privacy, trust and security.

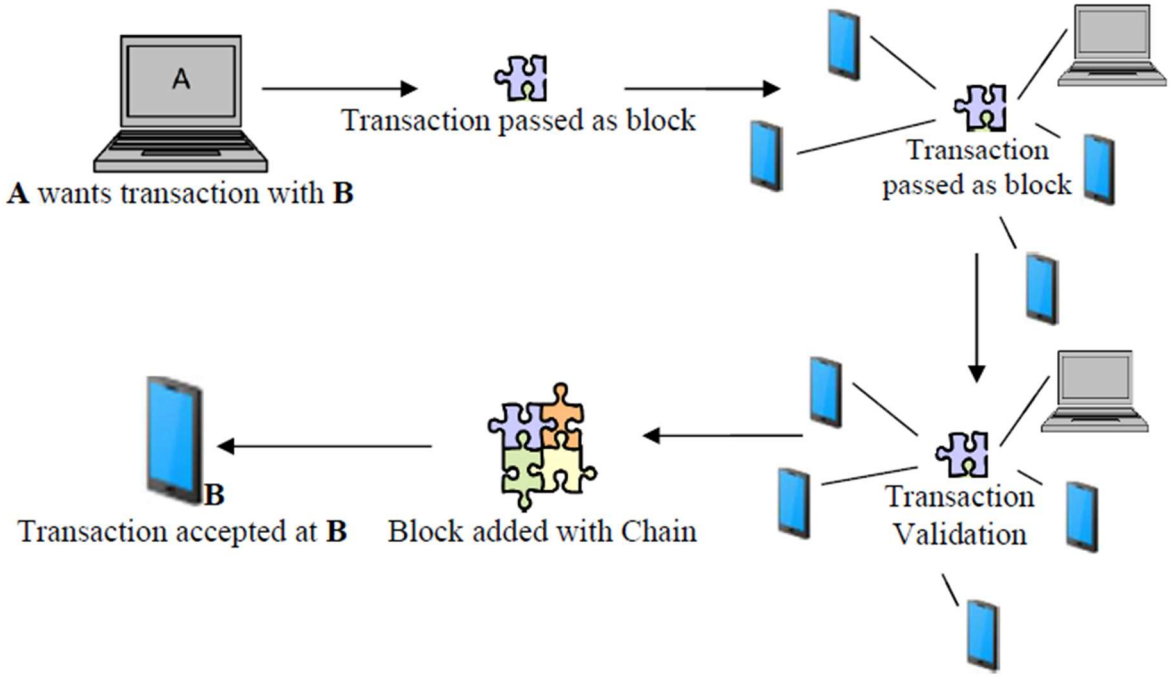

Figure 3.2 Blockchain Transaction example 1

Blockchain is a distributed database technology that provides very hard to tamper, ledger records. It allows storage of all transactions into immutable records and every record distributed across many participant nodes. The security comes from use of strong public-key cryptography, strong cryptographic hash and complete decentralization.

Blocks are the key concept of the technology. They are small sets of transactions that have taken place within the system. Each new block stores reference of the previous transaction by including a SHA-256 hash of the previous transaction. In this way, it creates a «chain» of blocks and hence the name. Blocks are computationally difficult to create, and takes multiple specialized processors and significant amounts of time to generate.

Since generating a block is difficult and to tamper one block, one has to tamper the previous block and then has to follow the chain to change it completely, Blockchain technology is considered to be tamper resistant. Miners are the ones who run powerful computers to create blocks.

So, the key strengths of Blockchain technology can be summarized as:

- It is strongly tamper-resistant
- If is highly scalable due to not having any single point of failure and being peer-to-peer network
- It can serve as an immutable system of records for all stakeholders

With IoT started getting into the mainstream industry, the key challenges of the technology are fast emerging. One of the key areas of IoT deployment is security. Following are the key security challenges for IoT infrastructure and services:

- With the prospect of devices in the infrastructure growing exponentially, it is a huge challenge to identify, authenticate and secure the devices.
- A centralized security model will be very difficult and expensive to scale, maintain and manage.
- A centralized security infrastructure will introduce a single point of failure and will be an easy target for DDoS attack.
- Centralized infrastructure will be difficult to implement in industrial setup where the edge nodes are widespread geographically [10]
- Blockchain technology seems to be a viable alternative due to the key strengths described above.

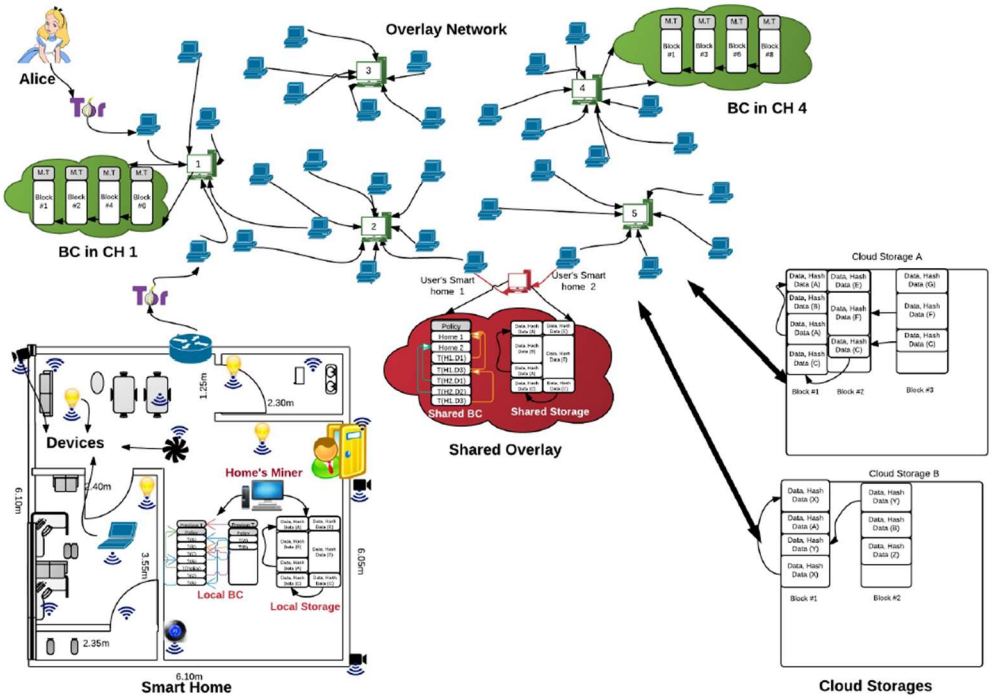

Figure 3.3 Smart Home and Mining computer network example

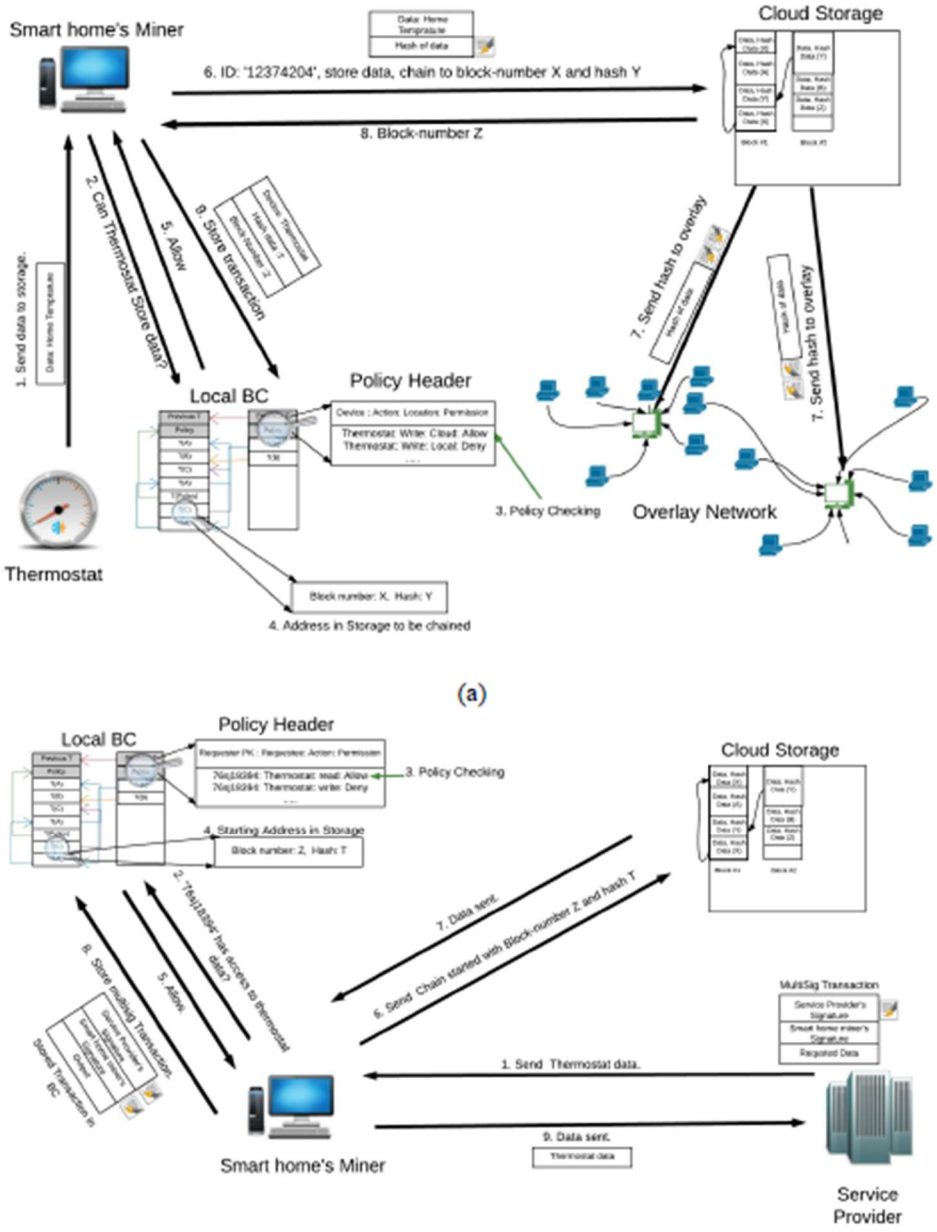

Figure 3.4 Smart Home data transaction workflow

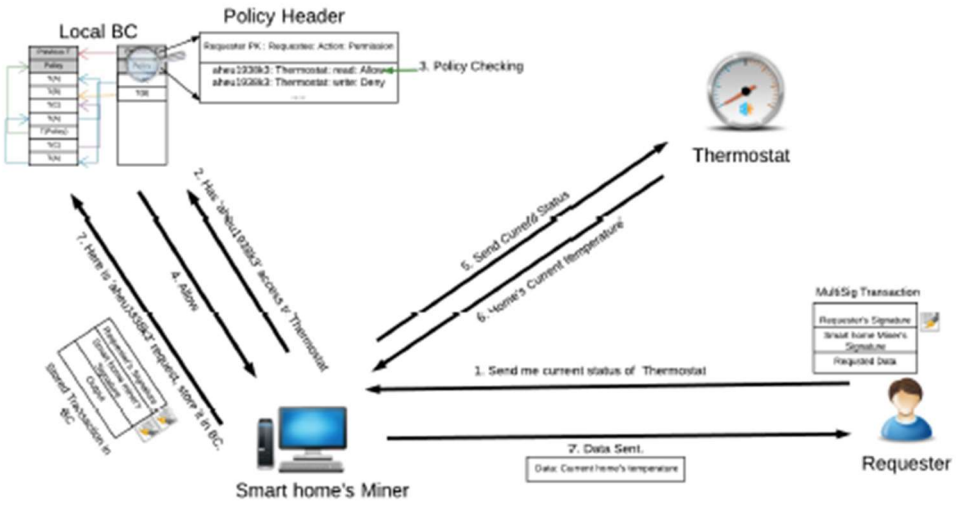

Figure 3.5 Smart Home data transaction workflow 2

3.6 Cases where Blockchain can be used

It can be used to create secured mesh network that will allow IoT devices to connect securely and reliably avoiding the threats of device spoofing and impersonation.

Every IoT node can be registered in the Blockchain and will have a Blockchain id which will uniquely identify a device in the universal namespace. For a device to connect another device, one will use the Blockchain id as URL and will use its local Blockchain wallet to raise an identity request. The wallet will create a digitally signed request and send to the target device which will use Blockchain services to validate the signature using the public key of the sender. In this way, M2M authentication can take place without the need of any centralized arbitrator or service.

For a device that is constrained by a resource can be connected to proxies where the wallet can be stored. This will introduce some form of aggregation but it will be fairly limited. The above possible solution will be applicable to a wide range of IoT services. Some of the examples will be intelligent healthcare connected vehicles, logistics, transportation etc.

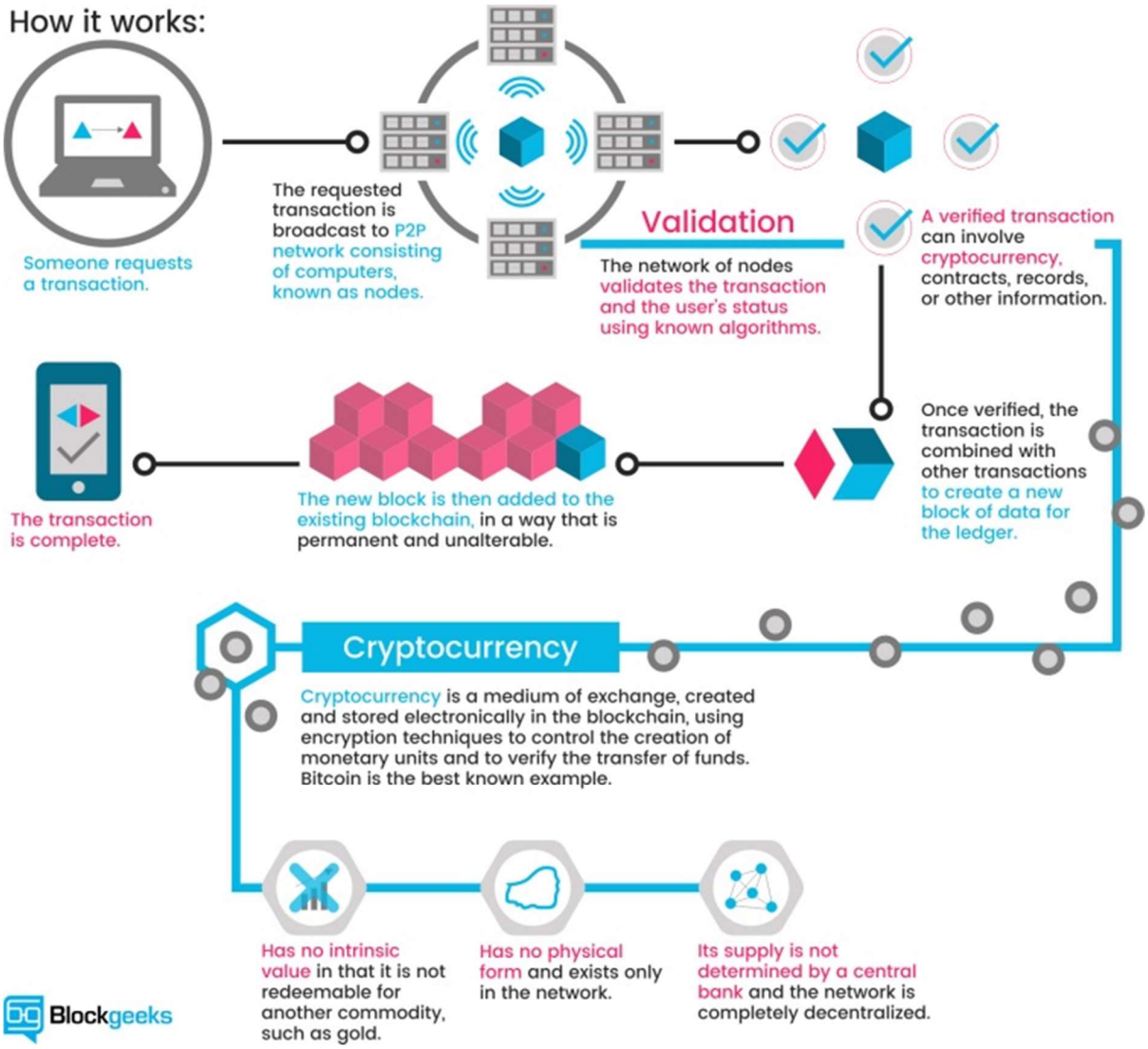

Figure 3.5 Smart Home data transaction workflow 2

3.7 Cases where Blockchain is not the best solution

One key benefit of using Blockchain technology is its use as a distributed recording system. It allows to securely write immutable records. To do that, it used strong cryptography and replication. For example, in supply change management, a consignment has to go via a series of activities and the status of the piece of an item can be monitored via RFID and recorded using Blockchain technology.

However, this comes with its overhead. The replication introduces latency. Getting a block sometimes take longer. Strong cryptographic processes introduce latency. The latencies are not acceptable in a near-time and real-time service situation. Hence, Blockchain is not best suited in a recording of raw data at the source [8], [10].

A slight improvisation may make Blockchain adapted to near-time situations. An introduction of aggregation caching node at the closest distance of the sources can be used as a broker between source and Blockchain services. However, this will be a deviation from the key strength of Blockchain and must be used after careful consideration.

When it comes to competitive advantages in a company, the Internet of Things (IoT) turns out to be a very powerful weapon. Each piece of data collected is extremely important to initiate or successfully request an action without human intervention, in which both the privacy and security of the user are compromised.

Considering each technological and physical component of the Internet ecosystem of Things, this technology is understood as if it were a system of systems, with great business value, which needs integrated solutions and protection to complement its functionality.

3.8 How to implement Blockchain for IoT Safety

Blockchain technology began to be known with the advent of crypto coins mining since it is its main technology. But now, it also has much to do with the IoT. The amount of data processed by IoT devices is enormous, all supplied in a chain and exposed to attacks by cybercriminals. It is in this context where the possibility arises to take advantage of the Blockchain architecture to authenticate, standardize and protect the adoption of data handled by the devices.

For IoT safety, the Blockchain is able to monitor the information collected by the sensors, without allowing them to be duplicated by any wrong data. Sensors can also transfer data using Blockchain technology, without the need for a trusted third party. In addition, we must add device autonomy, data integrity, virtual identity and point-to-point communication, all to get rid of technical deficiencies and bottlenecks. As if that weren’t enough, Blockchain and devices related to the Internet of Things are addressable and are able to list a history of connected equipment, opening a bank so that in the future problems can be solved [10].

3.9 Coordination between devices

As far as IoT is concerned, Blockchain technology stands out thanks to its ability to solve scalability, reliability and privacy issues. It enables coordination

between devices, as well as tracking millions of connected devices and processing transactions.

This is a decentralized approach in which cryptographic algorithms are implemented so that customer data enjoy greater privacy. It is an approach that eradicates faults and offers a resilient ecosystem. The connectivity it provides is unprecedented because the Blockchain is based on an optimal platform, which is efficient considering solutions for the IoT require coordination so that the devices work integrated, without causing problems. It is a secure infrastructure, far from the centralized model.

3.10 A trend towards protection

For greater transparency, convenience and security, Identity Management is systems chosen by companies to control access management. Blockchain Identity is one of those trends, for its ability to store information in chains of transactions that prevent its modification when verified. The structure stores the data equitably, preventing server leaks. In addition, it is also important to mention Authentication systems, which require the verification of data, as well as the protection of company and staff information, approved by consensus as a right by the General Data Protection Regulations.

3.11 Processing transactions

When we speak of transactions, we refer to the actions created by the participants of the system. Blockchain records these or digital interactions so that they are carried out in a safe, auditable, transparent, efficient and interruption-resistant manner. Each block registers the operations with a time stamp and verifies that they are in the correct sequence, without manipulations. If someone wants to add a transaction to the chain, everyone in the network validates it through an algorithm; the approved transactions are gathered into a block and distributed to each node in the network. The new block and successive blocks are validated with a single fingerprint corresponding to the previous block.

There are billions of transactions per device, and adopting a standardized, point-to-point communication model would reduce installation and maintenance costs in huge Big Data centers, as well as the storage of devices that make up the IoT networks, preventing errors in nodes dragged by a collapse or arrest.

So that there is no theft and much less impersonation in each transaction that takes place, it is proposed to use some kind of consensus and validation of peer-to-peer communications, so that the privacy and security of large networks of the IoT persists.

3.12 Data Tracking

On the basis of all devices that can communicate with ledgers, entrenched in Blockchain, the devices used in IoT end up being safe in transactions. The information provided by the customer can be tracked so that the experience is smooth and continues as private and inviolable; furthermore, by using storage and encryption, every part of the chain can rely on the data.

All heavy work falls on technology, through machines, without the need for a human to execute the processes. The Blockchain is an ally for solving scalability and trust issues. The keys will always be private and nobody will be able to overwrite the codes, offering this way the security dreamed in operations of the Internet of the Things.

3.13 More advantages of Blockchain on IoT

- It is public, so those who participate can see the blocks, but not the actual content of the transaction, as they are protected by private keys.
- It is decentralized and there is enough trust.
- Network participants reach a consensus to approve transactions.
- The database expands, although records are kept. If someone wanted to modify the previous records, the cost would be very high.
- Blockchain Identity is one of the trends in high-capacity technologies such as authentication systems. These aspire to become a law, as they encompass the protection of information that benefits both businesses and individuals, a topic that has been widely discussed.
- It allows you to share the use of multiple files.
- It guarantees robustness and stability of resources, eliminating the flow of traffic to one and lowering the delay.

- The network is secure, the user's identity will always be private.

3.14 Privacy in IoT

Privacy is one of the main unknowns and sensitive issues raised by the IoT. So much so that throughout today's post we will analyze the control systems and regulations in force for compliance [10].

The Internet of Things (IoT) is becoming more widespread every day, and this means that consumers need more and better security, which translates into privacy. All this in the face of the vulnerability represented by corporate surveillance and data breaches.

Consumers gradually unwittingly expose their privacy, as they do not know what data is collected and how it is used, for example by mobile applications or apps. The percentage of people who do not read security policies and accept them without knowing is very high. In fact, there are those who try to read them, but their legal language is in most cases unintelligible to the average consumer, even allowing them to omit clauses that include the right to be heard in court.

As you know, companies are becoming increasingly crowded with intelligent things and industrial sensors; unfortunately, security will always be difficult. Most Internet-connected devices are effectively managed by the Dynamic Host Configuration Protocol (DHCP) which automates IPs. However, the support that gives additional functions is not regular [9], [10].

In the specific case of the Internet of Things, privacy in layers is a policy that companies should adopt. They consist of the legal code, what is legible by man and what the machine reads.

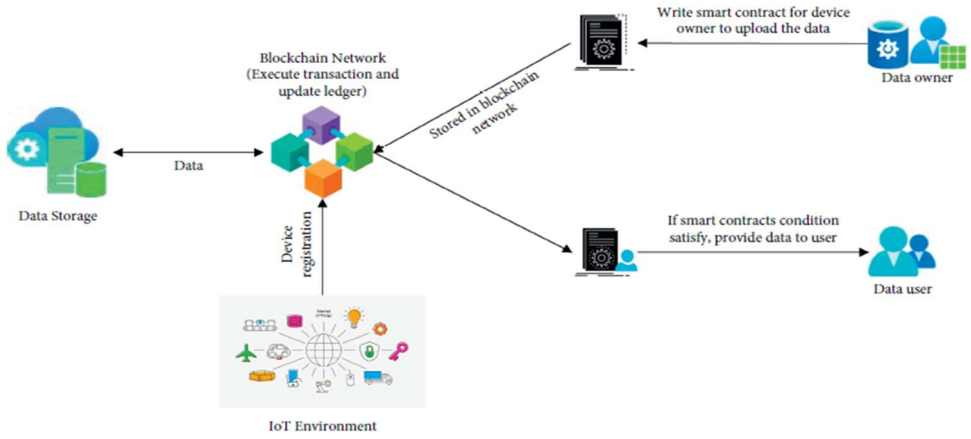

Figure 3.6 Smart Contracts and Device registration workflow

The first refers to the actual policy that lawyers write and that judges will interpret; the second is a simple summary for the client to read and understand; while the third is the code read by search engines or software, or understood by technology that would only access the information that the consumer allows. The implementation of the different layers would be significant progress in safety regulations.

3.15 Control systems

Nowadays, to speak of a control system for the security of the IOT is to refer directly to the response that a company must offer when the client claims security. As a real case that deserves special mention, there is the response of the Alliance of Automobile Manufacturers, which developed privacy policies after its customers expressed in a survey their concern for information privacy and the security of connected cars.

At present, a control system corresponds to the self-regulation and practices that the industry implements on data minimization and security since it is their obligation to protect them and if they do not agree to do so, then they should refrain from collecting them.

Privacy by design is another method of the control system, in which manufacturers analyze risks and considerations at the product design stage In addition, it is logical that they take into account that privacy goes beyond the useful life of a piece of equipment and the acquisition of a first customer because if IoT devices were resold, the data of the original purchaser should not remain forever in the device.

The general ethical and legal framework of rights and obligations involving the IOT. Yes, more corporate transparency is needed for IoT's privacy success, and it would be achieved through the rules that the government requires of companies and industrial self-regulation.

The Industrial Internet Consortium, the GSM Association and the IoT Security Foundation, among others, have so far generated some statutes.

3.16 How Blockchain Technology Works

Say a burglar is planning a sophisticated act on a high-profile target. To prevent the act from being recorded, the burglar can first attack the server running the database where the videos are stored, he said.

The distributed aspect of Blockchain means that data are replicated across several computers. This fact makes the hacking more challenging since there are now several target devices.

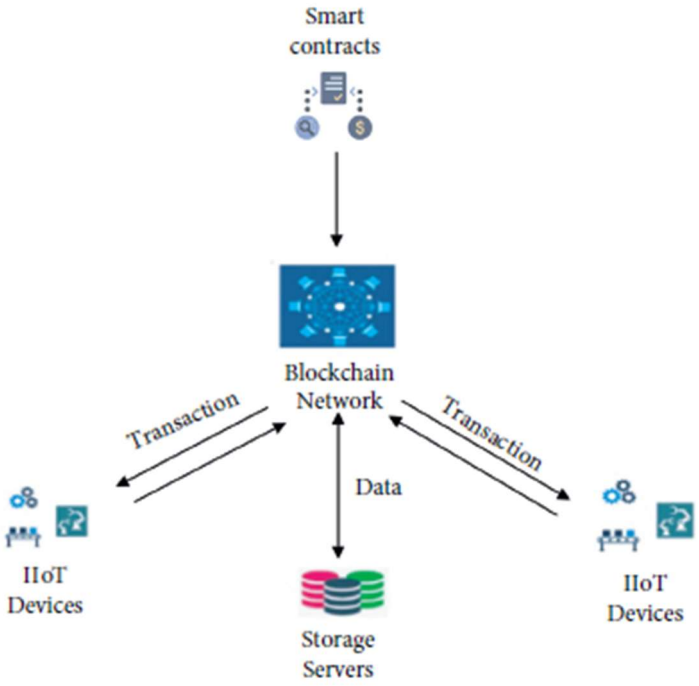

Figure 3.7 Smart Contracts in Blockchain Network

The redundancy in storage brought by Blockchain technology brings extra security and enhances data access since users in IoT ecosystems can submit to and retrieve their data from different devices.

Continuing with this example, say the burglar is captured and claims in court that the recorded video is forged evidence. The immutability nature of Blockchain technology means that any change to the stored data can be easily detected. Thus, the burglar's claim can be verified by looking at attempts to tamper with the data, he said. However, the decentralization aspect of Blockchain technology can be a major issue when storing data from IoT devices.

Decentralization means that the computers used to store data might belong to different entities. In other words, if not implemented appropriately, there is a risk that users' sensitive data can now be by default stored by and available to third parties

A different possibility when using Blockchain in the IoT context is to store access logs and permissions. Specifically, the distributed and decentralization aspects of Blockchain make it notoriously expensive to store big data. An alternative is to keep the data in a central repository while storing logs concerning access to the data using Blockchain technology.

Thereafter, users have an immutable data structure that can tell who accessed their data and when that happened. Going one step further, Blockchain technology can be used to store data access permissions issued by users.

Any third-party requiring access to a user's data must request it first and such a request and response can be stored in the Blockchain. Now, users and data requesters have an immutable database that can unequivocally determine who has access to specific data and for long that access is valid. This application has a great potential to enhance privacy and even be the backbone of a data marketplace where users can profit from selling their own data

3.17 The Benefits of Blockchain and IoT

A Blockchain's distributed ledger is tamper-proof, eliminating the need for the involved parties to trust one another, said Andres Ricaurte, senior vice president and global head of payments at an IT services company. As such, no single party has control over the massive amount of data the IoT devices generate. Blockchain encryption makes it virtually impossible for anyone to overwrite existing data records. And using Blockchain to store IoT data adds another layer of security to prevent malicious attackers from gaining access to the network.

A primary challenge for IoT players is to protect the information in the entire IoT ecosystem, said Vipul Parekh, senior director with management consulting firm Alvarez & Marsal. Security vulnerabilities make IoT devices an easy target for distributed-denial-of-service attacks, malicious attackers and data breaches [11].

The integration of IoT and Blockchain opens the door for new possibilities that inherently reduce inefficiencies, enhance security and improve transparency

for all involved parties while enabling secured machine-to-machine transactions, Parekh said. The coupling of these technologies allows a physical asset to be tracked from the moment raw materials are mined, for example, and among every step of the supply chain until it is with the end consumer.

Parekh noted the following benefits of integrating Blockchain and IoT.

1. Enhanced security.

Blockchain technology incorporates security with the ability to verify and allow transactions originated by a trusted party as well as encryption while data is being transmitted and stored. Blockchain technology provides transparency about who has access, who is transacting and a record of all of the interactions. Plus, Blockchain adds a security layer in terms of encryption, the removal of single point of failure and the ability to quickly identify the weak link in the entire network.

2. Reduced costs.

By automating the transaction validation and processing steps on Blockchain, the entire ecosystem can be made proactive at a reduced cost.

3. Speed of transactions.

This is especially true for supply chain transactions with multiple suppliers, producers, distributors and consumers. With the Blockchain serving as a shared ledger to a degree, untrusted parties can exchange data directly with one another, eliminating the manual processes and increasing the speed of transactions.

The challenge for every technology is being clear about the customer problem or need that is being met, said John Rossman, managing partner at consulting firm Rossman Partners, former Amazon executive and author of «The Amazon Way: 14 Leadership Principles Behind the World's Most Disruptive Company»

«While at Amazon, we addressed this challenge with a technique called «working backwards' where we started with the customer and worked backwards to the solution» Rossman said. «Blockchain is an example that suffers from sounding like a transformational technology, but the meaningful adoption beyond cryptocurrencies has not met the hype. In figuring out how Blockchain can benefit the Internet of Things, let's start with the customer and work backwards»

There are many challenges in IoT deployments, including costs, security, privacy and data exchange. While these are separate issues, there are many dependencies to them, according to Rossman.

Customers of IoT, oftentimes a collaboration of business partners, need the data and insights from IoT devices quickly, at a performant cost basis, and they must be trustworthy. The Blockchain can be the backbone ledger helping with all of these.

Blockchain is encrypted and secure by design with many independent nodes verifying updates to the chain prior to updates to avoid nefarious actions, Rossman said. This is secure by design. The Blockchain can be inspected and verified by all parties, helping to improve both access and trust to the data without burdensome and costly bureaucratic layers. This greatly improves access, trust and cost.

3.18 Use Cases for Blockchain and IoT

The use cases for Blockchain and IoT include the following:

Supply chain/smart contracts IoT and Blockchain can be combined for quality assurance in the supply chain, said John Thielens, CTO of Cleo. Perishable goods, such as wine or rare foods, are typically subjected to varying temperatures and light exposures as they pass through transportation and warehousing networks. «By combining IoT and Blockchain, the journey of the perishable goods from producer to retailer can be captured» Thielens said. «Location and temperature data can be collected and incorporated into the Blockchain at the case or pallet level, enabling the ability to check the history of the product as it passes through the supply chain and reject accepting the product and moving it forward if the terms of the handling contract have been violated»

Other than storing data, some Blockchain models allow organizations to store and run immutable algorithms in a distributed and decentralized fashion, Carvahlo said. Often called smart contracts, these algorithms enable companies to encode business and domain rules naturally.

Consider a supply chain example where a product requires cold storage, Carvahlo said. «IoT devices, such as temperature sensors, can continuously monitor the temperature of packages and send data to a running smart contract, which can in real-time inform stakeholders of any temperature drop» Carvahlo said. «Since the smart contract is running on top of Blockchain, the underlying temperature data are stored in an immutable data structure, which helps prevent data tampering» [9], [10]

Truck leasing. IoT sensors placed in leased trucks can record key events on a Blockchain to help manage fleet whereabouts and returns and also to support more meaningful billing practices, according to the Gartner Inc. report «Integrating Blockchain With IoT Strengthens Trust in Multiparty Processes»

«With IoT sensors on board trucks, truck leasing companies can charge renters' fees based on the torque of the loads rather than on mileage, which is the current practice» the report noted. «The Blockchain distributed ledger technology supports a shared, single version of truth across participants. No single entity is in control of the data, and the truckers and leasing companies can all independently verify their own copy of the distributed ledger. This Blockchain/IoT integration should help the leasing companies increase revenue and cut costs»

Oil operations and field service. IoT sensors on oil and water wells can enable oil companies to manage the performance of hauling companies that pick up and deliver oil and water from the wells and transport them to various destinations, including environmental waste dumping grounds, according to the Garter report [10].

«The IoT sensors on the wells help the oil companies schedule truck pickups and allow them to monitor the amount of material picked up and delivered to eliminate fraud and false representations» the report noted. «[T]he Blockchain distributed ledger technology records key events in the logistics chain and supports a shared single version of independently verifiable truth across multiple participants»

In this use case, implementing Blockchain could help the oil companies save money and operate their pickup and delivery operations more efficiently, according to the Gartner report. In addition, by giving regulators a view into the data, such as the amount of water delivered to a water dumping ground as compared to the amount picked up from the water well, the Blockchain distributed ledger technology will help the oil company manage its compliance reporting requirements., Gartner noted.

3.19 Challenges of Integrating Blockchain Technology with IoT

One of the biggest challenges associated with integrating Blockchain and IoT revolves around the constraints associated with the limited battery life of some IoT devices, according to Paul Brody, global innovation leader, Blockchain technology at EY.

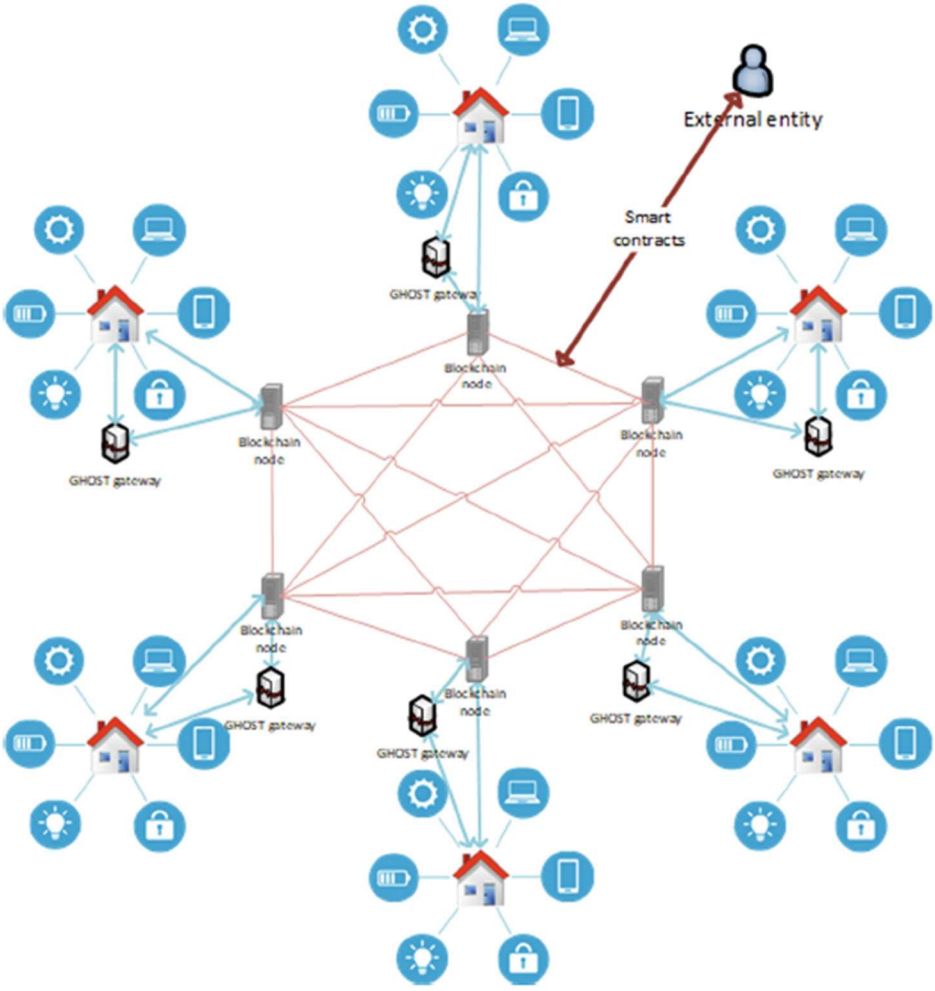

Figure 3.8 Smart Home systems in Network with Blockchain nodes

«Some IoT devices are connected to the power and Wi-Fi all the time, so you don't really have substantial constraints» he said. «But a lot of IoT devices aren't. And you can't have a compute- and bandwidth-intensive Blockchain transaction system going on a very, very small device. They may need to use some kind of server-based infrastructure or they may need to get help from a gateway device or related device. These ecosystems by their nature are going to have to be relatively cooperative ecosystems» [11], [12]

In addition, device security is only as good as the weakest link in the infrastructure, Brody said. «If I have a very sophisticated hack-resilient Blockchain network, but the operating system that my device runs on is poorly patched or isn't maintained or isn't updated, I've rendered all of that pointless and my device is easily hacked at the edge» he said.

3.20 Considerations

Blockchain and IoT can be an incredible combination, Parekh said. However, it is essential to note that Blockchain and IoT are not evolving at the same pace.

For example, Blockchain has such constraints as scalability to handle large amounts of data, regulatory and data privacy issues as well as standardization, which are all pre-requisites for enterprise adoption, according to Parekh. IoT technology also needs to prove that the infrastructure is secure, efficient and resilient. It still must overcome these constraints before new business solutions become staples in enterprise technology.

«In our observations, the client's willingness to adopt these technologies is not matched by the ability to deliver successful results» he said. «You need to equip leaders with an authentic understanding of the technologies to make the right decisions and avoid «a hammer looking for a nail scenario' because not every [IoT] use case is made for Blockchain. We suggest performing a business feasibility assessment to ascertain the benefits of removing intermediaries, e.g., cost, speed, reliance on market participants in completing transactions as well as the trust needed to share and maintain data integrity among participants» [11]

3.21 Convenience is prioritized over security

Connected devices are designed principally for users' convenience: they enable easy network access, which is usually automatic or by entering user credentials. This allows people to use their devices easily from anywhere in the world. At the same time, this opens numerous doors for cybercriminals, who can access internet-connected devices and steal personal information, such as financial data or sensitive medical information.

Paradoxically, most consumers are aware of these vulnerabilities of IoT devices and yet are willing to sacrifice security for the sake of convenience. Probably the most notable example of this trade-off is smart speakers often used in IoT home automation, such as Amazon Echo and Google Home. Although both companies' employees admittedly listen to users' conversations for the purpose of improving the services, this barely impacted the sales figures of these devices.

Security is secondary to profit-making. For example, a couple living in Milwaukee has suffered a privacy-breach incident that reminds a scene from a horror movie. A cybercriminal took over their smart home system, played

disturbing music loudly, talked to them via a camera, and changed the room temperature to 32 degrees Celsius. Although this was a relatively harmless act, such incidents are becoming more common and should raise major red flags. At the end of the day, a regular consumer's privacy is a low-hanging fruit for hackers. Until users' information is stolen and misused, most consumers seem to be not bothered at all.

From a business perspective, time to market is a critical metric in today's competitive reality. Unfortunately, ensuring stability and security of the devices comes second. For example, the Global Print Security Landscape report reveals that in 2019 an astounding 60% of businesses in the UK, France, and Germany have been hacked through printers, which led to more than $400,000 in losses.

3.22 The centralized IoT network model

Currently, IoT uses a client/server model, or a centralized model of networking. IoT devices use a single gateway to transfer data between them and connect through a cloud server. This model has been utilized over the last decades, but it is no longer suitable for the increasing number of IoT devices and the volumes of data they share. The centralized architecture has a number of shortcomings:

1. High costs of centralized cloud maintenance and networking equipment. The costs will continue to rise with the proliferation of connected devices.
2. Low interoperability due to restricted data exchange with other centralized infrastructures.
3. Single gateway is not trustworthy, as it allows gaining access to a whole IoT network by compromising a single device.

The Mirai incident is one of the examples proving that the centralized model is not reliable. Being the largest DDoS attack ever, Mirai caused a temporary failure of many popular websites, including Amazon, Reddit, CNN, Netflix, the Guardian, Twitter, Spotify, and GitHub. The Mirai botnet first attacked Dyn, a popular DNS provider, and then the internet's biggest websites through the unprotected network. As a result, the companies lost millions of dollars and their reputation was compromised [12].

The following features make Blockchain an effective weapon in combating IoT cyberthreats.

1. Decentralization

In a Blockchain ledger, data is stored on various nodes all over the world, which eliminates the single point of failure. Before adding any data to the network, all nodes must approve and verify it. Thus, no change is allowed without a common agreement from all of the network participants. This approach is named peer to peer communication and is intended to protect Blockchain transactions from malicious parties. Since there is no single server, there is no chance of a man in the middle attack, when hackers can grab the information sent between a server and a device.

2. Public access

Blockchain is public, which means that it's accessible to everyone in the network. All network participants can see the common history of stored blocks and transactions, but they need a private key to see the content. This gives a complete transparency to all operations and keeps data safe at the same time. Once a piece of information is stored on a Blockchain, it is impossible to change it.

3. Secure data

Blockchain uses advanced encryption algorithms to secure data, which makes it more private. This is done primarily for financial operations to be carried out without risks. Using the Blockchain model, IoT devices may send and receive messages in the same way as financial transactions to enable secure data communication between connected things.

3.23 Examples of Blockchain mechanisms for IoT security

The application of Blockchain in IoT security enables a direct information sharing between connected devices instead of communication via a centralized network, thus decreasing the susceptibility of IoT to cyber-threats. Currently, the highest rate of Blockchain adoption among IoT-enabled businesses in the US is seen in pharmaceuticals, transportation and energy sectors, according to a Gartner survey. All these industries rely on transportation of physical goods, and the majority of companies that have successfully adopted Blockchain are veterans of the IoT industry.

Perhaps the most promising way of successfully combining the two technologies is to install chips in every IoT device. For example, the alliance of Ubirch, a Blockchain-anchoring security specialist, G+D Mobile Security, and IoT carrier 1NCE has developed an IoT security service that leverages the power of

Blockchain and sensor-embedded chips to significantly increase security. Data no longer travels from sensors to the cloud to be approved, which single-handedly eliminates the possibility of the «man in the middle' type of hacking attacks. Now the information is sealed by a private key directly on the device and is anchored in a public Blockchain, which means that data about every access to a particular sensor is forever recorded on a ledger. Adopting smart contracts for this purpose also opens up more opportunities for enhancing enterprise cybersecurity.

Modum.io, a Zurich-based startup, combines IoT with Blockchain to help Swiss Post track the temperature of heat-sensitive packages. Temperature-sensitive cargo is a major concern for logistics companies. Modum.io has solved the problem by developing the MODsense T temperature logger, which automatically reports temperature each time the packet is scanned along the journey. Not only it protects customers, but it also allows Swiss Post to gain insight into how exactly temperature-related problems occur. The data about temperature fluctuations is recorded to the Blockchain, which ensures that data cannot be manipulated. Watch the video below to see the technology in action.

Sophisticated chips, sensors, and actuators in cars, industrial robots, or programmable logic controllers (PLCs) transmit data to the Industrial Internet of Things (IIoT) network. Distributed computing resources can use this data to convert insights into action, impacting business processes, and new ways of working. Various technical and security concerns remain unaddressed, but that's changing.

Security is a significant concern with IoT that has slowed its deployment in critical application areas. Various IoT devices demonstrate security vulnerabilities. They become an easy target for DDoS attacks (Distributed Denial of Service). In this scenario, several compromised computer systems bombard a target, such as a central server with a vast volume of simultaneous data requests. Following that, legitimate users are denied access to the service.

Another issue is that of scalability. As the number of devices connected through an IoT network grows, current centralized systems to authenticate, authorize, and connect different nodes in a network will turn into a bottleneck. To fix this, huge investments were necessary to deploy servers that can handle the information exchange, and the entire network can go down if the server becomes unavailable.

Another breakthrough technology could potentially address some of the IoT security and scalability challenges: Blockchain, which is deemed to be an

information game-changer. At its core, a Blockchain system consists of a distributed digital ledger, shared between participants in the system, that resides on the internet. Transactions or events are validated and recorded in the ledger and cannot subsequently be amended or removed. It provides a way for information to be registered and shared by a community of users. Within this community, selected members maintain their copy of the ledger and must validate any new transactions collectively through a consensus process before they are accepted on to the ledger.

3.24 Built-in Security

A Blockchain is a decentralized and distributed digital ledger used to record transactions across many computers so that any record involved can't (easily) be altered retroactively without altering all subsequent blocks. This allows the participants to verify and audit transactions independently. A Blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. Depending on the use case, people or machines and devices can trigger Blockchain transactions. Typically, all participants can access and verify all data, including the full history of a Blockchain. In many applications, this eliminates the need for a central trusted authority and trust between the participants. Authentication takes place by mass collaboration that's in turn powered by collective self-interests. In terms of cryptocurrency, a Blockchain confirms that each unit of value is transferred only once, solving double spending.

A Blockchain network can be built several ways. They can be public, private, permissioned, or implemented by a consortium. A public Blockchain is one that anyone can join and participate in, such as Bitcoin. Drawbacks might include substantial computational power required, little or no privacy for transactions, and weak security. These are essential considerations for enterprise use cases of Blockchain.

A private Blockchain network is a decentralized peer-to-peer network, with the significant difference that it's governed by one organization. That organization controls who is allowed to participate in the network, execute a consensus protocol, and maintain the shared ledger. Depending on the use case, this can significantly boost trust and confidence between participants. A private Blockchain can be run behind a corporate firewall and even be hosted on-premises.

Businesses who set up a private Blockchain will generally set up a permissioned Blockchain network. It is important to note that public Blockchain

networks can also be permissioned. This places restrictions on who is allowed to participate in the network, and only in certain transactions. Participants need to obtain an invitation or permission to join.

Multiple organizations can share the responsibilities of maintaining a Blockchain. These pre-selected organizations determine who can submit transactions or access the data. A consortium Blockchain is ideal for business when all participants need to be permissioned and have a shared responsibility for the Blockchain.

3.25 Securing a Network

Blockchain can enable the fast processing of transactions and coordination among billions of connected devices. As the number of interconnected devices grows, the distributed ledger technology provides a viable solution to support a large number of transactions.

As the distributed ledger in a Blockchain system is tamper-proof, trust verification is not needed for the most part among the involved parties. Going beyond the authentication issue, Blockchain can also store IoT data. This adds another layer of security that hackers would need to bypass if they want to access the network. Blockchain provides a much more robust encryption level that makes it virtually impossible to overwrite existing data records.

Should the network be compromised, Blockchain's built-in transparency provides a reliable way to identify a specific source of data leakages and take remedial action. Anyone who is authorized to access the network can track the transactions that happened in the past.

A few organizations are dedicated to IoT and Blockchain. The most famous is IOTA, a protocol for fast transaction settlement and data integrity, with a Tangle ledger that eliminates the need for expensive mining (validation of transactions). IOTA is a promising infrastructure for IoT devices that need to process large amounts of microdata. Features of the Tangle ledger, the distributed ledger that supports IOTA, are machine-to-machine communication, fee-less micropayments, and quantum-resistant data.

Another player is Chain of Things (CoT), a consortium of technologists and Blockchain companies. It investigates the best possible use cases where a combination of Blockchain and IoT can offer significant benefits to industrial,

environmental, and humanitarian applications. So far, CoT has built Maru, an integrated Blockchain and IoT hardware solution to solve issues with identity, security, and interoperability. Three developed use cases are available and named Chain of Security, Chain of Solar, and Chain of Shipping.

Riddle&Code provides cryptographic tagging solutions for Blockchains in smart logistics and supply chain management. Working on the integration between IoT devices and distributed ledger networks, Riddle&Code offers a combined, patented hardware and software solution that enables secure and trusted interaction with machines in the IoT age by giving physical devices a trusted digital identity. This technology breaks through the physical/digital divide to balance the demand for paper documentation and the advantages that Blockchain technology offers.

Combining IoT sensors with Blockchain technology, Modum.io provides data integrity for transactions involving physical products. Modum sensors record environmental conditions, such as temperature, that goods are subject to while in transit. When the goods arrive at the next transit point or end customer, the sensor data is verified against predetermined conditions in a smart contract on the Blockchain. The contract validates that the terms meet all of the requirements set out by the sender, their clients, or a regulator and triggers various actions such as notifications to sender and receiver, payment, or release of goods.

3.26 Hardware security

The typical entry point for malicious entities is the same as that for good ones: Access credentials are generally regarded as the weakest areas.

The success of a Blockchain system hinges on secured user access to the distributed database. If an attacker gains access to another user's highly confidential credentials, the attacker would have full control over that Blockchain account (currency, assets, ID, contracts, etc.). Similarly, if users lose their credentials, they lose access to all Blockchain assets and can no longer use or valorize them. Additionally, transactions and operations stored in a Blockchain cannot be simply undone. Hardware-based security tokens are one effective way against attacks and unauthorized access.

Storing Blockchain user credentials on a computer or a cellphone is extremely risky as an attacker might identify and read confidential information. This could even be done remotely utilizing software attacks. Integrating a dedicated Hardware Security Module (HSM) into the device microcontroller can

significantly enhance security. This separates critical operations and credential storage from other software operations and therefore provides robust protection against software attacks.

3.27 Blockchain Security

Blockchain is a specific type of database. It differs from a typical database in the way it stores information; Blockchains store data in blocks that are then chained together. As new data comes in it is entered into a fresh block. Once the block is filled with data it is chained onto the previous block, which makes the data chained together in chronological order.

Different types of information can be stored on a Blockchain but the most common use so far has been as a ledger for transactions. In Bitcoin's case, Blockchain is used in a decentralized way so that no single person or group has control, rather, all users collectively retain control.

Decentralized Blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, this means that transactions are permanently recorded and viewable to anyone.

3.28 Storage Structure

One key difference between a typical database and a Blockchain is the way the data is structured. A Blockchain collects information together in groups, also known as blocks, that hold sets of information. Blocks have certain storage capacities and, when filled, are chained onto the previously filled block, forming a chain of data known as the «Blockchain» All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled.

A database structures its data into tables whereas a Blockchain, like its name implies, structures its data into chunks (blocks) that are chained together. This makes it so that all Blockchains are databases but not all databases are Blockchains. This system also inherently makes an irreversible timeline of data when implemented in a decentralized nature. When a block is filled it is set in stone and becomes a part of this timeline. Each block in the chain is given an exact timestamp when it is added to the chain.

3.29 Decentralization

For the purpose of understanding Blockchain, it is instructive to view it in the context of how it has been implemented by Bitcoin. Like a database, Bitcoin needs a collection of computers to store its Blockchain. For Bitcoin, this Blockchain is just a specific type of database that stores every Bitcoin transaction ever made. In Bitcoin's case, and unlike most databases, these computers are not all under one roof, and each computer or group of computers is operated by a unique individual or group of individuals.

Imagine that a company owns a server comprised of 10,000 computers with a database holding all of its client's account information. This company has a warehouse containing all of these computers under one roof and has full control of each of these computers and all the information contained within them. Similarly, Bitcoin consists of thousands of computers, but each computer or group of computers that hold its Blockchain is in a different geographic location and they are all operated by separate individuals or groups of people. These computers that makeup Bitcoin's network are called nodes.

In this model, Bitcoin's Blockchain is used in a decentralized way. However, private, centralized Blockchains, where the computers that make up its network are owned and operated by a single entity, do exist.

In a Blockchain, each node has a full record of the data that has been stored on the Blockchain since its inception. For Bitcoin, the data is the entire history of all Bitcoin transactions. If one node has an error in its data it can use the thousands of other nodes as a reference point to correct itself. This way, no one node within the network can alter information held within it. Because of this, the history of transactions in each block that make up Bitcoin's Blockchain is irreversible.

If one user tampers with Bitcoin's record of transactions, all other nodes would cross-reference each other and easily pinpoint the node with the incorrect information. This system helps to establish an exact and transparent order of events. For Bitcoin, this information is a list of transactions, but it also is possible for a Blockchain to hold a variety of information like legal contracts, state identifications, or a company's product inventory.

In order to change how that system works, or the information stored within it, a majority of the decentralized network's computing power would need to agree on said changes. This ensures that whatever changes do occur are in the best interests of the majority.

3.30 Transparency

Because of the decentralized nature of Bitcoin's Blockchain, all transactions can be transparently viewed by either having a personal node or by using Blockchain explorers that allow anyone to see transactions occurring live. Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and added. This means that if you wanted to, you could track Bitcoin wherever it goes.

For example, exchanges have been hacked in the past where those who held Bitcoin on the exchange lost everything. While the hacker may be entirely anonymous, the Bitcoins that they extracted are easily traceable. If the Bitcoins that were stolen in some of these hacks were to be moved or spent somewhere, it would be known.

3.31 More about security of a Blockchain

Blockchain technology accounts for the issues of security and trust in several ways. First, new blocks are always stored linearly and chronologically. That is, they are always added to the «end» of the Blockchain. If you take a look at Bitcoin's Blockchain, you'll see that each block has a position on the chain, called a «height» As of November 2020, the block's height had reached 656,197 blocks so far.

After a block has been added to the end of the Blockchain, it is very difficult to go back and alter the contents of the block unless the majority reached a consensus to do so. That's because each block contains its own hash, along with the hash of the block before it, as well as the previously mentioned time stamp. Hash codes are created by a math function that turns digital information into a string of numbers and letters. If that information is edited in any way, the hash code changes as well.

Here's why that's important to security. Let's say a hacker wants to alter the Blockchain and steal Bitcoin from everyone else. If they were to alter their own single copy, it would no longer align with everyone else's copy. When everyone else cross-references their copies against each other, they would see this one copy stand out and that hacker's version of the chain would be cast away as illegitimate.

Succeeding with such a hack would require that the hacker simultaneously control and alter 51% of the copies of the Blockchain so that their new copy becomes the majority copy and thus, the agreed-upon chain. Such an attack would

also require an immense amount of money and resources as they would need to redo all of the blocks because they would now have different timestamps and hash codes.

Due to the size of Bitcoin's network and how fast it is growing, the cost to pull off such a feat would probably be insurmountable. Not only would this be extremely expensive, but it would also likely be fruitless. Doing such a thing would not go unnoticed, as network members would see such drastic alterations to the Blockchain. The network members would then fork off to a new version of the chain that has not been affected.

This would cause the attacked version of Bitcoin to plummet in value, making the attack ultimately pointless as the bad actor has control of a worthless asset. The same would occur if the bad actor were to attack the new fork of Bitcoin. It is built this way so that taking part in the network is far more economically incentivized than attacking it.

3.32 Bitcoin vs. Blockchain

The goal of Blockchain is to allow digital information to be recorded and distributed, but not edited. Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn't until almost two decades later, with the launch of Bitcoin in January 2009, that Blockchain had its first real-world application.

The Bitcoin protocol is built on a Blockchain. In a research paper introducing the digital currency, Bitcoin's pseudonymous creator, Satoshi Nakamoto, referred to it as «a new electronic cash system that's fully peer-to-peer, with no trusted third party»

The key thing to understand here is that Bitcoin merely uses Blockchain as a means to transparently record a ledger of payments, but Blockchain can, in theory, be used to immutably record any number of data points. As discussed above, this could be in the form of transactions, votes in an election, product inventories, state identifications, deeds to homes, and much more.

Currently, there is a vast variety of Blockchain-based projects looking to implement Blockchain in ways to help society other than just recording transactions. One good example is that of Blockchain being used as a way to vote

in democratic elections. The nature of Blockchain's immutability means that fraudulent voting would become far more difficult to occur.

For example, a voting system could work such that each citizen of a country would be issued a single cryptocurrency or token. Each candidate would then be given a specific wallet address, and the voters would send their token or crypto to whichever candidate's address they wish to vote for. The transparent and traceable nature of Blockchain would eliminate the need for human vote counting as well as the ability of bad actors to tamper with physical ballots.

3.33 Blockchain vs. Banks

Banks and decentralized Blockchains are vastly different. To see how a bank differs from Blockchain, let's compare the banking system to Bitcoin's implementation of Blockchain.

3.33.1 Usage of Blockchain

As we now know, blocks on Bitcoin's Blockchain store data about monetary transactions. But it turns out that Blockchain is actually a reliable way of storing data about other types of transactions, as well.

Some companies that have already incorporated Blockchain include Walmart, Pfizer, AIG, Siemens, Unilever, and a host of others. For example, IBM has created its Food Trust Blockchain1п»ї to trace the journey that food products take to get to its locations.

Why do this? The food industry has seen countless outbreaks of e Coli, salmonella, listeria, as well as hazardous materials being accidentally introduced to foods. In the past, it has taken weeks to find the source of these outbreaks or the cause of sickness from what people are eating.

Using Blockchain gives brands the ability to track a food product's route from its origin, through each stop it makes, and finally its delivery. If a food is found to be contaminated then it can be traced all the way back through each stop to its origin. Not only that, but these companies can also now see everything else it may have come in contact with, allowing the identification of the problem to occur far sooner, potentially saving lives. This is one example of Blockchains in practice, but there are many other forms of Blockchain implementation.

3.33.2 Banking and finance

Perhaps no industry stands to benefit from integrating Blockchain into its business operations more than banking. Financial institutions only operate during business hours, five days a week. That means if you try to deposit a check on Friday at 6 p.m., you will likely have to wait until Monday morning to see that money hit your account. Even if you do make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps.

By integrating Blockchain into banks, consumers can see their transactions processed in as little as 10 minutes,2п»ї basically the time it takes to add a block to the Blockchain, regardless of holidays or the time of day or week. With Blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. In the stock trading business, for example, the settlement and clearing process can take up to three days (or longer, if trading internationally), meaning that the money and shares are frozen for that period of time.

Given the size of the sums involved, even the few days that the money is in transit can carry significant costs and risks for banks. European bank Santander and its research partners put the potential savings at $15 billion to $20 billion a year.3п»ї Capgemini, a French consultancy, estimates that consumers could save up to $16 billion in banking and insurance fees each year4п»ї through Blockchain-based applications.

3.33.3 Currency

Blockchain forms the bedrock for cryptocurrencies like Bitcoin. The U.S. dollar is controlled by the Federal Reserve. Under this central authority system, a user’s data and currency are technically at the whim of their bank or government. If a user’s bank is hacked, the client’s private information is at risk. If the client’s bank collapses or they live in a country with an unstable government, the value of their currency may be at risk. In 2008, some of the banks that ran out of money were bailed out partially using taxpayer money. These are the worries out of which Bitcoin was first conceived and developed.

By spreading its operations across a network of computers, Blockchain allows Bitcoin and other cryptocurrencies to operate without the need for a central authority. This not only reduces risk but also eliminates many of the processing

and transaction fees. It can also give those in countries with unstable currencies or financial infrastructures a more stable currency with more applications and a wider network of individuals and institutions they can do business with, both domestically and internationally.

Using cryptocurrency wallets for savings accounts or as a means of payment is especially profound for those who have no state identification. Some countries may be war-torn or have governments that lack any real infrastructure to provide identification. Citizens of such countries may not have access to savings or brokerage accounts and therefore, no way to safely store wealth.

3.33.4 Healthcare

Health care providers can leverage Blockchain to securely store their patients' medical records. When a medical record is generated and signed, it can be written into the Blockchain, which provides patients with the proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the Blockchain with a private key, so that they are only accessible by certain individuals, thereby ensuring privacy.

3.33.5 Records of Property

If you have ever spent time in your local Recorder's Office, you will know that the process of recording property rights is both burdensome and inefficient. Today, a physical deed must be delivered to a government employee at the local recording office, where it is manually entered into the county's central database and public index. In the case of a property dispute, claims to the property must be reconciled with the public index.

This process is not just costly and time-consumingвЂ”it is also riddled with human error, where each inaccuracy makes tracking property ownership less efficient. Blockchain has the potential to eliminate the need for scanning documents and tracking down physical files in a local recording office. If property ownership is stored and verified on the Blockchain, owners can trust that their deed is accurate and permanently recorded.

In war-torn countries or areas that have little to no government or financial infrastructure, and certainly no «Recorder's Office» it can be nearly impossible to prove ownership of a property. If a group of people living in such an area is able to

leverage Blockchain, transparent and clear timelines of property ownership could be established.

3.33.6 Smart Contracts

A smart contract is a computer code that can be built into the Blockchain to facilitate, verify, or negotiate a contract agreement. Smart contracts operate under a set of conditions that users agree to. When those conditions are met, the terms of the agreement are automatically carried out.

Say, for example, a potential tenant would like to lease an apartment using a smart contract. The landlord agrees to give the tenant the door code to the apartment as soon as the tenant pays the security deposit. Both the tenant and the landlord would send their respective portions of the deal to the smart contract, which would hold onto and automatically exchange the door code for the security deposit on the date the lease begins. If the landlord doesn't supply the door code by the lease date, the smart contract refunds the security deposit. This would eliminate the fees and processes typically associated with the use of a notary, third-party mediator, or attorneys.

3.33.7 Supply Chains

As in the IBM Food Trust example, suppliers can use Blockchain to record the origins of materials that they have purchased. This would allow companies to verify the authenticity of their products, along with such common labels as «Organic» «Local» and «Fair Trade»

As reported by Forbes, the food industry is increasingly adopting the use of Blockchain to track the path and safety of food throughout the farm-to-user journey.

3.33.8 Voting

As mentioned, Blockchain could be used to facilitate a modern voting system. Voting with Blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia. Using Blockchain in this way would make votes nearly impossible to tamper with. The Blockchain protocol would also maintain transparency in the

electoral process, reducing the personnel needed to conduct an election and providing officials with nearly instant results. This would eliminate the need for recounts or any real concern that fraud might threaten the election.

3.34 Advantages and Disadvantages of Blockchain

For all of its complexity, Blockchain's potential as a decentralized form of record-keeping is almost without limit. From greater user privacy and heightened security to lower processing fees and fewer errors, Blockchain technology may very well see applications beyond those outlined above. But there are also some disadvantages.

Pros

- Improved accuracy by removing human involvement in verification
- Cost reductions by eliminating third-party verification
- Decentralization makes it harder to tamper with
- Transactions are secure, private, and efficient
- Transparent technology

Provides a banking alternative and way to secure personal information for citizens of countries with unstable or underdeveloped governments

Cons

- Significant technology cost associated with mining bitcoin
- Low transactions per second
- History of use in illicit activities
- Regulation

3.34.1 Advantages of Blockchain

1. Accuracy of the Chain

Transactions on the Blockchain network are approved by a network of thousands of computers. This removes almost all human involvement in the verification process, resulting in less human error and an accurate record of

information. Even if a computer on the network were to make a computational mistake, the error would only be made to one copy of the Blockchain. In order for that error to spread to the rest of the Blockchain, it would need to be made by at least 51% of the network's computers near impossibility for a large and growing network the size of Bitcoin's.

2. Cost Reductions

Typically, consumers pay a bank to verify a transaction, a notary to sign a document, or a minister to perform a marriage. Blockchain eliminates the need for third-party verification and, with it, their associated costs. Business owners incur a small fee whenever they accept payments using credit cards, for example, because banks and payment processing companies have to process those transactions. Bitcoin, on the other hand, does not have a central authority and has limited transaction fees.

3. Decentralization

Blockchain does not store any of its information in a central location. Instead, the Blockchain is copied and spread across a network of computers. Whenever a new block is added to the Blockchain, every computer on the network updates its Blockchain to reflect the change. By spreading that information across a network, rather than storing it in one central database, Blockchain becomes more difficult to tamper with. If a copy of the Blockchain fell into the hands of a hacker, only a single copy of the information, rather than the entire network, would be compromised.

4. Efficient Transactions

Transactions placed through a central authority can take up to a few days to settle. If you attempt to deposit a check on Friday evening, for example, you may not actually see funds in your account until Monday morning. Whereas financial institutions operate during business hours, five days a week, Blockchain is working 24 hours a day, seven days a week, and 365 days a year. Transactions can be completed in as little as ten minutes and can be considered secure after just a few hours. This is particularly useful for cross-border trades, which usually take much longer because of time-zone issues and the fact that all parties must confirm payment processing.

5. Private Transactions

Many Blockchain networks operate as public databases, meaning that anyone with an internet connection can view a list of the network's transaction

history. Although users can access details about transactions, they cannot access identifying information about the users making those transactions. It is a common misperception that Blockchain networks like bitcoin are anonymous, when in fact they are only confidential.

That is, when a user makes public transactions, their unique code called a public key, is recorded on the Blockchain, rather than their personal information. If a person has made a Bitcoin purchase on an exchange that requires identification then the person's identity is still linked to their Blockchain address, but a transaction, even when tied to a person's name, does not reveal any personal information.

6. Secure Transactions

Once a transaction is recorded, its authenticity must be verified by the Blockchain network. Thousands of computers on the Blockchain rush to confirm that the details of the purchase are correct. After a computer has validated the transaction, it is added to the Blockchain block. Each block on the Blockchain contains its own unique hash, along with the unique hash of the block before it. When the information on a block is edited in any way, that block's hash code changes, however, the hash code on the block after it would not. This discrepancy makes it extremely difficult for information on the Blockchain to be changed without notice.

7. Transparency

Most Blockchains are entirely open-source software. This means that anyone and everyone can view its code. This gives auditors the ability to review cryptocurrencies like Bitcoin for security. This also means that there is no real authority on who controls Bitcoin's code or how it is edited. Because of this, anyone can suggest changes or upgrades to the system. If a majority of the network users agree that the new version of the code with the upgrade is sound and worthwhile then Bitcoin can be updated.

8. Banking the Unbanked

Perhaps the most profound facet of Blockchain and Bitcoin is the ability for anyone, regardless of ethnicity, gender, or cultural background, to use it. According to the world bank there are nearly 2 billion adults that do not have bank accounts or any means of storing their money or wealth.5п»ї Nearly all of these individuals live in developing countries where the economy is in its infancy and entirely dependent on cash.

These people often earn little money that is paid in physical cash. They then need to store this physical cash in hidden locations in their homes or places of living leaving them subject to robbery or unnecessary violence. Keys to a bitcoin wallet can be stored on a piece of paper, a cheap cell phone, or even memorized if necessary. For most people, it is likely that these options are more easily hidden than a small pile of cash under a mattress.

Blockchains of the future are also looking for solutions to not only be a unit of account for wealth storage, but also to store medical records, property rights, and a variety of other legal contracts.

3.34.2 Disadvantages of Blockchain

While there are significant upsides to the Blockchain, there are also significant challenges to its adoption. The roadblocks to the application of Blockchain technology today are not just technical. The real challenges are political and regulatory, for the most part, to say nothing of the thousands of hours (read: money) of custom software design and back-end programming required to integrate Blockchain to current business networks. Here are some of the challenges standing in the way of widespread Blockchain adoption.

1. Technology Cost

Although Blockchain can save users money on transaction fees, the technology is far from free. The «proof of work» system that bitcoin uses to validate transactions, for example, consumes vast amounts of computational power. In the real world, the power from the millions of computers on the bitcoin network is close to what Denmark consumes annually. Assuming electricity costs of $0.03~$0.05 per kilowatt-hour, mining costs exclusive of hardware expenses are about $5,000~$7,000 per coin.10

Despite the costs of mining bitcoin, users continue to drive up their electricity bills in order to validate transactions on the Blockchain. That’s because when miners add a block to the bitcoin Blockchain, they are rewarded with enough bitcoin to make their time and energy worthwhile. When it comes to Blockchains that do not use cryptocurrency, however, miners will need to be paid or otherwise incentivized to validate transactions.

Some solutions to these issues are beginning to arise. For example, bitcoin mining farms have been set up to use solar power, excess natural gas from fracking sites, or power from wind farms.

2. Speed Inefficiency

Bitcoin is a perfect case study for the possible inefficiencies of Blockchain. Bitcoin's «proof of work» system takes about ten minutes to add a new block to the Blockchain. At that rate, it's estimated that the Blockchain network can only manage about seven transactions per second (TPS). Although other cryptocurrencies such as Ethereum perform better than bitcoin, they are still limited by Blockchain. Legacy brand Visa, for context, can process 24,000 TPS.

Solutions to this issue have been in development for years. There are currently Blockchains that are boasting over 30,000 transactions per second.

3. Illegal Activity

While confidentiality on the Blockchain network protects users from hacks and preserves privacy, it also allows for illegal trading and activity on the Blockchain network. The most cited example of Blockchain being used for illicit transactions is probably the Silk Road, an online «dark web» drug marketplace operating from February 2011 until October 2013 when it was shut down by the FBI.

The website allowed users to browse the website without being tracked using the Tor browser and make illegal purchases in Bitcoin or other cryptocurrencies. Current U.S. regulations require financial service providers to obtain information about their customers when they open an account, verify the identity of each customer, and confirm that customers do not appear on any list of known or suspected terrorist organizations. This system can be seen as both a pro and a con. It gives anyone access to financial accounts but also allows criminals to more easily transact. Many have argued that the good uses of crypto, like banking the unbanked world, outweigh the bad uses of cryptocurrency, especially when most illegal activity is still accomplished through untraceable cash.

4. Regulation

Many in the crypto space have expressed concerns about government regulation over cryptocurrencies. While it is getting increasingly difficult and near impossible to end something like Bitcoin as its decentralized network grows, governments could theoretically make it illegal to own cryptocurrencies or participate in their networks.

Over time this concern has grown smaller as large companies like PayPal begin to allow the ownership and use of cryptocurrencies on its platform.

3.35 The next of Blockchain

First proposed as a research project in 1991,7п»ї Blockchain is comfortably settling into its late twenties. Like most millennials its age, Blockchain has seen its fair share of public scrutiny over the last two decades, with businesses around the world speculating about what the technology is capable of and where it’s headed in the years to come.

With many practical applications for the technology already being implemented and explored, Blockchain is finally making a name for itself at age twenty-seven, in no small part because of bitcoin and cryptocurrency. As a buzzword on the tongue of every investor in the nation, Blockchain stands to make business and government operations more accurate, efficient, secure, and cheap with fewer middlemen.

CHAPTER IV. EXAMPLE SIMPLE BLOCKCHAIN PROJECT

I have divided the process of building a Blockchain into several steps for better understanding. These steps are as follows:

- Step 1: Creating a Blockchain class
- Step 2: Writing a Function to build New Blocks
- Step 3: Writing Functions to create New Transactions and get the Last Block
- Step 4: Writing a Function to "Hash" the Blocks
- Step 5: Creating a New Blockchain and Sending some money

4.1 Creating a Blockchain class

I will start by importing the required libraries. In this case, I will be needing the hashlib library for the encryption, the JSON library for our blocks formatting, and the time library for the timestamp of each block. I will then be creating a class and initializing the following variables:

chain: This will be an empty list to which I will add blocks. Quite literally, the 'Blockchain'.

pendingTransactions: When users send the coins to each other, their transactions will locate in this array until I approve and insert them into a new block.

newBlock: This is a method that I will define soon, and I will utilize it in order to include each block in the chain.

Example:

```python
import hashlib
import json
from time import time

# creating the Block_chain class
```

```
class Block_chain(object):
   def __init__(self):
                        self.chain = []
                        self.pendingTransactions = []


                        self.newBlock(previousHash = "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks», the_proof = 100)
```

In the above snippet of code, we have imported the required libraries and created the Block_chain class where we initialized the different variables described earlier.

4.2 Writing a Function to construct New Blocks

Now that we have initialized an empty chain, let us begin inserting blocks into it. We will then define the JSON object with the following properties:

index: Taking the length of the Blockchain and adding 1 to it. We will use this to reference an individual block, so for instance, the genesis block has index = 1.

timestamp: With the help of the time() module, we will stamp the block when it's created. Users can now check when their transaction was confirmed on-chain.

transactions: Any transactions that have been in the 'pending' list will be displayed in the new block.

proof: This property comes from the miner who thinks they found a valid 'proof' or 'nonce'.

previous_hash: A hashed version of the most recent approved block.

Once we add the above properties to the new block, we will include them in the chain. Initially, we empty the pending list of transactions and then add the new block to the self.chain and return it.

```python
# Creating a new block listing key/value pair of
```

```
# block information in a JSON object.
# Reset the list of pending transactions &
# append the newest block to the chain.
        def newBlock(self, the_proof, previousHash = None):
                the_block = {
                        'index': len(self.chain) + 1,
                        'timestamp': time(),
                        'transactions': self.pendingTransactions,
                        'proof': the_proof,
                        'previous_hash': previousHash or self.hash(self.chain[-1]),
                }
                self.pendingTransactions = []
                self.chain.append(the_block)


                return the_block
```

In the above snippet of code, we have defined the newBlock function and included the properties described earlier. We emptied the pending list of transactions and added the new block to the chain. At last, we have returned the new block.

4.3 Create New Transactions and Get the Last Block

Now, let us include the list of transactions in the program because this whole program is quite pointless without one. So, let us first define a method that returns the block that was added most recently (we will use this in a second for the new index).

After that, we will create another method to represent a new transaction. This method will consist of the three most significant variables - the_sender, the_recipient, and the_amount. Without these variables included in every

transaction, the users cannot spend, earn, or buy things with the newly produced cryptocurrency. Remember that these transactions are over-simplified and do not reflect the things one may find in a true cryptocurrency.

We will include the the_transaction JSON object to the pool of pendingTransactions. These will stay in an indetermination state until a new block is mined and added to the Blockchain. And for future reference, we will return the index of the block to which the new transaction is about to be added.

```python
#Searching the Blockchain for the most recent block.
@property
def lastBlock(self):
    return self.chain[-1]


# Adding a transaction with relevant info to the 'blockpool' - list of pending transactions.
def newTransaction(self, the_sender, the_recipient, the_amount):
    the_transaction = {
        'sender': the_sender,
        'recipient': the_recipient,
        'amount': the_amount
    }
    self.pendingTransactions.append(the_transaction)
    return self.lastBlock['index'] + 1
```

In the above snippet of code, we defined the method as lastBlock(), which returns the most recent block added. We have then defined the function as newTransaction(), within which we have defined the JSON object as the_transaction and included the addresses to the sender, recipient, and amount. We added this JSON object to the pendingTransaction and returned the last block.

4.4 Writing a Function to "Hash" the Blocks

Now, let us add Cryptography to the program. As we know, Bitcoin and many other Blockchains utilize SHA-256, an encryption hash function, which accepts some text string (stored as a Unicode value) and spits out a 64-character long encrypted string. In a Blockchain, the text that we encrypt is considered a block. For instance, the encrypted string, or "hash", of the Bitcoin genesis block appears like this:

fbc13b85c4ade52e2def26eae950f3b55b174df887ad0f0fb5ebfd56881f7fcb

Blockchains are considered tamper-proof as every block consists of a copy of the previous hash of the block. And as the new hash is derived from the last block, we cannot change any aspect of a block without altering every single hash in front of it.

Suppose that someone downloaded the Bitcoin Blockchain to their computer and wrote "Satoshi sends Alex 7,236,000 Bitcoin!" into the genesis block and broadcasted this to the Bitcoin network and claimed that he is a secret billionaire. However, as soon as any self-respecting miner compares their current copy of the Blockchain, especially the hash values stored in each block, with his copy of the chain, they will notice that he is a liar, refusing to validate it and run him off the network.

We will define the method that accepts the new block and alter its key/value pairs into strings. We will then convert that string into Unicode, which we will pass into the SHA256 method from the hashlib library and create a hexadecimal string from its return value. We will then return the new hash.

```python
# receiving one block. Turning it into a string, turning that into
# Unicode (for hashing). Hashing with SHA256 encryption,
# then translating the Unicode into a hexadecimal string.
def hash(self, the_block):
    stringObject = json.dumps(the_block, sort_keys = True)
    blockString = stringObject.encode()

    rawHash = hashlib.sha256(blockString)
```

```
        hexHash = rawHash.hexdigest()


        return hexHash
```

In the above snippet of code, we have defined the hash() function and accepts one block and turned them into Strings and then into Unicode for hashing. We have then used the SHA256() function for encryption and then translated the Unicode into a Hexadecimal string.

4.5 Creating a New Blockchain and Sending some Money

Since we have created a class for the Blockchain and included various methods in order to build a new block and a new transaction, along with a custom method utilized to hash any block with SHA256 encryption, let us begin building the chain.

We will initialize an instance of the Block_chain class and perform some dummy transactions. Make sure to list them in some blocks that we include in the chain.

```python
block_chain = Block_chain()

transaction1 = block_chain.newTransaction("Satoshi", "Alex", '10 BTC')

transaction2 = block_chain.newTransaction("Alex", "Satoshi", '2 BTC')

transaction3 = block_chain.newTransaction("Satoshi", "James", '10 BTC')

block_chain.newBlock(10123)


transaction4 = block_chain.newTransaction("Alex", "Lucy", '2 BTC')

transaction5 = block_chain.newTransaction("Lucy", "Justin", '1 BTC')

transaction6 = block_chain.newTransaction("Justin", "Alex", '1 BTC')

block_chain.newBlock(10384)
```

```
print("Genesis block: ", block_chain.chain)
```

We have instantiated the Block_chain() class in the above snippet of code. We have then performed some transactions and printed them for the users. Now, let us have a look at a complete code for the project of building Blockchain using Python.

4.6 Complete Project Code

```python
# importing the required libraries
import hashlib
import json
from time import time


# creating the Block_chain class
class Block_chain(object):
def __init__(self):
    self.chain = []
    self.pendingTransactions = []


    self.newBlock(previousHash = "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks», the_proof = 100)


# Creating a new block listing key/value pairs of
# block information in a JSON object.
# Reset the list of pending transactions &
# append the newest block to the chain.
def newBlock(self, the_proof, previousHash = None):
```

```
        the_block = {
                'index': len(self.chain) + 1,
                'timestamp': time(),
                'transactions': self.pendingTransactions,
                'proof': the_proof,
                'previous_hash': previousHash or self.hash(self.chain[-1]),
        }
        self.pendingTransactions = []
        self.chain.append(the_block)

        return the_block

#Searching the Blockchain for the most recent block.
@property
def lastBlock(self):
        return self.chain[-1]

# Adding a transaction with relevant info to the 'blockpool' - list of pending tx's.
def newTransaction(self, the_sender, the_recipient, the_amount):
        the_transaction = {
                'sender': the_sender,
                'recipient': the_recipient,
                'amount': the_amount
        }
        self.pendingTransactions.append(the_transaction)
        return self.lastBlock['index'] + 1
```

```
# receiving one block. Turning it into a string, turning that into
# Unicode (for hashing). Hashing with SHA256 encryption,
# then translating the Unicode into a hexidecimal string.
def hash(self, the_block):
        stringObject = json.dumps(the_block, sort_keys = True)
        blockString = stringObject.encode()

        rawHash = hashlib.sha256(blockString)
        hexHash = rawHash.hexdigest()

        return hexHash

block_chain = Block_chain()
transaction1 = block_chain.newTransaction("Satoshi", "Alex", '10 BTC')
transaction2 = block_chain.newTransaction("Alex", "Satoshi", '2 BTC')
transaction3 = block_chain.newTransaction("Satoshi", "James", '10 BTC')
block_chain.newBlock(10123)

transaction4 = block_chain.newTransaction("Alex", "Lucy", '2 BTC')
transaction5 = block_chain.newTransaction("Lucy", "Justin", '1 BTC')
transaction6 = block_chain.newTransaction("Justin", "Alex", '1 BTC')
block_chain.newBlock(10384)

print("Genesis block: ", block_chain.chain)
```

Output:

```
Genesis block:  [
```

{

'index': 1,

'timestamp': 1640067926.584454,

'transactions': [],

'proof': 100,

'previous_hash': 'The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.'

},

{

'index': 2,

'timestamp': 1640067926.584454,

'transactions': [

{'sender': 'Satoshi', 'recipient': 'Alex', 'amount': '10 BTC'},

{'sender': 'Alex', 'recipient': 'Satoshi', 'amount': '2 BTC'},

{'sender': 'Satoshi', 'recipient': 'James', 'amount': '10 BTC'}

],

'proof': 10123,

'previous_hash': 'a1b0cf063d43989421eb4b28d9be8f82c2e2e9e40bc9814321e3cbb70b00530a'

},

{

'index': 3,

'timestamp': 1640067926.584454,

'transactions': [

{'sender': 'Alex', 'recipient': 'Lucy', 'amount': '2 BTC'},

{'sender': 'Lucy', 'recipient': 'Justin', 'amount': '1 BTC'},

{'sender': 'Justin', 'recipient': 'Alex', 'amount': '1 BTC'}

```
        ],
        'proof': 10384,
        'previous_hash':
'23699917fdcc013a85bbb5872251768e976bfcc2cd8403565c04970bca24a871'
    }
]
```

In the above output, we can observe that our Blockchain contains three blocks right now: The genesis block (with an index of 1 and no transactions), in addition to the 2 that we added ourselves. We can also notice that the encrypted hashes (derived from every preceding block) and the timestamps do not match each other. Granted, the computer constructed each block almost simultaneously as we executed the program and generated blocks at almost the same time; however, Bitcoin blocks are created approximately every ten minutes.

Blockchains are not banks, and here is a good example to distinguish between the two. A cryptocurrency wallet will estimate the balance by scanning the complete chain and summing up how many coins we received and spent. We do not have to rely on a bank to tell us the amount present in the account. We are only trusting the network instead of one mega-corporation.

In the following code, we have successfully built a Blockchain that we can fill with blocks full of transactions of cryptocurrency; however, this is not a secure network. First, we created a block any time somebody calls newBlock(), and there are no conditions. The newBlock() method requires a parameter called proof; however, that can be anything in our case. It can either be by a number or string saying, "hello world", or literally anything [2].

In the network of Bitcoin, there is a consensus mechanism in a place called Proof of Work, which illustrates the rules by which security is achieved. A proof is a random number that is very difficult to find unless we have some dedicated high-performance machines working around the clock.

There are many other details we are missing, such as fees for the miners to collect, a count of the transaction, public/private key, a Merkle tree structure, and more. However, the above walkthrough was helpful for us as a fundamental example of the moving segments in a Blockchain [3], [5].

CONCLUSION

The system works flawlessly using the base architecture, even if it could keep upgraded to get the client needs. The Blockchain part is implemented as a hashing, but it also requires to be developed for a better security and speed.

The availability of the Blockchain doesn't mean that it is important to use it, but it's one of the ideas and solutions that could live or probably lives somewhere in the other analogs of the Smart Home system. Every software written and every data transfer ever done has to be secured and encrypted, cybersecurity became one of the main parts in every IT field.

With this project the future development, expanding of functions, a wider range of usage and connections becomes possible. Additionally, the connection of Smart devices and Smart Home in a module-based architecture makes it much more flexible.

Monitoring the security of district and their residents became one of the important tasks. Smart Home system connects with each other creating a Smart City. Fire accidents could be easily located by signals and sensors of the IoT web. Electronics nowadays doesn't come without a written algorithm in microprocessor. Better algorithms they have, more creative and smarter technology develops in the output.

The components of a Smart Home can be changed for any other pre-developed device from any company (ex. Mimi Smart by Xiaomi). The developer required to learn a datasheet of the device and create a request for Smart Home server, as it is done with a Smart Door Lock.

REFERENCES

1. https://innovationatwork.ieee.org/Blockchain-iot-security/
2. https://www2.deloitte.com/ch/en/pages/innovation/articles/Blockchain-accelerate-iot-adoption.html
3. https://www.uk.sogeti.com/content-hub/blog/iot-security-using-Blockchain/
4. https://www.hindawi.com/journals/scn/2021/7142048/
5. https://www.chakray.com/privacy-in-iot/
6. https://www.chakray.com/what-is-internet-of-things-and-what-challenges-does-it-pose/
7. https://www.chakray.com/10-security-problems-internet-of-things/
8. https://www.ibm.com/topics/Blockchain-security
9. https://www.investopedia.com/terms/b/Blockchain.asp
10. https://www.iotworldtoday.com/2021/05/31/how-Blockchain-technology-can-benefit-the-internet-of-things/
11. https://eu.mouser.com/applications/securing-iot-Blockchain/
12. https://www.itransition.com/blog/Blockchain-iot-security
13. https://sonin.agency/future-smart-home/
14. https://iopscience.iop.org/article/10.1088/1757-899X/185/1/012019
15. https://www.digiteum.com/create-smart-home-application/
16. https://opensource.com/resources/raspberry-pi
17. https://www.nabto.com/esp8266-for-iot-complete-guide/
18. https://maker.pro/esp8266/tutorial/esp8266-tutorial-how-to-control-anything-from-the-internet
19. https://www.elprocus.com/esp8266-wi-fi-module/
20. Marco Picone, Simone Cirani, and Luca Veltri: “Blockchain Security and Privacy for the Internet of Things”, 2021
21. Karan Singh Garewal: “Practical Blockchains and Cryptocurrencies”, 2020
22. Wiley Hidawi: “Blockchain-based Internet of Things and Industrial IoT: A Comprehensive Survey”, 2020

23. Ali Dorri, Salil S. Kanhere, and Raja Jurdak: “Blockchain in Internet of Things: Challenged and Solutions”, 2020

24. Siraj Raval: “Decentralized Applications”, 2016