**ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

**KHOA KỸ THUẬT MÁY TÍNH**

**CHU TIẾN TRỌNG**

**TRẦN HIỂN LONG**

**NGUYỄN XUÂN MINH TÂN**

**ĐẠO TRỌNG PHIÊN**

**ĐỒ ÁN MÔN HỌC**

**THIẾT KẾ HỆ THỐNG NHÚNG 2**

**TÊN ĐỒ ÁN**

**ỨNG DỤNG BLOCKCHAIN – IOT VÀO HỆ THỐNG VOTING**

**TP. HỒ CHÍ MINH, 2022**

**ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

**KHOA KỸ THUẬT MÁY TÍNH**

**CHU TIẾN TRỌNG – 16521833**

**TRẦN HIỂN LONG – 16520697**

**NGUYỄN XUÂN MINH TÂN – 16521529**

**<ĐẠO TRỌNG PHIÊN – 16521765**

**ĐỒ ÁN MÔN HỌC**

**THIẾT KẾ HỆ THỐNG NHÚNG 2**

**TÊN ĐỒ ÁN**

**ỨNG DỤNG BLOCKCHAIN – IOT VÀO HỆ THỐNG VOTING**

**GIẢNG VIÊN HƯỚNG DẪN**

**LÊ HOÀI NGHĨA**

**TP. HỒ CHÍ MINH, 2022**

MỤC LỤC

[Chương 1. TỔNG QUAN 2](#_Toc106653393)

[1.1. Công nghệ Blockchain 2](#_Toc106653394)

[1.2. Công nghệ IOT 3](#_Toc106653395)

[Chương 2. CƠ SỞ LÝ THUYẾT 4](#_Toc106653396)

[2.1. Công nghệ Blockchain 4](#_Toc106653397)

[2.1.1. Lịch sử Blockchain 4](#_Toc106653398)

[2.1.2. Kiến trúc của Blockchain 5](#_Toc106653399)

[2.1.2.1. Cơ sở dữ liệu 5](#_Toc106653400)

[2.1.2.2. Khối 5](#_Toc106653401)

[2.1.2.3. Hàm băm 6](#_Toc106653402)

[2.1.2.4. Minor 7](#_Toc106653403)

[2.1.2.5. Transaction – Giao dịch 7](#_Toc106653404)

[2.1.2.6. Cơ chế đồng thuận 7](#_Toc106653405)

[2.1.3. Đặc điểm của Blockchain 8](#_Toc106653406)

[2.1.4. Các loại Blockchain 10](#_Toc106653407)

[2.1.5. Cách thức hoạt động của Blockchain 11](#_Toc106653408)

[2.1.6. Bảo mật và quyền riêng tư trong IoT sử dụng machine learning và Blockchain 13](#_Toc106653409)

[2.1.6.1. Các mối đe dọa trong IOT - Blockchain 13](#_Toc106653410)

[2.1.6.2. Các mối đe doạ về quyền riêng tư 16](#_Toc106653411)

[2.1.6.3. Các phương thức sử dụng Machine leaning- Blockchain 17](#_Toc106653412)

[2.1.6.4. Ứng dụng Machine learning trong quyền riêng tư 20](#_Toc106653413)

[2.1.6.5. Các phương pháp ứng dụng Blockchain trong bảo mật 21](#_Toc106653414)

[2.1.6.6. Các phương pháp ứng dụng Blockchain trong quyền riêng tư 25](#_Toc106653415)

[2.1.6.7. Các phương pháp ứng dụng blockchain và ML trong bảo mật 26](#_Toc106653416)

[2.1.6.8. Các phương pháp ứng dụng blockchain và ML trong bảo mật 29](#_Toc106653417)

[2.1.7. Các ứng dụng của Blockchain 30](#_Toc106653418)

[2.1.7.1. Ngành âm nhạc 30](#_Toc106653419)

[2.1.7.2. Ngành giáo dục 31](#_Toc106653420)

[2.1.7.3. Ngành Dịch vụ cộng đồng 31](#_Toc106653421)

[2.1.7.4. Chăm sóc sức khoẻ 32](#_Toc106653422)

[2.1.7.5. An ninh mạng 32](#_Toc106653423)

[2.1.7.6. Bỏ phiếu 33](#_Toc106653424)

[2.1.8. Những thách thức của Blockchain 34](#_Toc106653425)

[2.2. Internet of Things (IOT) 37](#_Toc106653426)

[2.2.1. Lịch sử IOT 37](#_Toc106653427)

[2.2.2. Các định nghĩa về IOT 38](#_Toc106653428)

[2.2.3. Mở rộng IOT 39](#_Toc106653429)

[2.2.4. Kiến trúc của IOT 41](#_Toc106653430)

[2.2.5. Đặc điểm của IOT 43](#_Toc106653431)

[2.2.6. Điện toán đám mây (cloud computing) và lưu trữ 46](#_Toc106653432)

[2.2.6.1. Điện toán đám mây 46](#_Toc106653433)

[2.2.6.2. Ảo hóa 47](#_Toc106653434)

[2.2.6.3. Mối quan hệ giữa IoT, Big Data và điện toán đám mây 48](#_Toc106653435)

[2.2.7. Ứng dụng IOT 48](#_Toc106653436)

[2.2.7.1. Tự động hóa nhà 48](#_Toc106653437)

[2.2.7.2. Chăm sóc sức khỏe 49](#_Toc106653438)

[2.2.7.3. Nông nghiệp thông minh 49](#_Toc106653439)

[2.2.7.4. Chuỗi cung ứng và hậu cần 50](#_Toc106653440)

[2.2.7.5. Thành phố thông minh 50](#_Toc106653441)

[2.2.7.6. Lưới thông minh 51](#_Toc106653442)

[2.2.7.7. Xe được kết nối 51](#_Toc106653443)

[2.2.7.8. Thiết bị đeo được 52](#_Toc106653444)

[2.2.8. Những thách thức của IOT 52](#_Toc106653445)

[2.2.8.1. Dữ liệu lớn 53](#_Toc106653446)

[2.2.8.2. Kết nối mạng 54](#_Toc106653447)

[2.2.8.3. Tính không đồng nhất 54](#_Toc106653448)

[2.2.8.4. Khả năng tương tác 54](#_Toc106653449)

[2.2.8.5. Khả năng mở rộng 55](#_Toc106653450)

[2.2.8.6. Bảo mật và quyền riêng tư 55](#_Toc106653451)

[2.2.9. 5G Internet of Things 56](#_Toc106653452)

[2.2.9.1. Giới thiệu 56](#_Toc106653453)

[2.2.9.2. Thực trạng nghiên cứu của 5G và IOT 56](#_Toc106653454)

[2.2.9.3. 5G-IoT Architecture 58](#_Toc106653455)

[2.2.9.4. Các công nghệ cho phép chính trong 5G-IOT 59](#_Toc106653456)

[Chương 3. PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG 61](#_Toc106653457)

[3.1. Mục tiêu của đồ án 61](#_Toc106653458)

[3.2. Thiết kế hệ thống 61](#_Toc106653459)

[3.2.1. Thiết kế phần cứng 61](#_Toc106653460)

[3.2.1.1. Giới thiệu ESP8266 61](#_Toc106653461)

[3.2.1.2. Thông số kĩ thuật 61](#_Toc106653462)

[3.2.2. Thiết kế phần mềm 62](#_Toc106653463)

[3.2.2.1. NodeJS 62](#_Toc106653464)

[3.2.2.2. ArduinoIDE 64](#_Toc106653465)

[3.2.2.3. Visual Studio Code 65](#_Toc106653466)

[3.2.3. Thiết kế phần chức năng 67](#_Toc106653467)

[3.2.3.1. Thiết kế tổng quan 67](#_Toc106653468)

[3.2.3.2. Thiết kế giao diện trên Webserver sử dụng ESP8266 67](#_Toc106653469)

[3.2.3.3. Thiết kế mạng Blockchain 69](#_Toc106653470)

[Chương 4. KẾT QUẢ THỰC NGHIỆM 71](#_Toc106653471)

[4.1. Kết quả đạt được 71](#_Toc106653472)

[4.2. Chủ đề cấp độ 2 72](#_Toc106653473)

[Chương 5. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 73](#_Toc106653474)

[5.1. Kết kuận 73](#_Toc106653475)

[5.1.1. Những khó khăn 73](#_Toc106653476)

[5.1.2. Kết quả và những kinh nghiệm tích lũy 73](#_Toc106653477)

[5.2. Hướng phát triển 73](#_Toc106653478)

DANH MỤC HÌNH VẼ

[Chương 1. TỔNG QUAN 2](#_Toc106653479)

[1.1. Công nghệ Blockchain 2](#_Toc106653480)

[1.2. Công nghệ IOT 3](#_Toc106653481)

[Chương 2. CƠ SỞ LÝ THUYẾT 4](#_Toc106653482)

[2.1. Công nghệ Blockchain 4](#_Toc106653483)

[2.1.1. Lịch sử Blockchain 4](#_Toc106653484)

[2.1.2. Kiến trúc của Blockchain 5](#_Toc106653485)

[2.1.2.1. Cơ sở dữ liệu 5](#_Toc106653486)

[2.1.2.2. Khối 5](#_Toc106653487)

[2.1.2.3. Hàm băm 6](#_Toc106653488)

[2.1.2.4. Minor 7](#_Toc106653489)

[2.1.2.5. Transaction – Giao dịch 7](#_Toc106653490)

[2.1.2.6. Cơ chế đồng thuận 7](#_Toc106653491)

[2.1.3. Đặc điểm của Blockchain 8](#_Toc106653492)

[2.1.4. Các loại Blockchain 10](#_Toc106653493)

[2.1.5. Cách thức hoạt động của Blockchain 11](#_Toc106653494)

[2.1.6. Bảo mật và quyền riêng tư trong IoT sử dụng machine learning và Blockchain 13](#_Toc106653495)

[2.1.6.1. Các mối đe dọa trong IOT - Blockchain 13](#_Toc106653496)

[2.1.6.2. Các mối đe doạ về quyền riêng tư 16](#_Toc106653497)

[2.1.6.3. Các phương thức sử dụng Machine leaning- Blockchain 17](#_Toc106653498)

[2.1.6.4. Ứng dụng Machine learning trong quyền riêng tư 20](#_Toc106653499)

[2.1.6.5. Các phương pháp ứng dụng Blockchain trong bảo mật 21](#_Toc106653500)

[2.1.6.6. Các phương pháp ứng dụng Blockchain trong quyền riêng tư 25](#_Toc106653501)

[2.1.6.7. Các phương pháp ứng dụng blockchain và ML trong bảo mật 26](#_Toc106653502)

[2.1.6.8. Các phương pháp ứng dụng blockchain và ML trong bảo mật 29](#_Toc106653503)

[2.1.7. Các ứng dụng của Blockchain 30](#_Toc106653504)

[2.1.7.1. Ngành âm nhạc 30](#_Toc106653505)

[2.1.7.2. Ngành giáo dục 31](#_Toc106653506)

[2.1.7.3. Ngành Dịch vụ cộng đồng 31](#_Toc106653507)

[2.1.7.4. Chăm sóc sức khoẻ 32](#_Toc106653508)

[2.1.7.5. An ninh mạng 32](#_Toc106653509)

[2.1.7.6. Bỏ phiếu 33](#_Toc106653510)

[2.1.8. Những thách thức của Blockchain 34](#_Toc106653511)

[2.2. Internet of Things (IOT) 37](#_Toc106653512)

[2.2.1. Lịch sử IOT 37](#_Toc106653513)

[2.2.2. Các định nghĩa về IOT 38](#_Toc106653514)

[2.2.3. Mở rộng IOT 39](#_Toc106653515)

[2.2.4. Kiến trúc của IOT 41](#_Toc106653516)

[2.2.5. Đặc điểm của IOT 43](#_Toc106653517)

[2.2.6. Điện toán đám mây (cloud computing) và lưu trữ 46](#_Toc106653518)

[2.2.6.1. Điện toán đám mây 46](#_Toc106653519)

[2.2.6.2. Ảo hóa 47](#_Toc106653520)

[2.2.6.3. Mối quan hệ giữa IoT, Big Data và điện toán đám mây 48](#_Toc106653521)

[2.2.7. Ứng dụng IOT 48](#_Toc106653522)

[2.2.7.1. Tự động hóa nhà 48](#_Toc106653523)

[2.2.7.2. Chăm sóc sức khỏe 49](#_Toc106653524)

[2.2.7.3. Nông nghiệp thông minh 49](#_Toc106653525)

[2.2.7.4. Chuỗi cung ứng và hậu cần 50](#_Toc106653526)

[2.2.7.5. Thành phố thông minh 50](#_Toc106653527)

[2.2.7.6. Lưới thông minh 51](#_Toc106653528)

[2.2.7.7. Xe được kết nối 51](#_Toc106653529)

[2.2.7.8. Thiết bị đeo được 52](#_Toc106653530)

[2.2.8. Những thách thức của IOT 52](#_Toc106653531)

[2.2.8.1. Dữ liệu lớn 53](#_Toc106653532)

[2.2.8.2. Kết nối mạng 54](#_Toc106653533)

[2.2.8.3. Tính không đồng nhất 54](#_Toc106653534)

[2.2.8.4. Khả năng tương tác 54](#_Toc106653535)

[2.2.8.5. Khả năng mở rộng 55](#_Toc106653536)

[2.2.8.6. Bảo mật và quyền riêng tư 55](#_Toc106653537)

[2.2.9. 5G Internet of Things 56](#_Toc106653538)

[2.2.9.1. Giới thiệu 56](#_Toc106653539)

[2.2.9.2. Thực trạng nghiên cứu của 5G và IOT 56](#_Toc106653540)

[2.2.9.3. 5G-IoT Architecture 58](#_Toc106653541)

[2.2.9.4. Các công nghệ cho phép chính trong 5G-IOT 59](#_Toc106653542)

[Chương 3. PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG 61](#_Toc106653543)

[3.1. Mục tiêu của đồ án 61](#_Toc106653544)

[3.2. Thiết kế hệ thống 61](#_Toc106653545)

[3.2.1. Thiết kế phần cứng 61](#_Toc106653546)

[3.2.1.1. Giới thiệu ESP8266 61](#_Toc106653547)

[3.2.1.2. Thông số kĩ thuật 61](#_Toc106653548)

[3.2.2. Thiết kế phần mềm 62](#_Toc106653549)

[3.2.2.1. NodeJS 62](#_Toc106653550)

[3.2.2.2. ArduinoIDE 64](#_Toc106653551)

[3.2.2.3. Visual Studio Code 65](#_Toc106653552)

[3.2.3. Thiết kế phần chức năng 67](#_Toc106653553)

[3.2.3.1. Thiết kế tổng quan 67](#_Toc106653554)

[3.2.3.2. Thiết kế giao diện trên Webserver sử dụng ESP8266 67](#_Toc106653555)

[3.2.3.3. Thiết kế mạng Blockchain 69](#_Toc106653556)

[Chương 4. KẾT QUẢ THỰC NGHIỆM 71](#_Toc106653557)

[4.1. Kết quả đạt được 71](#_Toc106653558)

[4.2. Chủ đề cấp độ 2 72](#_Toc106653559)

[Chương 5. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 73](#_Toc106653560)

[5.1. Kết kuận 73](#_Toc106653561)

[5.1.1. Những khó khăn 73](#_Toc106653562)

[5.1.2. Kết quả và những kinh nghiệm tích lũy 73](#_Toc106653563)

[5.2. Hướng phát triển 73](#_Toc106653564)

DANH MỤC BẢNG

[Chương 1. TỔNG QUAN 2](#_Toc106653565)

[1.1. Công nghệ Blockchain 2](#_Toc106653566)

[1.2. Công nghệ IOT 3](#_Toc106653567)

[Chương 2. CƠ SỞ LÝ THUYẾT 4](#_Toc106653568)

[2.1. Công nghệ Blockchain 4](#_Toc106653569)

[2.1.1. Lịch sử Blockchain 4](#_Toc106653570)

[2.1.2. Kiến trúc của Blockchain 5](#_Toc106653571)

[2.1.2.1. Cơ sở dữ liệu 5](#_Toc106653572)

[2.1.2.2. Khối 5](#_Toc106653573)

[2.1.2.3. Hàm băm 6](#_Toc106653574)

[2.1.2.4. Minor 7](#_Toc106653575)

[2.1.2.5. Transaction – Giao dịch 7](#_Toc106653576)

[2.1.2.6. Cơ chế đồng thuận 7](#_Toc106653577)

[2.1.3. Đặc điểm của Blockchain 8](#_Toc106653578)

[2.1.4. Các loại Blockchain 10](#_Toc106653579)

[2.1.5. Cách thức hoạt động của Blockchain 11](#_Toc106653580)

[2.1.6. Bảo mật và quyền riêng tư trong IoT sử dụng machine learning và Blockchain 13](#_Toc106653581)

[2.1.6.1. Các mối đe dọa trong IOT - Blockchain 13](#_Toc106653582)

[2.1.6.2. Các mối đe doạ về quyền riêng tư 16](#_Toc106653583)

[2.1.6.3. Các phương thức sử dụng Machine leaning- Blockchain 17](#_Toc106653584)

[2.1.6.4. Ứng dụng Machine learning trong quyền riêng tư 20](#_Toc106653585)

[2.1.6.5. Các phương pháp ứng dụng Blockchain trong bảo mật 21](#_Toc106653586)

[2.1.6.6. Các phương pháp ứng dụng Blockchain trong quyền riêng tư 25](#_Toc106653587)

[2.1.6.7. Các phương pháp ứng dụng blockchain và ML trong bảo mật 26](#_Toc106653588)

[2.1.6.8. Các phương pháp ứng dụng blockchain và ML trong bảo mật 29](#_Toc106653589)

[2.1.7. Các ứng dụng của Blockchain 30](#_Toc106653590)

[2.1.7.1. Ngành âm nhạc 30](#_Toc106653591)

[2.1.7.2. Ngành giáo dục 31](#_Toc106653592)

[2.1.7.3. Ngành Dịch vụ cộng đồng 31](#_Toc106653593)

[2.1.7.4. Chăm sóc sức khoẻ 32](#_Toc106653594)

[2.1.7.5. An ninh mạng 32](#_Toc106653595)

[2.1.7.6. Bỏ phiếu 33](#_Toc106653596)

[2.1.8. Những thách thức của Blockchain 34](#_Toc106653597)

[2.2. Internet of Things (IOT) 37](#_Toc106653598)

[2.2.1. Lịch sử IOT 37](#_Toc106653599)

[2.2.2. Các định nghĩa về IOT 38](#_Toc106653600)

[2.2.3. Mở rộng IOT 39](#_Toc106653601)

[2.2.4. Kiến trúc của IOT 41](#_Toc106653602)

[2.2.5. Đặc điểm của IOT 43](#_Toc106653603)

[2.2.6. Điện toán đám mây (cloud computing) và lưu trữ 46](#_Toc106653604)

[2.2.6.1. Điện toán đám mây 46](#_Toc106653605)

[2.2.6.2. Ảo hóa 47](#_Toc106653606)

[2.2.6.3. Mối quan hệ giữa IoT, Big Data và điện toán đám mây 48](#_Toc106653607)

[2.2.7. Ứng dụng IOT 48](#_Toc106653608)

[2.2.7.1. Tự động hóa nhà 48](#_Toc106653609)

[2.2.7.2. Chăm sóc sức khỏe 49](#_Toc106653610)

[2.2.7.3. Nông nghiệp thông minh 49](#_Toc106653611)

[2.2.7.4. Chuỗi cung ứng và hậu cần 50](#_Toc106653612)

[2.2.7.5. Thành phố thông minh 50](#_Toc106653613)

[2.2.7.6. Lưới thông minh 51](#_Toc106653614)

[2.2.7.7. Xe được kết nối 51](#_Toc106653615)

[2.2.7.8. Thiết bị đeo được 52](#_Toc106653616)

[2.2.8. Những thách thức của IOT 52](#_Toc106653617)

[2.2.8.1. Dữ liệu lớn 53](#_Toc106653618)

[2.2.8.2. Kết nối mạng 54](#_Toc106653619)

[2.2.8.3. Tính không đồng nhất 54](#_Toc106653620)

[2.2.8.4. Khả năng tương tác 54](#_Toc106653621)

[2.2.8.5. Khả năng mở rộng 55](#_Toc106653622)

[2.2.8.6. Bảo mật và quyền riêng tư 55](#_Toc106653623)

[2.2.9. 5G Internet of Things 56](#_Toc106653624)

[2.2.9.1. Giới thiệu 56](#_Toc106653625)

[2.2.9.2. Thực trạng nghiên cứu của 5G và IOT 56](#_Toc106653626)

[2.2.9.3. 5G-IoT Architecture 58](#_Toc106653627)

[2.2.9.4. Các công nghệ cho phép chính trong 5G-IOT 59](#_Toc106653628)

[Chương 3. PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG 61](#_Toc106653629)

[3.1. Mục tiêu của đồ án 61](#_Toc106653630)

[3.2. Thiết kế hệ thống 61](#_Toc106653631)

[3.2.1. Thiết kế phần cứng 61](#_Toc106653632)

[3.2.1.1. Giới thiệu ESP8266 61](#_Toc106653633)

[3.2.1.2. Thông số kĩ thuật 61](#_Toc106653634)

[3.2.2. Thiết kế phần mềm 62](#_Toc106653635)

[3.2.2.1. NodeJS 62](#_Toc106653636)

[3.2.2.2. ArduinoIDE 64](#_Toc106653637)

[3.2.2.3. Visual Studio Code 65](#_Toc106653638)

[3.2.3. Thiết kế phần chức năng 67](#_Toc106653639)

[3.2.3.1. Thiết kế tổng quan 67](#_Toc106653640)

[3.2.3.2. Thiết kế giao diện trên Webserver sử dụng ESP8266 67](#_Toc106653641)

[3.2.3.3. Thiết kế mạng Blockchain 69](#_Toc106653642)

[Chương 4. KẾT QUẢ THỰC NGHIỆM 71](#_Toc106653643)

[4.1. Kết quả đạt được 71](#_Toc106653644)

[4.2. Chủ đề cấp độ 2 72](#_Toc106653645)

[Chương 5. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 73](#_Toc106653646)

[5.1. Kết kuận 73](#_Toc106653647)

[5.1.1. Những khó khăn 73](#_Toc106653648)

[5.1.2. Kết quả và những kinh nghiệm tích lũy 73](#_Toc106653649)

[5.2. Hướng phát triển 73](#_Toc106653650)

DANH MỤC HÌNH ẢNH

[Hình 1 Pinout Esp8266 5](#_Toc106653651)

[Hình 2 Các ưu điểm blockchain 9](#_Toc106653652)

[Hình 3 Các loại blockchain 10](#_Toc106653653)

[Hình 4 Tổng quan các mối đe dọa đối với thiết bị IoT 14](#_Toc106653654)

[Hình 5Security threats and Privacy threats 17](#_Toc106653655)

[Hình 6 Types of feature extractor 19](#_Toc106653656)

[Hình 7 Các phương pháp sử dụng 20](#_Toc106653657)

[Hình 8 IoT device lifecycle security management 24](#_Toc106653658)

[Hình 9 Mô hình hoạt động 26](#_Toc106653659)

[Hình 10Framework of CB-MDEE 28](#_Toc106653660)

[Hình 11 Cấu trúc của blockchain 28](#_Toc106653661)

[Hình 12Structure of multi-feature detection of Android malware 29](#_Toc106653662)

[Hình 13 Các thách thức của blockchain 34](#_Toc106653663)

[Hình 14 Các lợi ích của IoT 39](#_Toc106653664)

[Hình 15 Kỳ vọng tăng trưởng IoT từ 2015 đến 2025 40](#_Toc106653665)

[Hình 16 Mô hình tham chiếu IoT theo IWF. 42](#_Toc106653666)

[Hình 17 Đặc điểm chung của hệ thống IoT 44](#_Toc106653667)

[Hình 18 Mối quan hệ giữa IoT và big data, điện toán đám mây 48](#_Toc106653668)

[Hình 19 Những thách thức của IoT 53](#_Toc106653669)

[Hình 20 Số lượng bài báo về 5G-IoT theo năm 56](#_Toc106653670)

[Hình 21 Dòng thời gian cho đến 5G 57](#_Toc106653671)

[Hình 22 Machine type communication (MTC) trong 5G-IoT 57](#_Toc106653672)

[Hình 23 Kiến trúc của IMT 58](#_Toc106653673)

[Hình 24 Các yêu cầu mà 5G cần đáp ứng 59](#_Toc106653674)

[Hình 25 các công nghệ liên hệ với 5G-IoT 59](#_Toc106653675)

[Hình 26 Ví dụ về kiến trúc 5G-IoT thực tế 60](#_Toc106653676)

[Hình 27 ESP8266 Pinout 62](#_Toc106653677)

[Hình 28 Node JS 63](#_Toc106653678)

[Hình 29 Arduino IDE 64](#_Toc106653679)

[Hình 30 Visual Studio Code 66](#_Toc106653680)

[Hình 31 Sơ đồ tổng quan hệ thống 67](#_Toc106653681)

[Hình 32 Mã html hiển thị 4 checkbox và nút bấm 68](#_Toc106653682)

[Hình 33 Giao diện Voting 69](#_Toc106653683)

[Hình 34 Mã html hiển thị thông báo 69](#_Toc106653684)

[Hình 35 Giao diện hiển thị thông báo 69](#_Toc106653685)

[Hình 36 Cấu trúc một block 70](#_Toc106653686)

[Hình 37 Khởi tạo server 70](#_Toc106653687)

[Hình 38 API tạo một block mới 70](#_Toc106653688)

[Hình 39 Kết quả khi gọi API tạo mới block sử dụng Postman 71](#_Toc106653689)

[Hình 40 Kết quả khi tạo mới block trên terminal 71](#_Toc106653690)

[Hình 40 Kết quả khi truyền dữ liệu voting từ thiết bị IOT 72](#_Toc106653691)

[Hình 41 Kết quả khi goi API hiển thị dữ liệu voting từ port P2P trên Postman 72](#_Toc106653692)

DANH MỤC BẢNG

[Bảng 1 Các tiêu chí trong blockchain 11](#_Toc106653693)

# TỔNG QUAN

## Công nghệ Blockchain

Blockchain là một sổ cái phân tán và phi tập trung các giao dịch được sử dụng để quản lý một bộ hồ sơ không ngừng tăng lên. Để lưu trữ một giao dịch trong sổ cái, phần lớn người dùng tham gia vào mạng lưới blockchain được chấp thuận và ghi lại sự chấp thuận của họ.

Một tập hợp các giao dịch được nhóm lại với nhau và phân bổ một khối trong sổ cái được liên kết với các khối. Để liên kết các khối với nhau, mỗi khối bao gồm một dấu thời gian và hàm băm của khối trước đó. Hàm băm xác thực tính toàn vẹn và chấp thuận dữ liệu bên trong khối. Hơn nữa, để giữ cho tất cả người dùng tham gia mạng lưới blockchain được cập nhật, mỗi người dùng giữ một bản sao của sổ cái gốc, tất cả người dùng đều được đồng bộ hóa và cập nhật với những thay đổi mới.

Blockchain đã được nhiều tổ chức định nghĩa từ các quan điểm khác nhau. Ví dụ: Coinbase đã định nghĩa blockchain là “một sổ cái phân tán công khai chứa lịch sử của mọi giao dịch bitcoin”. Định nghĩa này giải thích blockchain từ góc nhìn của tiền điện tử vốn không xem xét thực tế là blockchain có thể được sử dụng trong các ứng dụng khác nhau một cách độc lập.

Trong từ điển Oxford cung cấp một định nghĩa phổ biến hơn cho blockchain. Nó nêu rõ “một sổ cái kỹ thuật số trong đó các giao dịch được thực hiện bằng bitcoin hoặc một loại tiền điện tử khác được ghi lại theo thứ tự thời gian và công khai”.

Ngoài ra, một định nghĩa rộng hơn cho blockchain được cung cấp bởi Webopedia. Trong đó nêu “một loại cấu trúc dữ liệu cho phép xác định và theo dõi các giao dịch kỹ thuật số và chia sẻ thông tin này trên một mạng máy tính phân tán, tạo ra một mạng tin cậy phân tán theo một nghĩa nào đó. Công nghệ sổ cái phân tán được cung cấp bởi blockchain cung cấp một phương tiện minh bạch và an toàn để theo dõi quyền sở hữu và chuyển giao tài sản”. Định nghĩa này cung cấp mô tả chi tiết hơn về blockchain bằng cách nêu bật các tính năng thiết yếu của nó với việc xác nhận rằng blockchain không chỉ là một công nghệ phân tán mà còn là một môi trường phi tập trung.

Hơn nữa, làm nổi bật các yếu tố chính của công nghệ blockchain, Sultan et al cung cấp một định nghĩa chung cho blockchain. Nó nêu rõ “các khối liên kết theo tuần tự, liên kết mật mã của các giao dịch tài sản được ký kết hợp lệ, được điều chỉnh bởi một mô hình đồng thuận”.

## Công nghệ IOT

IoT cho phép các thiết bị khác nhau xung quanh chúng ta trong môi trường có thể xác định được địa chỉ, nhận dạng và định vị được thông qua các thiết bị cảm biến. Ngoài ra, nó cho phép các thiết bị này có thể được điều khiển qua Internet bằng mạng truyền thông có dây hoặc không dây. Các đối tượng hàng ngày không chỉ liên quan đến các thiết bị điện tử thông thường hoặc các sản phẩm phát triển công nghệ như xe cộ, điện thoại, mà còn liên quan đến các đối tượng khác như thực phẩm, động vật, quần áo, cây cối,… Mục đích chính của hệ thống IoT là cho phép các đối tượng khác nhau được kết nối ở bất kỳ đâu, bất kỳ lúc nào bởi bất kỳ ai lý tưởng bằng cách sử dụng bất kỳ mạng nào và bất kỳ dịch vụ nào.

Phần này trình bày các định nghĩa khác nhau về IoT được các tổ chức và các nhà nghiên cứu khác nhau đề xuất. Kiến trúc, đặc điểm thiết yếu, ứng dụng và thách thức của hệ thống IoT cũng được trình bày.

# CƠ SỞ LÝ THUYẾT

## Công nghệ Blockchain

### Lịch sử Blockchain

Lịch sử của công nghệ blockchain bắt nguồn từ những năm 1980 và 1990 trong thế kỷ 20. Tuy nhiên vào năm 2008, sau khi phát hiện ra bitcoin, blockchain đã trở nên phổ biến hơn.

Theo Pilkington, khái niệm đầu tiên về tiền tệ kỹ thuật số được phát minh dựa trên một máy chủ tập trung để tránh tăng gấp đôi, đó là quá trình sử dụng cùng một số bitcoin nhiều lần. Tuy nhiên, nhận thức này không đưa ra được giải pháp cho các vấn đề chi tiêu kép, ẩn danh và tập trung hóa. Thế giới vẫn phải mất vài năm để sử dụng kiến trúc tập trung sử dụng bên thứ ba để kiểm soát và duy trì sự tin cậy giữa các bên liên lạc cho đến khi Szabo vào cuối năm 1990 phát minh ra một loại tiền tệ kỹ thuật số phi tập trung được gọi là bit gold.

Sau khoảng 10 năm, tiền điện tử Bitcoin đã được giới thiệu. Blockchain trở nên phổ biến rộng rãi sau bài báo của Nakamoto. Ông đề xuất thay thế kiến trúc tập trung cổ điển bằng một kỹ thuật mới dựa trên cơ chế đồng thuận. Ban đầu, công nghệ này được đặt tên là blockchain với hai từ “khối” và “chuỗi”; tuy nhiên, vào năm 2016, hai từ được kết hợp thành một là blockchain.

Trong khoảng thời gian từ 2011 đến 2013, blockchain đã được sử dụng rộng rãi trong tiền điện tử, đặc biệt là trong chuyển tiền và thanh toán kỹ thuật số. Ngày nay, công nghệ blockchain đã xuất hiện trong nhiều ứng dụng và dịch vụ khác nhau để tận dụng các tính năng phi tập trung và bất biến.

Diagram

Description automatically generated

Hình 1 Pinout Esp8266

### Kiến trúc của Blockchain

#### Cơ sở dữ liệu

Cơ sở dữ liệu cổ điển là một cấu trúc dữ liệu được sử dụng để lưu trữ thông tin. Nó sử dụng mô hình quan hệ để cung cấp nhiều cách kết hợp hơn để truy vấn và thu thập dữ liệu bằng cách liên kết thông tin từ nhiều cơ sở dữ liệu. Thông tin được lưu trữ trong cơ sở dữ liệu có thể được tổ chức bằng Hệ thống quản lý Database (DBMS). Một cơ sở dữ liệu đơn giản được lưu trữ trong các phần tử dữ liệu được gọi là bảng chứa các trường. Mỗi trường chứa các cột để mô tả trường và các hàng để xác định một bản ghi được lưu trữ trong cơ sở dữ liệu.

Một trong những yếu tố chính của blockchain là cơ sở dữ liệu. Tuy nhiên, đây không phải là một cơ sở dữ liệu bình thường chứa các hàng và cột; thay vào đó, nó là một sổ cái của tất cả các giao dịch trước đó cho tất cả người dùng tham gia trong mạng blockchain. Loại cơ sở dữ liệu này có đặc điểm là có thông lượng cao, kiểm soát phi tập trung, độ trễ thấp, lưu trữ dữ liệu bất biến và bảo mật tích hợp.

#### Khối

Khối là yếu tố lưu trữ quan trọng trong chuỗi khối. Nó chứa và lưu trữ dữ liệu liên quan đến nhiều giao dịch. Các khối được liên kết với nhau bằng cách lưu trữ băm của khối trước đó trong khối hiện tại, điều này làm cho các khối được liên kết thành một vòng tròn để bao bọc trong sổ cái công khai.

Các khối thường được chia thành hai phân đoạn, tiêu đề và một nhóm giao dịch. Tiêu đề chứa siêu dữ liệu khối được sử dụng để chứa tất cả các chi tiết về khối trong sổ cái. Thông tin tiêu đề khối được mô tả như sau:

• Số phiên bản: 4byte để chỉ ra số phiên bản của khối.

• Hàm băm khối trước: 32byte để mô tả hàm băm của khối trước đó của chuỗi khối. Nó hoạt động như một con trỏ giữa khối hiện tại và khối trước đó.

• TimeStamp: 4byte để ghi lại thời gian khối đã được tạo.

• Merkle tree: 32byte là một hàm băm (SHA-256) của tất cả các giao dịch có liên quan đến khối này.

• Difficulty: 4byte để xác định mục tiêu độ khó của khối.

• Nonce: 4byte để tạo khối và tính các hàm băm khác nhau.

#### Hàm băm

Hàm băm là một vấn đề toán học phức tạp mà các thợ đào phải giải để tìm ra một khối. Khái niệm hàm băm được sử dụng như một cách để tìm kiếm dữ liệu trong cơ sở dữ liệu. Các hàm băm không có xung đột, có nghĩa là rất khó tìm thấy hai hàm băm giống nhau cho hai thông báo khác nhau. Do đó, các khối được xác định thông qua hàm băm của chúng, phục vụ hai mục đích; xác minh và xác minh tính toàn vẹn.

Để liên kết các khối với nhau, mỗi khối bao gồm băm của khối trước bên trong tiêu đề của chính nó, đặt một chuỗi quay trở lại khối đầu tiên, tạo ra một chuỗi các băm. Các giá trị băm được giữ trong bảng băm là một cơ chế lập chỉ mục được tổ chức tốt để tăng hiệu suất của các hoạt động tìm kiếm.

#### Minor

Một CPU cố gắng giải quyết một vấn đề toán học phức tạp về tính toán để khám phá ra một khối mới được gọi là một công cụ khai thác. Các thợ đào có thể làm việc một mình hoặc trong các nhóm để cố gắng tìm ra lời giải của vấn đề toán học. Quá trình tìm kiếm một khối mới được bắt đầu bằng cách phát các giao dịch mới cho tất cả người dùng của mạng blockchain. Mỗi người dùng thu thập các giao dịch mới vào một khối và làm việc để tìm ra bằng chứng công việc của khối. Nếu người dùng tìm thấy nó, khối sẽ được phát cho tất cả người dùng để xác minh nó. Khối sẽ chỉ được xác minh nếu tất cả các giao dịch bên trong đều hợp lệ. Khối có thể được coi là được chấp nhận từ tất cả những người dùng tham gia trong mạng blockchain khi họ bắt đầu làm việc để tạo khối tiếp theo trong chuỗi bằng cách sử dụng hàm băm của khối được chấp nhận làm hàm băm trước đó.

Trong một số trường hợp, các giao dịch có chi phí cao nhất trước tiên được chọn từ trẻ vị thành niên, vì trẻ vị thành niên tìm thấy khối kiếm được chi phí hoặc lệ phí của tất cả các giao dịch trong khối đó.

#### Transaction – Giao dịch

Một giao dịch blockchain có thể được định nghĩa là một đơn vị nhỏ được lưu trữ trong hồ sơ công khai. Các bản ghi này chỉ được thực hiện, thực thi và lưu trữ trong blockchain sau khi được xác minh bởi đa số người dùng tham gia vào mạng blockchain.

Mỗi giao dịch trước đó có thể được xem lại bất kỳ lúc nào nhưng không thể cập nhật. Quy mô của giao dịch có ý nghĩa quan trọng đối với các thợ đào vì các giao dịch lớn hơn cần nhiều không gian hơn trong khối và tiêu thụ nhiều năng lượng hơn, trong khi các giao dịch nhỏ hơn dễ xác thực hơn và tiêu thụ ít năng lượng hơn.

#### Cơ chế đồng thuận

Blockchain là loại sổ cái phân tán được sử dụng để lưu trữ bản ghi của tất cả các giao dịch trước đó. Nó được gọi là phân phối vì nó được lưu trữ trên nhiều máy tính qua mạng trên toàn thế giới. Hoạt động chính của sổ cái phân tán là đảm bảo rằng toàn bộ mạng lưới phê duyệt nội dung của sổ cái, được thực hiện bằng cách sử dụng cơ chế đồng thuận. Có nhiều số cơ chế đồng thuận, tuy nhiên, các cơ chế đồng thuận blockchain phổ biến nhất là Proof of Stake (PoS) và Proof of Work (PoW). Sự khác biệt chính giữa các cơ chế đồng thuận khác nhau là cách chúng ủy quyền và thưởng cho việc xác minh các giao dịch.

PoW là một cơ chế đồng thuận phổ biến được sử dụng bởi các mạng tiền điện tử phổ biến nhất như Bitcoin và Litecoin. Người tham gia-người dùng trong mạng blockchain được yêu cầu chứng minh công việc đã được thực hiện để đủ điều kiện cho họ có được khả năng thêm các khối mới vào sổ cái.

Tuy nhiên, quá trình khai thác đòi hỏi tiêu thụ nhiều năng lượng và thời gian xử lý. PoS là một cơ chế đồng thuận công khai khác để cung cấp mức tiêu thụ năng lượng thấp, chi phí thấp so với cơ chế PoW. Ngoài ra, nó phân bổ trách nhiệm cho người dùng tham gia tương ứng với số lượng mã thông báo tiền ảo mà nó nắm giữ. Tuy nhiên, điều này dẫn đến một mặt trái vì nó khuyến khích tiết kiệm tiền điện tử, thay vì chi tiêu nó.

### Đặc điểm của Blockchain

Blockchain có thể được coi là một kiến trúc phi tập trung với tính năng bảo mật được tích hợp sẵn nhằm tăng độ tin cậy và tính toàn vẹn của các giao dịch. Phần này cung cấp các đặc điểm chung liên quan đến blockchain. Các tính năng này được mô tả trong hình bên dưới, bao gồm:

Chart, bubble chart

Description automatically generated

Hình 2 Các ưu điểm blockchain

* Decentralization (phi tập trung): blockchain sử dụng một sổ cái phân tán và phi tập trung để tận dụng khả năng xử lý của tất cả những người dùng tham gia trong mạng blockchain, giúp giảm độ trễ và loại bỏ những lỗi không mong muốn.
* Immutability (tính bất biến): một trong những tính năng thiết yếu của blockchain là khả năng đảm bảo tính toàn vẹn của các giao dịch bằng cách tạo các sổ cái bất biến. Trong các kiến trúc tập trung truyền thống, cơ sở dữ liệu có thể bị thay đổi và cần tạo ra sự tin cậy với bên thứ ba để đảm bảo tính toàn vẹn của thông tin. Trong công nghệ blockchain, vì mỗi khối trong sổ cái phân tán liên quan đến khối trước đó tạo thành một chuỗi khối, các khối được lưu vĩnh viễn và không bao giờ thay đổi miễn là người dùng tham gia tiếp tục duy trì mạng blockchain.
* Transparency (tính minh bạch): blockchain mang lại mức độ minh bạch cao bằng cách chia sẻ chi tiết giao dịch giữa tất cả người dùng tham gia liên quan đến các giao dịch đó. Trong môi trường blockchain, không cần bên thứ ba để cải thiện tính thân thiện với doanh nghiệp và đảm bảo quy trình làm việc đáng tin cậy.
* Better Security (bảo mật tốt hơn): blockchain cung cấp tính bảo mật tốt hơn vì nó sử dụng cơ sở hạ tầng khóa công khai để bảo vệ chống lại các hành động độc hại nhằm thay đổi dữ liệu. Những người dùng tham gia mạng blockchain đặt niềm tin vào tính toàn vẹn và bảo mật của cơ chế đồng thuận.
* Efficiency (hiệu quả): Blockchain cải thiện kiến trúc tập trung cổ điển bằng cách phân phối các bản ghi cơ sở dữ liệu giữa những người dùng khác nhau tham gia vào mạng blockchain. Việc phân phối các giao dịch làm cho việc xác minh tất cả các bản ghi được lưu trữ trong cơ sở dữ liệu trở nên minh bạch hơn. Blockchain hiệu quả hơn kiến trúc tập trung cổ điển về chi phí, tốc độ giải quyết và quản lý rủi ro.

### Các loại Blockchain

Có 3 loại blockchain: public, private và federated:

* Public blockchain (blockchain công khai): cho phép thêm bất kỳ người dùng ẩn danh nào vào mạng blockchain, gửi một giao dịch mới, xác minh các khối mới được thêm vào và đọc nội dung của blockchain. Blockchain công khai được mở cho tất cả các loại thiết bị tham gia vào mạng.Bảo mật của public blockchain sử dụng các cơ chế đồng thuận như PoW hoặc PoS. Một số public blockchain phổ biến như: Ethereum, Bitcoin và NXT.

Diagram

Description automatically generated

Hình 3 Các loại blockchain

* Private blockchain (blockchain riêng tư): chỉ một tổ chức cụ thể mới có quyền tham gia vào mạng blockchain, gửi một giao dịch mới và tham gia vào cơ chế đồng thuận.Người dùng phải nhận được sự cho phép của tổ chức trước khi tham gia vào mạng lưới blockchain. Các ứng dụng có thể đã sử dụng private blockchain bao gồm quản lý và kiểm tra cơ sở dữ liệu. Một số private blockchain phổ biến như: Ripple, Everledger và Eris. So với public blockchain, private blockchain có kích thước nhỏ hơn do số lượng người dùng tham gia nhỏ, do đó việc xác minh các khối mới không tốn nhiều thời gian và công suất.Ngoài ra, nó còn cung cấp sự riêng tư tốt hơn vì chỉ những người dùng được xác định trong mạng blockchain mới có thể đọc các giao dịch.
* Federated blockchain (blockchain liên kết): Nó được coi là một phần blockchain riêng tư, được vận hành dưới sự quản lý của một nhóm các công ty hoặc tổ chức. Không giống như public blockchain, federatedblockchain nhanh hơn và mang lại khả năng mở rộng cũng như quyền riêng tư tốt hơn. Ví dụ về các blockchains liên kết là R3, EWF và B3i.

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiêu chí** | **Public blockchain** | **Private Blockchain** | **Federated Blockchain** |
| Truy cập | Mọi người | Nhũng người trong cùng một tổ chức | Nhiều tổ chức liên kết với nhau |
| Tốc độ | Chậm | Nhanh | Nhanh |
| Hiệu suất | Thấp | Cao | Cao |
| Bảo mật | PoW, PoS và các cơ chế đồng thuận khác | Người tham gia được quyền phê duyệt và biểu quyết | Người tham gia được quyền phê duyệt và biểu quyết |
| Tính bất biến | Gần như không thể làm giả | Có thể làm giả | Có thể làm giả |
| Quy trình đồng thuận | Không được phép và ẩn danh | Được phép và không ẩn danh | Được phép và không ẩn danh |
| Network | Phi tập trung | Nửa phi tập trung | Nửa phi tập trung |
| Nội dung | Nội dung gốc | Bất kỳ nội dung nào | Bất kỳ nội dung nào |

Bảng 1 Các tiêu chí trong blockchain

### Cách thức hoạt động của Blockchain

Trong một thời gian dài, sổ cái đã được sử dụng như một phương tiện để các chủ ngân hàng và chính phủ lưu trữ các giao dịch khác nhau liên quan đến sở hữu đất đai và các hoạt động khác đòi hỏi phải duy trì hồ sơ giao dịch. Duy trì và xây dựng mối quan hệ tin cậy giữa các bên của một giao dịch nhất định là vấn đề lớn, vì vậy ngân hàng hoặc văn phòng chính phủ được sử dụng như một cơ quan trung ương để thực hiện các thay đổi cần thiết trong giao dịch và thiết kế hợp đồng để xác định ai sở hữu cái gì. Do đó, việc phân biệt giao dịch thật và giả chỉ do cơ quan trung ương thực hiện.

Người quản lý sổ cái (ngân hàng hoặc văn phòng chính phủ) đã xây dựng sự tin cậy cần thiết, vì vậy mọi người có thể bán và mua mà không phải lo lắng vì người quản lý tập trung kiểm soát tài khoản lưu trữ thông tin của họ trên sổ cái. Các sổ cái này hoàn toàn tập trung, trong đó cá nhân hoặc tổ chức bên thứ ba được tất cả người dùng tin cậy và có toàn quyền kiểm soát việc quản lý giao dịch. Ngoài ra, các sổ cái này được cất trong hộp đen vì nội dung chỉ hiển thị cho người quản lý sổ cái.

Mặt khác, blockchain cung cấp các chức năng tương tự về lưu trữ và duy trì các giao dịch nhưng không cần bên thứ ba (người quản lý sổ cái). Nó giải quyết vấn đề của cơ quan trung tâm xác minh các giao dịch bằng cách phân quyền sổ cái, trong đó mỗi người dùng tham gia trong mạng blockchain giữ một bản sao của sổ cái gốc. Ngoài ra, bất kỳ người dùng nào tham gia đều có thể yêu cầu thêm giao dịch, tuy nhiên, giao dịch chỉ được thêm vào khối nếu phần lớn người dùng tham gia vào mạng lưới blockchain xác minh nó. Việc kiểm tra tự động được thực hiện một cách đáng tin cậy đối với mỗi người dùng để tạo ra một sổ cái nhanh và được bảo vệ, có khả năng chống giả mạo đáng kể đối với các giao dịch và các khối.

Khi một giao dịch được xác minh, nó sẽ được thêm và liên kết với các giao dịch khác trong một khối, được liên kết với các khối trước đó trong sổ cái thông qua dấu thời gian và hàm băm. Điều này tạo thành các chuỗi khối, tạo ra cái được gọi là blockchain. Khi khối mời được tạo, tất cả người dùng tham gia vào mạng blockchain bắt đầu tìm kiếm khối tiếp theo bằng cách giải hàm toán học phức tạp và tạo một khối giao dịch được mã hóa để thêm nó vào sổ cái. Quá trình này được gọi là khai thác, trong đó tất cả người dùng cạnh tranh để tạo ra khối mới. Đầu tiên tạo một khối nguồn và thêm nó vào sổ cái sẽ được thưởng tổng số phí cho các giao dịch của nó. Phí được áp dụng cho mỗi giao dịch. Vì các khối liên quan đến một số lượng lớn các giao dịch được thêm vào nhiều lần, có thể thu nhiều khoản phí.

Sổ cái do tất cả người dùng tham gia trong mạng nắm giữ được cập nhật khi một khối mới được thêm vào. Nếu khối mới được thêm vào đã được xác minh bởi tất cả người dùng tham gia và tất cả các giao dịch của khối đó là chính xác, khối sẽ được thêm vào và tồn tại vĩnh viễn trong sổ cái dưới dạng hồ sơ công khai. Nếu xung đột được phát hiện, khối sẽ bị loại bỏ. Để phá huỷ sổ kế toán cổ điển cần một cuộc tấn công vào bên thứ ba (người quản lý tập trung). Mặc dù blockchain là bất biến, vì vậy nếu có một nỗ lực xấu nhằm thay đổi liên hệ của bất kỳ giao dịch nào, điều này sẽ cần tính toán PoW lặp lại cho khối liên quan và tất cả các khối khác sau đó. Các phép tính rất khó thực hiện trừ khi hầu hết người dùng trong mạng blockchain là độc hại. Ngoài ra, khả năng có sổ cái giả không tồn tại vì tất cả người dùng tham gia đều có bản sao sổ cái chính xác của họ để đối chiếu.

### Bảo mật và quyền riêng tư trong IoT sử dụng machine learning và Blockchain

Bảo mật và quyền riêng tư của người dùng đã trở thành mối quan tâm đáng kể do sự tham gia của các thiết bị Internet of Things (IoT) trong nhiều ứng dụng. Các mối đe dọa mạng đang phát triển với tốc độ bùng nổ khiến các biện pháp bảo mật và quyền riêng tư hiện có không đủ. Do đó, các thuật toán Machine Learning (ML) được sử dụng để tạo ra kết quả đầu ra chính xác từ database có độ lớn và phức tạp, nơi các kết quả đầu ra được tạo có thể được sử dụng để dự đoán và phát hiện các lỗ hổng trong các hệ thống IoT. Ngoài ra còn một số phương pháp ứng dụng blockchain. Một số nghiên cứu đã được thực hiện trên ML hoặc BC.

#### Các mối đe dọa trong IOT - Blockchain

IoT là một mạng lưới các IoT đề cập đến một số lượng lớn các thiết bị cảm biến không đồng nhất giao tiếp với nhau, trong mạng LAN hoặc qua Internet. Các mối đe dọa IoT khác với các mạng thông thường đáng kể là do các nguồn lực có sẵn của các thiết bị đầu cuối. Các thiết bị IoT có bộ nhớ hạn chế và sức mạnh tính toán, trong khi Internet thông thường bao gồm các máy chủ mạnh mẽ và máy tính với nguồn tài nguyên dồi dào. Do đó, một mạng truyền thống có thể được bảo mật bởi các lớp bảo mật đa yếu tố và các giao thức phức tạp, đây là điều mà một hệ thống IoT thời gian thực không thể có được Trái ngược với các mạng truyền thống, các thiết bị IoT sử dụng các phương tiện truyền thông không dây kém an toàn hơn như như LoRa, ZigBee, 802.15.4 và 802.11a/b/n/g/p. Cuối cùng, do chức năng dành riêng cho ứng dụng và thiếu hệ điều hành phổ biến, các thiết bị IoT có nội dung và định dạng dữ liệu khác nhau, gây khó khăn cho việc phát triển một giao thức bảo mật tiêu chuẩn. Tất cả những hạn chế này làm cho IoT có xu hướng bảo mật đa và các mối đe dọa về quyền riêng tư, do đó mở ra các địa điểm cho các kiểu tấn công khác nhau.

Xác suất của một cuộc tấn công trong một mạng tăng lên theo kích thước mạng. Do đó, IoT mạng có nhiều lỗ hổng hơn mạng truyền thống, ví dụ: văn phòng công ty. Đặc biệt, các thiết bị IoT giao tiếp với nhau thường là các thiết bị đa nhà cung cấp với các tiêu chuẩn và giao thức. Giao tiếp giữa các thiết bị như vậy là một thách thức, đòi hỏi một bên thứ ba đáng tin cậy để làm cầu nối. Hơn nữa, một số nghiên cứu đã nêu lên mối quan tâm của cập nhật phần mềm thường xuyên cho hàng tỷ thiết bị thông minh

Diagram

Description automatically generated

Hình 4 Tổng quan các mối đe dọa đối với thiết bị IoT

* Denial of Service (Dos) có cách triển khai đơn giản nhất trong số tất cả các cuộc tấn công bảo mật. Hơn nữa, ngày càng có nhiều thiết bị IoT với các tính năng bảo mật yếu kém đã khiến DoS trở thành một công cụ yêu thích của những kẻ tấn công. Mục tiêu cốt lõi của cuộc tấn công DoS đó là xâm nhập vào mạng với các yêu cầu không hợp lệ, dẫn đến cạn kiệt tài nguyên mạng, chẳng hạn như tiêu thụ băng thông. Do đó, các dịch vụ không có sẵn cho người dùng chính hãng. DoS phân tán (DDoS) là phiên bản nâng cao của cuộc tấn công DoS, trong đó nhiều nguồn tấn công một mục tiêu duy nhất khiến việc theo dõi và tránh cuộc tấn công trở nên khó khăn hơn.

Mặc dù có nhiều kiểu tấn công DDoS khác nhau nhưng chúng đều có cùng một mục tiêu. Một số biến thể của các cuộc tấn công DDoS là SYN flooding (trong đó kẻ tấn công gửi liên tiếp các yêu cầu SYN đến một mục tiêu), Internet Control Message Protocol (ICMP) (trong đó một số lượng lớn các gói ICMP được phát đi bằng cách sử dụng IP giả mạo), các cuộc tấn công crossfire (sử dụng một mạng botnet phức tạp và quy mô lớn để thực hiện cuộc tấn công) và User Datagram Protocol (UDP) (gửi một số lượng lớn các gói UDP đến các cổng ngẫu nhiên trên một nạn nhân từ xa). Tấn công botnet là một kiểu tấn công DDoS trong mạng IoT. Mạng botnet là một mạng lưới các nút (thiết bị) IoT bị xâm nhập để khởi động một cuộc tấn công vào một mục tiêu cụ thể, ví dụ: máy chủ ngân hàng.

* Man-in-the-middle: Các cuộc tấn công Man-in-the-middle (MiTM) là một trong những cuộc tấn công lâu đời nhất trong thế giới mạng. Giả mạo và mạo danh có thể được phân loại là các cuộc tấn công MiTM. Tương tự, trong phân loại SSL, kẻ tấn công có thể lợi dụng các cuộc tấn công như vậy để tự kết nối với máy chủ bằng HTTPS liên quan.
* Malware: là tên viết tắt của phần mềm độc hại. Trong vài năm qua, số lượng thiết bị IoT đang tăng lên cùng với các bản vá lỗi phần mềm IoT thường xuyên, điều đó có thể bị kẻ tấn công lợi dụng để cài đặt phần mềm độc hại trên thiết bị và thực hiện các hoạt động độc hại. Phần mềm độc hại thường được hiểu là tồn tại dưới dạng vi rút, phần mềm gián điệp, sâu, trojan, rootkit hoặc quảng cáo độc hại. Các sản phẩm smarthome, thiết bị chăm sóc sức khỏe và cảm biến xe cộ là một vài ví dụ có thể bị xâm phạm. Azmoodeh và cộng sự đã nghiên cứu phần mềm độc hại trên Internet of Battlefield Things (IoBT). Những kẻ tấn công như vậy thường được nhà nước bảo trợ, có nguồn lực tốt hơn và được đào tạo chuyên nghiệp.

#### Các mối đe doạ về quyền riêng tư

Ngoài các mối đe dọa về bảo mật, người dùng IoT và dữ liệu của họ dễ bị tấn công quyền riêng tư, chẳng hạn như các cuộc tấn công sniffing, ẩn danh và suy luận. Trong mọi trường hợp, tác động đến tính bảo mật của dữ liệu, nơi dữ liệu có thể ở trạng thái nghỉ hoặc chuyển động. Trong phần này, chúng ta thảo luận về các cuộc tấn công quyền riêng tư khác nhau.

* MiTM: Các cuộc tấn công MiTM có thể được phân loại thành Các cuộc tấn công MiTM chủ động (AMA) và Các cuộc tấn công MiTM bị động (PMA). PMA lắng nghe thụ động quá trình truyền dữ liệu giữa hai thiết bị. Mặc dù PMA vi phạm quyền riêng tư nhưng chúng không làm thay đổi dữ liệu. Kẻ tấn công có quyền truy cập vào một thiết bị có thể âm thầm quan sát trong nhiều tháng trước khi thực hiện cuộc tấn công. Với số lượng ngày càng tăng của máy ảnh trong các thiết bị IoT như đồ chơi, điện thoại thông minh và đồng hồ đeo tay, tác động của PMA, chẳng hạn như nghe trộm và đánh hơi, là vô cùng lớn. Mặt khác, AMA đang tích cực tham gia vào việc lạm dụng dữ liệu có được bằng cách tương tác với người dùng giả danh người khác, ví dụ: mạo danh hoặc truy cập hồ sơ mà không có sự đồng ý, tấn công ủy quyền….
* Data privacy (bảo mật dữ liệu): Tương tự như các cuộc tấn công MiTM, các cuộc tấn công quyền riêng tư dữ liệu có thể được phân loại thành Các cuộc tấn công dữ liệu riêng tư chủ động (ADPA) và các cuộc tấn công dữ liệu riêng tư bị động (PDPA). Quyền riêng tư dữ liệu liên quan đến rò rỉ dữ liệu, giả mạo dữ liệu, đánh cắp danh tính và xác định lại. Các cuộc tấn công nhận dạng lại còn được gọi là các cuộc tấn công suy luận và dựa trên các cuộc tấn công ẩn danh, phát hiện vị trí và tổng hợp thông tin. Trong các cuộc tấn công này, mục tiêu chính của tin tặc là thu thập dữ liệu từ nhiều nguồn và tiết lộ danh tính của các mục tiêu. Một số kẻ tấn công có thể sử dụng dữ liệu thu thập được để mạo danh một mục tiêu riêng lẻ. Bất kỳ cuộc tấn công nào làm thay đổi dữ liệu, chẳng hạn như giả mạo dữ liệu, có thể được phân loại là ADPA, trong khi re-identification và rò rỉ dữ liệu là ví dụ của PDPA.

Table

Description automatically generated

Hình 5Security threats and Privacy threats

#### Các phương thức sử dụng Machine leaning- Blockchain

Thông qua một số bài báo đã được công bố, Chúng em đã tổng hợp được một số phương pháp sau:

* Restuccia và cộng sự của ông đã cố gắng trình bày phân loại các mối đe dọa bảo mật IoT hiện có và các giải pháp của chúng trong SDN bằng cách sử dụng các thuật toán ML. Họ cũng gợi ý rằng vì nhiệm vụ chính của hệ thống IoT là thu thập dữ liệu từ các thiết bị IoT, nên có thể chia quá trình thu thập dữ liệu thành 3 bước: xác thực IoT, mạng không dây IoT, tổng hợp & xác thực dữ liệu IoT. Nghiên cứu đã đưa ra một đánh giá ngắn gọn về các thuật toán ML được sử dụng để giảm thiểu các cuộc tấn công bảo mật, ví dụ: để phát hiện các cuộc tấn công độc hại xuyên lớp, học Bayes được sử dụng và để đánh giá tính hợp lệ của dữ liệu, mạng thần kinh được sử dụng.
* Sharmeen và cộng sự có mục tiêu nhằm hỗ trợ các nhà phát triển ứng dụng sử dụng Giao diện chương trình ứng dụng (API) một cách an toàn, trong quá trình phát triển các ứng dụng cho mạng IoT công nghiệp. Để phát hiện phần mềm độc hại, các tác giả gợi ý rằng mô hình ML có thể được đào tạo bằng cách sử dụng ba loại tính năng bao gồm tĩnh, động và kết hợp. Phân tích chi tiết của từng loại tính năng được thực hiện bằng cách sử dụng các số liệu hiệu suất của tập dữ liệu, kỹ thuật trích xuất tính năng, tiêu chí lựa chọn tính năng, độ chính xác và phương pháp phát hiện. Một số phương pháp phát hiện cho từng bộ tính năng đã được phân tích, nhưng các phương pháp thường được sử dụng là RF, SVM, KNN, J48 và NB. Bài báo kết luận rằng sự phân tích kết hợp nhằm cung cấp sự linh hoạt trong việc lựa chọn cả các tính năng tĩnh và động để cải thiện độ chính xác trong quá trình phát hiện. Ở đây chúng em sẽ đi sâu vào phương pháp này vì nó áp dụng cho android -một hệ điều hành rất phổ biến hiện nay. Thành phần đầu tiên của hệ thống pháp hiện phần mềm độc hại này là dataset. Dataset bao gồm các phần mềm độc hại và các apps khi bình thường. Dataset cần để phân tích các hành vi của mã độc. Nguồn mã độc thì đến từ các trang web như là Drebin data set, Virus share…. Apps thì là Google Play, App China, Amazon, Android market…. Thành phần thứ hai là Feature Extractor dùng để trích xuất những phần mong muốn từ malware và benign apps. Dựa trên phân loại các file đã trích xuất, chúng ta có thể lập danh mục thành feature extractor động, tĩnh, hybrid.

Diagram

Description automatically generated

Hình 6 Types of feature extractor

Static features thường là: Permission, API call, String extracted, Native commands, XML elements, Meta data, Intents, Broadcast receivers, Hardware components, … Những thành phần này có thể thu thập được trong manifest file, dex file và byte code, tool được dùng là APK.

Dynamic features thường là: System call, Network traffic, SMS, Process id, Process information, Memory usage, IP address, Log events Power consumption, System component, User interaction. Được trích xuất bằng cách dùng máy ảo thực thi chương trình.

Hybrid features thường là: system call and permission, system call and API call, permission and network traffic, API call, intents and system call… Là bao gồm động và tĩnh kết hợp với nhau.

Thành phần thứ ba là Feature selection: một phần quan trọng trong việc phát hiện phần mềm độc hại. Có nhiều tính năng, nhưng chúng ta cần chọn một vài tính năng trong số chúng, điều này sẽ cung cấp độ chính xác tốt hơn trong tiến trình. Các tính năng được chọn là loại sử dụng rộng rãi cho Điện thoại di động:

* Thuật toán thu thập thông tin
* Chọn hầu hết các tính năng được sử dụng trong nghiên cứu trước đây
* Chọn một tập hợp con của tất cả các tính năng (top 20, top 50…)

Detection method: Phương pháp phát hiện hay còn gọi là phân loại được dùng để xác định apps có là phần mềm động hại hoặc không. Có hai hoặc ba lớp và mỗi lớp chứa một bộ phân loại để cải thiện độ chính xác của hệ thống phát hiện.Trong các bộ phân loại song song, có nhiều bộ phân loại riêng lẻ khác nhau. Kết quả đầu ra của các bộ phân loại này được kết hợp để có được độ chính xác cao hơn. Các bộ phân loại khác như AHP và tính toán hình phạt không sử dụng phương pháp học máy. Các bộ phân loại học máy phổ biến được sử dụng để phát hiện phần mềm độc hại trên thiết bị di động Android là: SVM, KNN, J48, RF, Naïve Bayes, C4.5, …

Diagram

Description automatically generated

Hình 7 Các phương pháp sử dụng

#### Ứng dụng Machine learning trong quyền riêng tư

Machine learning trích xuất thông tin hữu ích từ dữ liệu thô, trong khi quyền riêng tư được bảo toàn bằng cách che giấu thông tin. Theo nghiên cứu của Al-Rubaie et al, hệ thống ML có ba môđun: (i) đầu vào, (ii) tính toán, và (iii) đầu ra. Nghiên cứu cũng tuyên bố rằng quyền riêng tư chỉ có thể được bảo toàn nếu cả ba mô-đun đều thuộc quyền sở hữu của một thực thể duy nhất.

Ngày nay, dữ liệu được thu thập trên toàn thế giới bởi hàng tỷ thiết bị IoT như điện thoại thông minh, cảm biến giám sát sức khỏe, camera tốc độ và cảm biến nhiệt độ, do đó không thể duy trì điều kiện sở hữu duy nhất. Vấn đề này đã thúc đẩy các nhà nghiên cứu quan tâm đến việc đề xuất các thuật toán ML bảo vệ quyền riêng tư mới hơn và được cải thiện. Ví dụ, việc thiếu các cơ chế bảo vệ quyền riêng tư trong môi trường VANET đã được nêu ra. Trong VANET, các nút Phương tiện có xu hướng học cộng tác, gây ra lo ngại về quyền riêng tư, nơi một nút độc hại có thể lấy dữ liệu nhạy cảm bằng cách suy luận từ dữ liệu được quan sát. Một nút duy nhất có tài nguyên tính toán và bộ nhớ hạn chế. Giải pháp là bằng cách sử dụng IDS hợp tác với các thuật toán ML phân tán và giải quyết các vấn đề về quyền riêng tư bằng cách đề xuất các khái niệm về quyền riêng tư khác biệt động để bảo vệ quyền riêng tư của tập dữ liệu đào tạo.

Hệ thống giám sát giao thông người và dịch vụ chăm sóc sức khỏe là hai trong số các công nghệ cảm biến IoT phổ biến nhất và cần được cải tiến liên tục. Dữ liệu hữu ích và hiệu quả nhất cho các ứng dụng đó được thu thập trực tiếp từ người dùng thông qua Mobile CrowdSensing (MCS), nơi thông tin quan tâm được trích xuất và những người tham gia tải lên các báo cáo cảm nhận về môi trường xung quanh của họ lên máy chủ MCS. Việc chia sẻ thông tin này gây ra các mối đe dọa về quyền riêng tư đáng kể đối với những người tham gia máy chủ MCS. Hệ thống dễ bị rò rỉ quyền riêng tư (liên quan đến thông tin cá nhân của người dùng), các cuộc tấn công giả mạo (gửi báo cáo giả đến máy chủ để giảm nỗ lực phát hiện) và các mối đe dọa liên tục nâng cao (gây rò rỉ quyền riêng tư trong một thời gian dài). Cuộc khảo sát đề xuất Mạng thần kinh sâu (DNN) và Mạng thần kinh hợp pháp (CNN) để bảo vệ quyền riêng tư, và Mạng tín ngưỡng sâu (DBN) và Mạng Q-Deep (DQN) để chống lại giả mạo.

#### Các phương pháp ứng dụng Blockchain trong bảo mật

Bảo mật là trọng tâm hàng đầu đối với bất kỳ trường hợp sử dụng IoT nào. Rất nhiều phương pháp dựa trên các kỹ thuật BC đã xuất hiện để giải quyết các vấn đề bảo mật trong IoT. Một nghiên cứu về bảo mật IoT đã được trình bày bởi Banerjee et al., được phân loại thành các kỹ thuật bảo mật như hệ thống phát hiện và ngăn chặn xâm nhập (IDPS), bảo mật cộng tác và bảo mật dự đoán. Hơn nữa, IDPS được phân loại theo cách tiếp cận, cấu trúc mạng và ứng dụng. Sau đó, bảo mật cộng tác và bảo mật dự đoán được thảo luận chi tiết. Trong cùng một nghiên cứu, các kỹ thuật bảo mật cộng tác được phân loại theo cấu trúc mạng và ứng dụng. Phần tiếp theo của nghiên cứu này là tính toàn vẹn của các bộ dữ liệu IoT hiện có được làm nổi bật và các tác giả đề xuất rằng một tiêu chuẩn dựa trên BC nên được phát triển để đảm bảo tính toàn vẹn trong các bộ dữ liệu được chia sẻ.

Ở đây, chúng em sẽ trình bày một số tiềm năng mà Minhaj Ahmad Khan and Khaled Salah đã trình bày trong bài báo cáo của họ.

Address Space: Blockchain có không gian địa chỉ 160 bit, trái ngược với không gian địa chỉ IPv6 có không gian địa chỉ 128 bit. Một địa chỉ blockchain là 20 byte hoặc một 160 bit-hash của khóa công khai được tạo bởi ECDSA. Với địa chỉ 160-bit, blockchain có thể tạo và phân bổ địa chỉ ngoại tuyến cho khoảng 1,46 ∗ 1048 thiết bị IoT. Xác suất xung đột địa chỉ là khoảng 1048, được coi là đủ an toàn để cung cấp GUID (Mã định danh duy nhất toàn cầu) không yêu cầu đăng ký hoặc xác minh tính duy nhất khi gán và cấp phát địa chỉ cho thiết bị IoT. Với blockchain, cơ quan quản lý và quyền hạn tập trung, chẳng hạn như Cơ quan quản lý số được ấn định trên Internet (IANA), bị loại bỏ. Hiện tại, IANA giám sát việc phân bổ địa chỉ IPv4 và IPv6 toàn cầu, Hơn nữa, blockchain cung cấp nhiều hơn 4,3 tỷ địa chỉ so với IPv6, do đó làm cho blockchain trở thành một giải pháp có khả năng mở rộng hơn cho IoT so với IPv6. Cuối cùng, cần lưu ý rằng nhiều thiết bị IoT bị hạn chế về bộ nhớ và dung lượng tính toán, do đó sẽ không thích hợp để chạy ngăn xếp IPv6.

Identity of Things (IDoT) and Governance: Quản lý Danh tính và Truy cập (IAM) cho IoT đang phải giải quyết một số vấn đề thách thức một cách hiệu quả, an toàn và đáng tin cậy. Một thách thức liên quan đến quyền sở hữu và mối quan hệ nhận dạng của các thiết bị IoT. Quyền sở hữu thiết bị thay đổi trong suốt thời gian tồn tại của thiết bị từ nhà sản xuất, nhà cung cấp, nhà bán lẻ và người tiêu dùng. Quyền sở hữu của người tiêu dùng đối với thiết bị IoT có thể bị thay đổi hoặc thu hồi, nếu thiết bị được bán lại, ngừng hoạt động hoặc bị xâm phạm. Quản lý các thuộc tính và mối quan hệ của một thiết bị IoT là một thách thức khác. Các thuộc tính của một thiết bị có thể bao gồm nhà sản xuất, chế tạo, loại, số sê-ri, tọa độ GPS triển khai, vị trí, v.v. Ngoài các thuộc tính, khả năng và tính năng, thiết bị IoT có các mối quan hệ. Các mối quan hệ IoT có thể bao gồm thiết bị với con người, thiết bị với thiết bị hoặc thiết bị với dịch vụ. Các mối quan hệ thiết bị IoT có thể được triển khai bởi, được sử dụng bởi, được vận chuyển bởi, được bán bởi, được nâng cấp bởi, được sửa chữa bởi, được bán bởi, v.v.

Blockchain có khả năng giải quyết những thách thức này một cách dễ dàng, an toàn và hiệu quả. Blockchain đã được sử dụng rộng rãi để cung cấp đăng ký danh tính đáng tin cậy và được ủy quyền, theo dõi quyền sở hữu và giám sát các sản phẩm, hàng hóa và tài sản. Các phương pháp tiếp cận như TrustChain được đề xuất để cho phép các giao dịch đáng tin cậy sử dụng blockchain trong khi duy trì tính toàn vẹn của các giao dịch trong môi trường phân tán. Các thiết bị IoT cũng không ngoại lệ. Blockchain có thể được sử dụng để đăng ký và cung cấp danh tính cho các thiết bị IoT được kết nối, với một tập hợp các thuộc tính và các mối quan hệ phức tạp có thể được tải lên và lưu trữ trên sổ cái phân tán blockchain.

Blockchain cũng cung cấp khả năng quản lý, quản trị và theo dõi phi tập trung đáng tin cậy tại mọi điểm trong chuỗi cung ứng và vòng đời của thiết bị IoT. Chuỗi cung ứng có thể bao gồm nhiều thành phần như nhà máy, nhà cung cấp, nhà cung cấp, nhà phân phối, người giao hàng, người cài đặt, người sở hữu, người sửa chữa, người cài đặt lại, v.v. Các cặp khóa có thể được thay đổi và cấp lại tại nhiều điểm trong vòng đời của thiết bị IoT. Việc phát hành cặp khóa có thể được thực hiện ban đầu bởi nhà sản xuất, sau đó bởi chủ sở hữu, kiểm tra định kỳ sau khi triển khai.

Diagram

Description automatically generated

Hình 8 IoT device lifecycle security management

Data Authentication and Integrity: Theo thiết kế, dữ liệu được truyền bởi các thiết bị IoT được kết nối với mạng blockchain sẽ luôn được chứng minh bằng mật mã và được ký bởi người gửi thực sự, người có khóa công khai và GUID duy nhất, và do đó đảm bảo xác thực và tính toàn vẹn của dữ liệu được truyền. Ngoài ra, tất cả các giao dịch được thực hiện đến hoặc bằng thiết bị IoT đều được ghi lại trên sổ cái phân tán blockchain và có thể được theo dõi một cách an toàn.

Authentication, Authorization, and Privacy: Hợp đồng thông minh blockchain có khả năng cung cấp quy tắc xác thực phi tập trung và logic để có thể cung cấp xác thực đơn và đa bên cho thiết bị IoT. Ngoài ra, hợp đồng thông minh có thể cung cấp quy tắc truy cập ủy quyền hiệu quả hơn cho các thiết bị IoT được kết nối với mức độ ít phức tạp hơn khi so sánh với các giao thức ủy quyền truyền thống như Quản lý truy cập dựa trên vai trò (RBAC), OAuth 2.0, OpenID, OMA DM và LWM2M. Ngày nay, các giao thức này được sử dụng rộng rãi để xác thực, ủy quyền và quản lý thiết bị IoT. Hơn nữa, quyền riêng tư của dữ liệu cũng có thể được đảm bảo bằng cách sử dụng các hợp đồng thông minh thiết lập các quy tắc, điều kiện và thời gian truy cập để cho phép một số cá nhân hoặc nhóm người dùng hoặc máy móc sở hữu, kiểm soát hoặc có quyền truy cập vào dữ liệu ở chế độ nghỉ ngơi hoặc đang chuyển tiếp. Các hợp đồng thông minh cũng có thể giải thích rõ ai có quyền cập nhật, nâng cấp, vá lỗi phần mềm IoT.

Secure Communications: Các giao thức giao tiếp IoT ứng dụng như giao thức HTTP, MQTT, CoAP hoặc XMPP, hoặc thậm chí các giao thức liên quan đến định tuyến như của RPL và 6LoWPAN, không được bảo mật theo thiết kế. Các giao thức như vậy phải được bao bọc trong các giao thức bảo mật khác như DTLS hoặc TLS đối với các giao thức ứng dụng và nhắn tin để cung cấp giao tiếp an toàn. Tương tự, đối với định tuyến, IPSec thường được sử dụng để cung cấp bảo mật cho các giao thức RPL và 6LoWPAN. DTLS, TLS, IPSec, hoặc thậm chí là các giao thức TinyTLS trọng lượng nhẹ, nặng và phức tạp về yêu cầu tính toán và bộ nhớ, đồng thời phức tạp với việc quản lý tập trung và phân phối khóa bằng cách sử dụng giao thức phổ biến của PKI. Với blockchain, khóa quản lý và phân phối hoàn toàn bị loại bỏ, vì mỗi thiết bị IoT sẽ có GUID duy nhất của riêng mình và cặp khóa bất đối xứng sau khi được cài đặt và kết nối với mạng blockchain. Điều này cũng sẽ dẫn đến việc đơn giản hóa đáng kể các giao thức bảo mật khác như của DTLS, không cần xử lý và trao đổi chứng chỉ PKI ở giai đoạn bắt tay trong trường hợp DTLS hoặc TLS (hoặc IKE trong trường hợp IPSec) để thương lượng các tham số của bộ mật mã cho mã hóa và băm và để thiết lập khóa chính và khóa phiên. Do đó, các giao thức bảo mật trọng lượng nhẹ sẽ phù hợp vì thế phân tầng các yêu cầu đối với tài nguyên máy tính và bộ nhớ của các thiết bị IoT trở nên khả thi hơn.

#### Các phương pháp ứng dụng Blockchain trong quyền riêng tư

Cón hiều bài phân tích về vấn đề này. Trong đó nổi trội nhất là bài báo A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications. Họ đã đã cung cấp tổng quan chi tiết về các vấn đề quyền riêng tư trong các hệ thống IoT dựa trên BC. Ở đây quyền riêng tư của người dùng được thực hiện bằng cách sử dụng phương pháp hợp tác nút, trong đó máy chủ đưa ra các task cũng như giá của nó, được trả trước trên BC. Người dùng sẽ thực hiện nhiệm vụ và tải lên dữ liệu của các cảm biến, và cuối cùng, người dùng được trả tiền theo thành tích của họ. Để đạt được sự riêng tư về dữ liệu người dùng, các tác giả đã đề xuất ẩn danh, trong đó nhiệm vụ không được giao cho một cá nhân, mà là một nhóm và dữ liệu được cảm biến được thu thập cũng ở dạng một nhóm, bảo vệ quyền riêng tư của một người dùng.

Diagram

Description automatically generated

Hình 9 Mô hình hoạt động

#### Các phương pháp ứng dụng blockchain và ML trong bảo mật

Trong lớp mạng, các nút liên kết có thể giao tiếp thông qua một mạng P2P. Mạng có các đặc điểm của sự phân quyền và thay đổi động, liên quan đến cách thức kết nối mạng và cơ chế giao tiếp giữa các nút. Các nút bao gồm các máy chủ, được phân tán về mặt địa lý. Không có nút trung tâm và mọi nút đều có thể tự do tham gia hoặc thoát khỏi mạng. Khi một nhiệm vụ kiểm tra được hoàn thành, thông tin phát hiện và thông tin khối đồng bộ hóa thường được gửi đến tất cả các nút CB bằng chế độ rơle-lặp. Mỗi nút gửi thông tin đến nút hàng xóm của nó và nút hàng xóm chuyển tiếp thông tin đã gửi đến nút hàng xóm của chính nó. Bằng cách này, nó dần dần lan rộng khắp mạng lưới. Thông tin khối đồng bộ sử dụng một mẫu phản hồi yêu cầu. Đầu tiên, nút gửi chiều cao khối của chính nó (tương tự như ID) đến nút hàng xóm. Nếu chiều cao của nút lân cận nhỏ hơn chiều cao của nút này, khối sẽ yêu cầu lấy thông tin còn thiếu. Nếu chiều cao của nút láng giềng cao hơn, nút láng giềng sẽ nhận thông tin khối ngược lại. Tất cả các nút liên tục trao đổi khối thông tin với các nút lân cận của chúng.

Trong lớp lưu trữ, các tính năng của mã độc hại được lưu trữ.Thông tin thực tế cũng được cung cấp trong lớp này để tạo thành cơ sở dữ liệu về phần mềm độc hại phân tán trong Consortium Blockchain. Mỗi khối chứa một trang về các tính năng của phần mềm độc hại và thông tin khác, bao gồm cả phần đầu khối và dữ liệu khối. Sau khi các khối này được xác nhận, chúng không thể được sửa đổi. Đầu khối chứa thông tin như dấu thời gian, Prehash, Nonce, v.v. Mỗi khối sử dụng giá trị mã hóa băm từ khối trước đó để xác thực thông tin. Dữ liệu khối bao gồm thông tin cụ thể liên quan đến các tính năng mã độc hại, chẳng hạn như tập hợp hành vi nhạy cảm, quyền và gói cài đặt

Trong lớp hỗ trợ, giao diện giữa người dùng và cơ sở dữ liệu của mã độc được cung cấp, bao gồm các chức năng của cơ chế đồng thuận, mã hóa dữ liệu, chữ ký số, quản lý khóa, xác thực danh tính, kiểm soát truy cập, quản lý đồng bộ hóa, v.v. Cơ chế đồng thuận xác định tính hợp pháp của các nút trong Consortium Blockchain, xác nhận thông tin đã gửi và đảm bảo tính hợp pháp và hợp lệ của thông tin khối trong cơ sở thực tế. Mã hóa dữ liệu là chức năng cơ bản của hệ thống bảo mật. Chữ ký kỹ thuật số làm cho dữ liệu do người dùng gửi không thể phủ nhận và làm cho blockchain có khả năng giữ người dùng gửi dữ liệu bất hợp pháp. Quản lý khóa được sử dụng để quản lý thông tin khóa một cách an toàn và hiệu quả. Kiểm soát truy cập ngăn chặn người dùng độc hại thao túng dữ liệu bất hợp pháp. Quản lý đồng bộ hóa cập nhật cơ sở thực tế.

Trong lớp ứng dụng, các chương trình và giao diện cho các ứng dụng khác nhau được cung cấp. Người dùng có thể tương tác với các ứng dụng khác nhau mà không cần xem xét chi tiết về công nghệ nền tảng của blockchain. Các ứng dụng điển hình bao gồm phát hiện phần mềm độc hại, phát hiện sự kiện độc hại, theo dõi và trích xuất bằng chứng cũng như các ứng dụng lưu trữ kỹ thuật số. Các thành viên liên minh phát hiện cần xác nhận danh tính hợp pháp của người dùng. Nếu kết quả, hồ sơ hoặc bằng chứng của thử nghiệm được tải lên, một khối mới sẽ được tạo và thông tin liên quan sẽ được phát đi.

Graphical user interface, diagram, table

Description automatically generated

Hình 10Framework of CB-MDEE

Graphical user interface, text, application

Description automatically generated

Hình 11 Cấu trúc của blockchain

Diagram

Description automatically generated

Hình 12Structure of multi-feature detection of Android malware

#### Các phương pháp ứng dụng blockchain và ML trong bảo mật

Nhiều công ty dựa vào bộ dữ liệu lớn để tối ưu hóa đối tượng mục tiêu của họvà nâng cao lợi nhuận, nhưng dữ liệu đó chứa thông tin cá nhân nhạy cảm, chẳng hạn như Bộ phân loại ML yêu cầu tập dữ liệu để đào tạo. Các tập dữ liệu này được thu thập từ các sở thích khác nhau của nhiều người, có thể được khai thác bởi các người quan tâm. Do đó, điều quan trọng là phải bảo tồnquyền riêng tư của những người dùng đó và nếu được yêu cầu, hãy bồi thường cho họ vì những đóng góp của họ. Hơn nữa, bộ nhớ sẽ không thống nhất dẫn đến rò rỉ dữ liệu. Đề án được đề xuất sử dụng các hàm băm và Bộ phân loại dựa trên SVM bảo vệ quyền riêng tư đã được sử dụng để đào tạo dữ liệu được mã hóa được thu thập nhằm tìm kiếm giải pháp về quyền riêng tư. Nhiều công ty dựa vào bộ dữ liệu lớn để tối ưu hóa đối tượng mục tiêu của họ và mỗi miền có rất nhiều dữ liệu, có thể có lợi cho nghiên cứu và phát triển, nhưngdữ liệu không thể được chia sẻ với các bên thứ ba. Hơn nữa, cùng một dữ liệu có thể bị thao tác vàđặt ra nghi ngờ về tính toàn vẹn của nó.

Trong một nghiên cứu, nỗ lực tạo ra các mô hình DNN chống giả mạo đã được thực hiện với sự trợ giúp của BC. Sử dụng các thuộc tính BC như băm bắc cầu, mã hóa mật mã và bản chất phi tập trung, một kiến trúc có tên là DeepRing được đề xuất. Một sổ cái chung được chia sẻ lưu trữ trạng thái của mô hình. Khối Ouroboros lưu trữ tất cả các hàm băm của khối, được sử dụng để theo dõi khối bị xâm phạm trong trường hợp có bất kỳ cuộc tấn công giả mạo nào. Vì querent đã mã hóa truy vấn bằng khóa công khai của nó và đầu ra chỉ được mã hóa bằng khóa công khai của querent, nên không ai khác có thể truy cập kết quả mô hình. Tập trung vào các cuộc tấn công đối nghịch vào các tham số mạng, các tác giả đã so sánh kiến trúc DNN với kiến trúc DeepRing. Kiến trúc DNN không có BC sử dụng tập dữ liệu CIFAR-10, MNIST và Tiny ImageNet đã giảm độ chính xác của chúng lần lượt là 20,71%, 47% và 34%Tuy nhiên, DNN với BC bị mất độ chính xác 0%

Ngoài ra, một nghiên cứu khác của Fadaeddini et al người đã đề xuất một khuôn khổ trong đó quyền riêng tư của chủ sở hữu dữ liệu được duy trì bằng cách đào tạo mô hình chia sẻ trên dữ liệu của họ tại địa phương nhằm chứng minh kịch bản ứng dụng ô tô tự lái, sử dụng nền tảng Stellar BC cho cơ sở hạ tầng học sâu phi tập trung. Những người đóng góp được trả tiền cho công việc của họ vì họ đã giúp cải thiện độ chính xác của ô tô tự lái. Mô hình đã học được lưu trên một hệ thống tệp phân tán được gọi là IPFS (Hệ thống tệp liên phẳng), hệ thống này có khả năng chống lại các cuộc tấn công DDoS. Khung cũng kiểm soát tính xác thực của các đối tác máy tính để tránh bất kỳ hoạt động độc hại nào.

### Các ứng dụng của Blockchain

Hiện nay có rất nhiều ngành đã ứng dụng được những khả năng mà blockchain mang lại như:

#### Ngành âm nhạc

Do sự phát triển của Internet và khả năng tiếp cận dễ dàng với các phương tiện online khác nhau qua Internet, ngành công nghiệp âm nhạc đã trở thành một trong những ứng dụng có thể hưởng những lợi ích to lớn do công nghệ blockchain cung cấp. Ngành công nghiệp âm nhạc liên quan đến nhiều đối tượng khác nhau như nhà sản xuất, nhạc sĩ, ca sĩ, hãng thu âm và nhà cung cấp dịch vụ phát trực tuyến. Quyền sở hữu âm nhạc đã thay đổi và trở nên khó khăn hơn do sự phát triển của Internet. Cần có sự minh bạch trong các khoản thanh toán bản quyền và quyền sở hữu cho các nhạc sĩ và nghệ sĩ.

Tích hợp ngành công nghiệp âm nhạc với công nghệ blockchain có thể giải quyết một số vấn đề liên quan đến tính minh bạch và thanh toán quyền sở hữu. Blockchain có thể được sử dụng để tạo cơ sở dữ liệu phân tán chính xác nhằm bảo vệ thông tin về quyền âm nhạc trong sổ cái. Ngoài ra, hợp đồng thông minh có thể được sử dụng để cung cấp hợp đồng kỹ thuật số và bảo mật cho ngành công nghiệp âm nhạc.

#### Ngành giáo dục

Giáo dục là một trong những ứng dụng áp dụng blockchain cho các ứng dụng thú vị và sáng tạo như quản lý chứng chỉ và bảng điểm, học bạ, quản lý hồ sơ học sinh. Blockchain có thể được sử dụng như một cơ sở dữ liệu phi tập trung để lưu trữ vĩnh viễn nhiều loại thông tin giáo dục khác nhau. Điều này có thể giúp các trường đại học áp dụng tiền điện tửđồ họachứng chỉ được ký và xác nhận trên blockchain cho phép cả nhà tuyển dụng và sinh viên truy cập dễ dàng.

Tích hợp blockchain với môi trường học tập có thể tạo ra các ứng dụng giáo dục sáng tạo, xây dựng một mô hình học tập mới, nơi trao đổi ý tưởng và khái niệm cùng với hệ thống theo dõi để đánh giá kết quả học tập. Blockchain có thể được sử dụng trong quy định về hợp đồng và thanh toán để đánh giá quá trình học tập và ghi lại tiến trình học tập, chẳng hạn như thanh toán học phí, giảng dạy với các sinh viên khác

#### Ngành Dịch vụ cộng đồng

Dữ liệu do các tổ chức chính phủ tạo ra được lưu hành nội bộ và không minh bạch đối với người dân và doanh nghiệp. Trong khi với việc sử dụng công nghệ blockchain, các bản ghi dữ liệu có thể được tạo và xác minh nhanh chóng với việc đảm bảo tính bảo mật và tính minh bạch của dữ liệu. Các tính năng của blockchain như chữ ký số và dấu thời gian được dự đoán sẽ cung cấp vô số lợi ích trong các dịch vụ công cộng để cho phép công dân xử lý các giao dịch và tạo tài khoản một cách độc lập mà không cần luật sư, chính phủ và các bên thứ ba.

Một số chính phủ bắt đầu áp dụng công nghệ blockchain để hỗ trợ các dịch vụ công cộng khác nhau cho công dân của họ. Ví dụ, chính phủ Estonia đã sử dụng công nghệ blockchain để cho phép công dân thực hiện một số nhiệm vụ bằng cách sử dụng thẻ ID của họ như bỏ phiếu, đăng ký kinh doanh, đặt đơn thuốc và thanh toán thuế. Ngoài ra, bộ phận lương hưu và công việc của Vương quốc Anh đã bắt đầu áp dụng blockchain trong các khoản thanh toán phúc lợi. Ngoài ra, Thụy Điển đã tiến hành các thử nghiệm để đưa các giao dịch bất động sản lên blockchain.

#### Chăm sóc sức khoẻ

Blockchain có tiềm năng to lớn để giải quyết các vấn đề về khả năng tương tác của các hệ thống chăm sóc sức khỏe hiện có. Nó có thể được sử dụng để cho phép các đối tượng chăm sóc sức khỏe và các nhà nghiên cứu chia sẻ Hồ sơ Sức khỏe Điện tử (EHR) của họ một cách an toàn và được bảo vệ. Ngoài ra, nó cho phép cải thiện chăm sóc y tế và xác nhận của bác sĩ.

Quản lý dữ liệu chăm sóc sức khỏe bằng cách lưu trữ hay phân tích không phải là một hoạt động dễ dàng, đặc biệt là liên quan đến quyền riêng tư của dữ liệu. Để cung cấp một môi trường an toàn cho lĩnh vực chăm sóc sức khỏe với blockchain, Cổng dữ liệu chăm sóc sức khỏe (HDG) có thể được sử dụng để quản lý và kiểm soát việc lưu trữ và chia sẻ dữ liệu một cách dễ dàng. Ngoài ra, việc cải thiện quyền riêng tư có thể được đảm bảo bằng cách áp dụng blockchain riêng tư cho phép chỉ những người cụ thể lưu trữ hoặc sửa đổi thông tin y tế.

#### An ninh mạng

Bảo mật là một trong những vấn đề quan trọng đối với tất cả các công nghệ hiện tại và mới. Các công ty nổi tiếng phải đối mặt với nhiều vấn đề về bảo mật. Ví dụ, hơn 50 triệu hồ sơ Facebook đã bị Cambridge Analytica xâm phạm để nhắm mục tiêu họ với các quảng cáo chính trị được cá nhân hóa, điều này đã ảnh hưởng đến các cử tri Hoa Kỳ về quyết định cuối cùng của họ về cuộc bầu cử tổng thống. Ngoài ra, vào năm 2016, Yahoo, công cụ tìm kiếm nổi tiếng, đã phải đối mặt với một cuộc tấn công lớn và khoảng một tỷ tài khoản Yahoo đã bị xâm nhập. Khi các công ty bảo mật thực hiện nghiên cứu về các lỗ hổng bảo mật phổ biến, họ phát hiện ra rằng 65% các vụ mất dữ liệu xảy ra do mật khẩu yếu hoặc bị đánh cắp. Ngoài ra, họ còn phát hiện thấy các email lừa đảo ăn cắp dữ liệu nhạy cảm như tên người dùng, mật khẩu và hồ sơ tài chính.

Blockchain có một số khả năng có thể được sử dụng để giải quyết vấn đề an ninh mạng. Đầu tiên, blockchain là một hệ thống không tin cậy, nơi sự tin tưởng không tồn tại. Nó giả định rằng bất kỳ người trong cuộc hoặc người ngoài cuộc nào cũng có thể tấn công hệ thống, vì vậy nó hoàn toàn độc lập với đạo đức con người. Thứ hai, blockchain là bất biến, vì vậy bất kỳ ai cũng có thể lưu trữ dữ liệu và bảo mật nó bằng các tính năng mật mã khác nhau như hashing và chữ ký số. Ngay khi dữ liệu được hình thành dưới dạng một khối trong blockchain, nó không thể bị thay đổi hoặc xóa. Thứ ba, blockchain liên quan đến nhiều người dùng trong mạng, vì vậy việc thay đổi hoặc thêm một khối cần phải được xác minh bởi đa số người dùng, điều này khiến cuộc tấn công rất khó thực hiện.

#### Bỏ phiếu

Bầu cử là một công cụ quan trọng đối với bất kỳ chính phủ dân chủ nào. Đó là một quá trình bắt buộc đối với tất cả mọi người; tuy nhiên, hệ thống bỏ phiếu bằng giấy truyền thống phải đối mặt với một số vấn đề. Ví dụ, hệ thống không thể tự động hóa và mọi người phải đến các địa điểm nơi giữ các thùng phiếu khiến họ phải xếp hàng chờ đợi trong thời gian dài. Ngoài ra, việc kiểm phiếu mất nhiều thời gian và cuộc bầu cử có thể bị gian lận do các lá phiếu ảo. Ngoài ra, chi phí và số lượng giấy tờ bị lãng phí trong hoạt động là rất cao.

Với các tính năng minh bạch và bất biến của blockchain, quá trình bỏ phiếu có thể đơn giản hơn nhiều và tiết kiệm chi phí lãng phí khổng lồ trong hệ thống bỏ phiếu bằng phiếu giấy cổ điển. Người bỏ phiếu có thể tạo một khối, đó là phiếu bầu của họ, vì vậy khi cuộc bỏ phiếu được thực hiện, bất kỳ ai cũng có thể xác minh xem chữ ký đó có hợp lệ hay không và đảm bảo rằng không có phiếu bầu nào bị giả mạo.

### Những thách thức của Blockchain

Blockchain không đơn giản. Nó đặt ra một số thách thức với các công nghệ hiện có cần được giải quyết. Những thách thức này được tóm tắt và được mô tả như sau:

Diagram

Description automatically generated

Hình 13 Các thách thức của blockchain

* Scalability (khả năng mở rộng): mọi giao dịch được lưu trữ trong sổ cái phân tán, các giao dịch này đang tăng lên mỗi ngày. Để xác thực một giao dịch, mỗi người dùng phải lưu trữ nó trên sổ cái để kiểm tra nguồn gốc của giao dịch hiện có. Hơn nữa, việc tạo một khối phải đối mặt với một số hạn chế về thời gian và kích thước. Ví dụ, Bitcoin chỉ có thể tạo gần bảy giao dịch mỗi giây, điều này không thể thực hiện được nhu cầu xử lý của hàng tỷ giao dịch trong các ứng dụng thời gian thực. Ngoài ra, quy mô của giao dịch đóng một vai trò quan trọng trong lệnh thực hiện vì các minor thích tạo các khối có kích thước giao dịch lớn và phí giao dịch cao. Điều này dẫn đến độ trễ nhiều hơn cho các giao dịch nhỏ. Một số nghiên cứu đã đề xuất các giải pháp cho vấn đề khả năng mở rộng. Ví dụ: Bruce đã đề xuất một phương pháp tối ưu hóa lưu trữ cho blockchain để xóa các bản ghi giao dịch cũ khỏi sổ cái. Tuy nhiên, cần có thêm nhiều nghiên cứu để giải quyết thách thức này.
* Privacy (quyền riêng tư): một số quyền riêng tư nhất định có thể được bảo vệ thông qua công nghệ blockchain. Người dùng ẩn danh để tạo và xác minh các giao dịch bằng khóa riêng tư và khóa công khai của họ. Tuy nhiên, vì tất cả người dùng tham gia vào mạng blockchain đều có thể xem các giá trịcủa tất cả các giao dịch, blockchain không thể đảm bảo quyền riêng tư của các giao dịch. Ngoài ra, J. Barcelo chỉ ra rằng giao dịch của người dùng có thể được liên kết để tiết lộ thông tin cá nhân của người dùng. Do đó, vấn đề quyền riêng tư của công nghệ blockchain cần được nghiên cứu thêm để tăng tỷ lệ chấp nhận blockchain trong các ứng dụng khác nhau.
* Wasted Resources (lãng phí tài nguyên): cho đến thời điểm hiện tại, sử dụng tài nguyên hiệu quả là một trong những thách thức quan trọng trong kỹ thuật máy tính cần được giải quyết. Về công nghệ blockchain, quá trình khai thác cần một lượng lớn sức mạnh tính toán để tính toán và xác minh các giao dịch một cách an toàn. Tuy nhiên, điều cần thiết là giảm tài nguyên lãng phí trong quá trình khai thác. Một số nhà nghiên cứu đã đề xuất giải pháp để giải quyết vấn đề này. Ví dụ: Janish đã đề xuất một kế hoạch để tăng tốc quá trình khai thác bằng cách sử dụng đồng thời CPU và GPUcho các máy riêng lẻ trong các nhóm khai thác.
* Data Malleability (tính dễ uốn của dữ liệu): duy trì tính toàn vẹn của dữ liệu là một trong những khía cạnh quan trọng trong blockchain. Dữ liệu không được thay đổi hoặc giả mạo khi truyền hoặc xác minh. Cuộc tấn công về tính dễ uốn đối với tính toàn vẹn của dữ liệu chỉ ra rằng chữ ký của các giao dịch được sử dụng để xác minh việc sở hữu Bitcoin không mang lại bất kỳ sự đảm bảo tính toàn vẹn nào cho bản thân chữ ký. Do đó, kẻ xâm nhập có thể nắm bắt, thay đổi và phát lại một giao dịch khiến người tạo giao dịch nghĩ rằng giao dịch đó chưa được xác minh.
* Usability (khả năng sử dụng): vấn đề khả năng sử dụng đề cập đến thực tế là API khó sử dụng. Mục tiêu chính của tất cả các công nghệ mới phải liên quan đến việc cung cấp các giao diện có thể sử dụng và dễ sử dụng cho cả người dùng và nhà phát triển. Khả năng sử dụng của blockchain từ quan điểm của miền tiền điện tử sẽ cho phép người dùng phân tích blockchain. Trong môi trường blockchain, các khối được tạo liên tục và được xác nhận bởi những người dùng tham gia, điều này tạo ra một bầu không khí sôi động của các luồng giao dịch. Do đó, điều quan trọng là phải cải thiện khả năng sử dụng của blockchain bằng cách cung cấp các công cụ cần thiết để cho phép người dùng phân tích toàn bộ mạng blockchain.
* Bootstrapping (khởi tạo): chuyển các tài liệu, hợp đồng hoặc khuôn khổ kinh doanh hiện tại sang công nghệ dựa trên blockchain mới mang lại nhiều trách nhiệm di chuyển cần được thực hiện. Ví dụ: trong trường hợp có quyền sở hữu đất, các biểu mẫu hiện có yêu cầu phải được di chuyển và định dạng để tương đương với biểu mẫu blockchain, điều này sẽ mất thời gian và chi phí.
* Bandwitch (băng thông): kích thước khối trong blockchain xác định số lượng giao dịch cần thiết cho mỗi khối. Để giữ bình đẳng và cung cấp cho tất cả người dùngcủa mạng lưới blockchain có cơ hội ngang nhau để trở thành người dẫn đầu trong vòng tiếp theo, tất cả người dùng phải được thông báo về các khối mới cùng một lúc. Kích thước khối thường bị giới hạn ở băng thông đường lên của người dùng. Ví dụ: kích thước khối hiện tại của Bitcoin là 1 MB, tương đương với khoảng 1000 giao dịch. Do đó, kích thước khối và băng thông của người dùng cần được xem xét khi tạo khối mới.
* Authentication (xác thực): trong blockchain hiện tại, khi danh tính người dùng được tạo, không có gì đảm bảo rằng người dùng yêu cầu danh tính là chủ sở hữu chính xác của danh tính đó và không phải là người độc hại. Có một số vấn đề trong quá trình xác thực Bitcoin. Ví dụ, có một sự cố nổi tiếng ở Mt. Gox, nơi khóa cá nhân của người dùng bị xâm nhập. Vì vậy, duy trì một kế hoạch xác thực mạnh mẽ là một trong những ưu tiên cơ bản đối với công nghệ blockchain cần nhiều nghiên cứu và nỗ lực hơn để phát triển.

## Internet of Things (IOT)

### Lịch sử IOT

Khái niệm về IoT không phải là mới, nó đã trải qua nhiều giai đoạn cho đến hiện tại. Khái niệm IoT bắt đầu vào năm 1982 khi bốn sinh viên từ Đại học Carnegie Mellon phát minh ra ARPANETkết nối máy coke để cho biết đồ uống chứa trong máy có lạnh hay không. Ý tưởng chính của họ là đếm xem có bao nhiêu chai coke còn lại trong mỗi hàng và trong bao lâu. Nếu chai đã nạp được để lâu trong máy, nó sẽ được dán nhãn là “lạnh”. Tất cả dữ liệu này sau đó được cung cấp từ xa cho khách hàng thông qua giao diện ngón tay. Thử nghiệm nàyđã truyền cảm hứng cho rất nhiều nhà phát minh trên khắp thế giới tạo ra thiết bị kết nối của riêng họ.

Vào đầu những năm 1990, các nhà khoa học của IBM đã trình bày và cấp bằng sáng chế về Nhận dạng tần số vô tuyến tần sốcao (UHF) (RFID) bao phủ khoảng cách rộng hơn và cung cấp truyền dữ liệu nhanh hơn. Mặc dù IBM đã thực hiện một số thí nghiệm thí điểm, nhưng nó chưa bao giờ thương mại hóa công nghệ mới này. Vào giữa những năm 1990, IBM đã gặp phải những vấn đề khó khăn về tài chính khiến họ phải bán bằng sáng chế của mình cho Intermec, một nhà cung cấp hệ thống mã vạch. Một số ứng dụng được xây dựng bằng hệ thống Intermec RFID, nhưng do chi phí công nghệ này cao vào thời điểm này và khả năng marketing thấp, công nghệ này đã không lan rộng như mong đợi.

Năm 1999, Trung tâm Nhận dạng tại Viện Công nghệ Massachusetts (MIT) đã tài trợ thông qua các tổ chức khác nhau để liên quan đến UHF RFID trong việc kết nối các đối tượng khác nhau với nhau. Điều này xảy ra khi hai giáo sư David Brock và Sanjay Sarma đề xuất sử dụng thẻ RFID để theo dõi sản phẩm thông qua chuỗi cung ứng. Đề xuất của họ về cơ bản là chỉ sử dụng số sê-ri của thẻ để theo dõi sản phẩm nhằm tiết kiệm chi phí, vì việc sản xuất một con chip phức tạp so với bộ nhớ lưu trữ lớn sẽ đắt hơn. Dữ liệu được liên kết với thẻ RFID được lưu giữ trong cơ sở dữ liệu có thể được truy cập qua Internet.

Một số nghiên cứu và ấn phẩm đã xác nhận rằng thuật ngữ IoT được Ashton, giám đốc điều hành của Trung tâm ID MIT trình bày lần đầu tiên vào năm 1999. Ashton đã nói, “Internet of Things có tiềm năng thay đổi thế giới, giống như Internet đã làm. Có khi còn hơn thế nữa”.

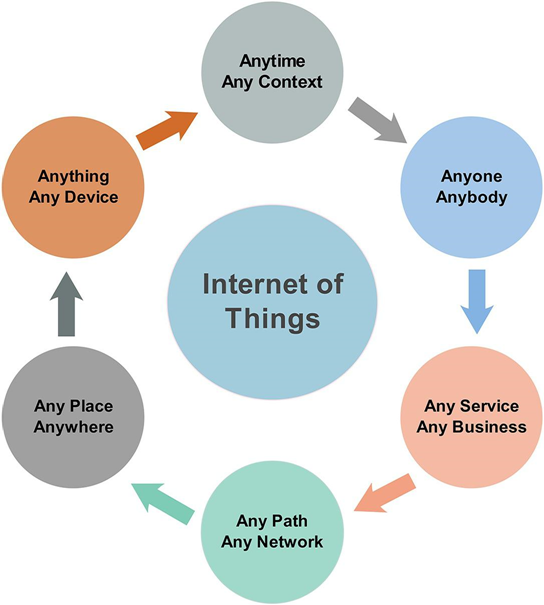
### Các định nghĩa về IOT

Khái niệm IoT mô tả khả năng kết nối mạng của nhiều loại đối tượng khác nhau trong môi trường không chỉ riêng máy tính. Những đối tượng này có thể hoạt động một cách thông minh và trao đổi dữ liệu với các thiết bị khác màkhông cần quá nhiều sự can thiệp của con người. Mặc dù sự phổ biến của hệ thống IoT và sự chấp nhận cao của công nghệ mới này trên toàn cầu, nhưng một định nghĩa chính xác vẫn chưa tồn tại. Có nhiều định nghĩa khác nhau tập trung vào một cái nhìn cụ thể về IoT. Chúng tôi sẽ cố gắng cung cấp các định nghĩa chung về IoT từ các khía cạnh khác nhau.

Liên minh Viễn thông Quốc tế (ITU) vào năm 2012 đã đưa ra một định nghĩa chung cho IoT đã được một sốCác nhà nghiên cứu. Nó nêu rõ “một cơ sở hạ tầng toàn cầu cho xã hội thông tin, cho phép các dịch vụ tiên tiến bằng cách kết nối với nhau (vật lý và ảo) dựa trên các công nghệ thông tin và truyền thông tương tác, hiện có và đang phát triển”. Trong khi Ban Kiến trúc Internet (IAB) mô tả IoT là“Internet of Things biểu thị một xu hướng trong đó một số lượng lớn các thiết bị nhúng sử dụng các dịch vụ truyền thông do các giao thức Internet cung cấp. Nhiều thiết bị trong số này, thường được gọi là 'vật thể thông minh', không được vận hành trực tiếp bởi con người, nhưng tồn tại như các thành phần trong các tòa nhà hoặc phương tiện, hoặc được phát tán trong môi trường " .

Có những quan điểm khác từ các nhà nghiên cứu khác nhau. Ví dụ, Atzori et alđã đề xuất ý tưởng cơ bản của IoT là sự tồn tại phổ biến của sự đa dạng của những thứ như cảm biến, thẻ RFID, thiết bị truyền động và điện thoại di động có thể tương tác với nhau để đạt được mục tiêu chung. Ngoài ra, Ma đã đề xuất một định nghĩa cho IoT trong đó nêunhư “IoT có thể cho phép kết nối và tích hợp giữa thế giới vật lý và không gian mạng; đại diện cho xu hướng kết nối mạng trong tương lai đồng thời dẫn đầu làn sóng thứ ba của cuộc cách mạng công nghiệp CNTT”.

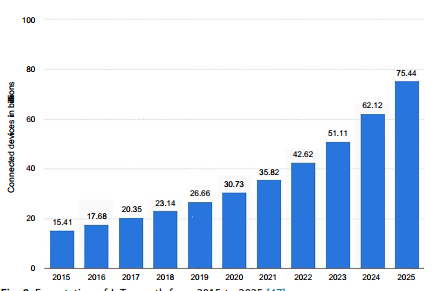
Tương tự, Gubbi et al. đã định nghĩa hệ thống IoT từ quan điểm của một môi trường thông minh. Nó mô tả IoT là “sự kết nối giữa các thiết bị cảm biến và kích hoạt cung cấp khả năng chia sẻ thông tin trên các nền tảng thông qua một khuôn khổ thống nhất, phát triển một bức tranh hoạt động chung chocho phép các ứng dụng sáng tạo.” Ngoài ra, Guillemin và Friess đã định nghĩa IoT theo những thuật ngữ đơn giản, như được thể hiện trong Hình 7. Nó nêu rõ: “Internet of Things cho phép mọi người và mọi thứ được kết nối mọi lúc, mọi nơi, với bất kỳ thứ gì và bất kỳ ai, lý tưởng là sử dụng bất kỳ đường dẫn / mạng nào và bất kỳ dịch vụ nào.”



Hình 14 Các lợi ích của IoT

### Mở rộng IOT

IoT đề cập đến một mạng lưới thiết bị và cảm biến khổng lồ có thể thu thập và chia sẻ dữ liệu với nhau. Các thiết bị này liên quan đến cả các đối tượng vật lý và ảo được kết nối với nhau qua Internet. Có những phát triển công nghệ khổng lồ đã mở rộng IoT để bao gồm các công nghệ khác như Điện toán đám mây và Mạng cảm biến không dây (WSN). IoT có khả năng chủ yếu sửa đổi các mô hình kinh doanh và chuỗi giá trị trong các tổ chức khác nhau. Nó không chỉ là một chiếc lò nướng thông minh kết nối Internet. Trong một số giai đoạn, tất cả các sản phẩm sẽ có khả năng kết nối Internet một cách kinh tế.



Hình 15 Kỳ vọng tăng trưởng IoT từ 2015 đến 2025

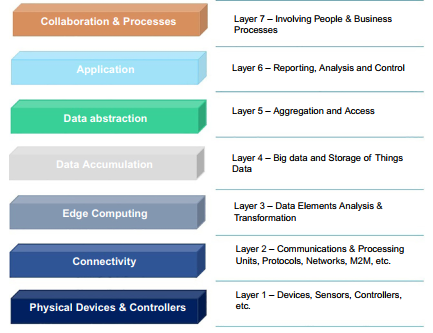
Số lượng thiết bị được kết nối vượt quá dân số trên toàn thế giới từ năm 2008 và với khả năng vô hạn của hệ thống IoT, các ứng dụng và dịch vụ mới có thể được tạo ra mỗi ngày bằng cách sử dụng công nghệ hấp dẫn này. Số lượng thiết bị IoT đang tăng lên mỗi ngày. Theo Statista, số lượng thiết bị IoT dự kiến sẽ đạt khoảng 31 tỷ trên toàn thế giới vào cuối năm 2020. Con số này sẽ tăng đáng kể lên khoảng 75 tỷ thiết bị vào cuối năm 2025. Ngoài ra, IoT có doanh thu dự kiến đạt khoảng 1,8 nghìn tỷ đô la vào năm 2026.

Một trong những vấn đề lớn đang là rào cản đối với việc áp dụng các sản phẩm IoT khác nhau là các thách thức về bảo mật và quyền riêng tư. Sự phát triển của các thiết bị IoT tạo ra các dịch vụ và ứng dụng mới, nhưng đồng thời, nó tạo ra một số lỗ hổng bảo mật ngày càng rõ ràng. Các nhà sản xuất thiết bị IoT không xem xét vấn đề bảo mật trong các ưu tiên của họ. Với nhận thức của cộng đồng về bảo mật và quyền riêng tư thấp, các thiết bị IoT có thể dẫn đến các vấn đề nghiêm trọng có thể dẫn đến mất mạng của chúng ta theo đúng nghĩa đen. Chính phủ nên khuyến khích các nhà sản xuất thiết bị IoT áp dụng các biện pháp bảo mật mới trong các sản phẩm của họ. Ngoài ra, các nhà sản xuất nên sử dụng khái niệm bảo mật theo thiết kế để triển khai các thuật toán bảo mật tích hợp trong sản phẩm của họ nhằm đảm bảo an ninh và an toàn tối thiểu cho nhiều người tiêu dùng khác nhau.

### Kiến trúc của IOT

Có các kiến trúc khác nhau cho hệ thống IoT thể hiện các quan điểm khác nhau về IoT và các chức năng của nó. Tuy nhiên, kiến trúc chung nhất cho IoT là kiến trúc do Ủy ban kiến trúc của Diễn đàn Thế giới IoT (IWF) đưa ra vào tháng 10 năm 2014. Mô hình tham chiếu này cung cấp một khuôn khổ chung cho phép triển khai IoT dễ dàng và nhanh chóng trong ngành.

Tương tự như mô hình tham chiếu kết nối hệ thống mở (OSI) của mạng, mô hình tham chiếu IoT được chia thành bảy lớp để thúc đẩy sự liên kết và mở rộng các mô hình triển khai IoT, như trong hình bên dưới. Nó xác định nơi các loại xử lý khác nhau được vận hành thông qua các lớp khác nhau của mô hình tham chiếu IoT và cho phép các nhà sản xuất khác nhau sản xuất các sản phẩm IoT tương thích hoạt động với nhau một cách trơn tru và hiệu quả. Ngoài ra, mô hình kiến trúc này chuyển đổi IoT từ một mô hình khái niệm thành một hệ thống thực tế và có thể tiếp cận.



Hình 16 Mô hình tham chiếu IoT theo IWF.

Lớp 1 là lớp vật lý. Đây là lớp phần cứng thu thập dữ liệu từ thế giới vật lý và chuyển nó lên lớp trên. Lớp này liên quan đến các đối tượng vật lý và cảm biến. Về cơ bản, mục đích của lớp này là xác định các đối tượng khác nhau và thu thập thông tin về môi trường xung quanh như nhiệt độ, độ ẩm, áp suất, chất lượng nước, phát hiện chuyển động, lượng bụi trong không khí,…

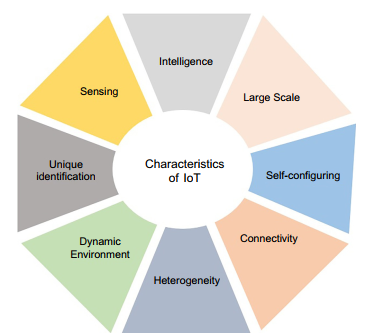
Lớp 2 là kết nối. Lớp này được sử dụng để kết nối những thứ IoT khác nhau với nhau bằng cách sử dụng các thiết bị kết nối như công tắc,cổng vào và bộ định tuyến. Nó cũng chuyển dữ liệu thu thập được một cách an toàn từ các cảm biến lên lớp trên để xử lý. Lớp 3 là tính toán biên. Lớp này lấy dữ liệu đến từ lớp kết nối và chuyển nó thành thông tin thích hợp để lưu trữ và xử lý ở cấp cao hơn. Tại lớp này, các thành phần xử lý làm việc với một lượng lớn dữ liệu có thể thực hiện một số chuyển đổi dữ liệu để giảm kích thước dữ liệu.

Tích lũy dữ liệu xảy ra ở lớp 4. Chức năng chính của lớp này là lưu trữ dữ liệu đến từ lớp 3. Nó hấp thụ một lượng lớn dữ liệu và đặt chúng vào các kho lưu trữ để các lớp trên có thể truy cập được. Vì vậy, nó chỉ đơn giản là thay đổi dữ liệu dựa trên sự kiện thành thông tin xử lý dựa trên truy vấn cho các lớp trên. Lớp 5 là sự trừu tượng hóa dữ liệu. Lớp này kết hợp dữ liệu đến từ các nguồn khác nhau và chuyển đổi dữ liệu được lưu trữ sang định dạng thích hợp cho các ứng dụng theo cách có thể quản lý và hiệu quả.

Lớp 6 là lớp ứng dụng. Lớp này liên quan đến việc giải thích thông tin của các ứng dụng IoT khác nhau. Nó bao gồm các ứng dụng IoT khác nhau như chăm sóc sức khỏe, thành phố thông minh, lưới điện thông minh, nhà thông minh, ô tô kết nối, nông nghiệp thông minh, v.v. Lớp 7 là sự cộng tác và các quy trình. Lớp này xác định các cá nhân có thể giao tiếp và cộng tác để sử dụng dữ liệu IoT một cách hiệu quả. Nó cung cấp các chức năng khác như tạo đồ thị và mô hình kinh doanh và các chức năng khác dựa trên dữ liệu được truy xuất từ lớp ứng dụng. Nó cũng hỗ trợ các nhà quản lý đưa ra các lựa chọn chính xác về doanh nghiệp của họ dựa trên phân tích dữ liệu của họ.

### Đặc điểm của IOT

Khái niệm cơ bản của IoT là cung cấp một hệ thống tự trị có khả năng chia sẻ thông tin hữu ích giữa các đối tượng thế giới thực có thể nhận dạng duy nhất bằng cách sử dụng thẻ RFID và WSN. Hệ thống IoT cho thấy những đặc điểm chung. Phần này cung cấp các đặc điểm chung mô tả tốt hơn hệ thống IoT được tóm tắt trong hình bên dưới.



Hình 17 Đặc điểm chung của hệ thống IoT

* Large Scale (quy mô lớn): hệ thống IoT mở rộng đạt khoảng 30 tỷ thiết bị vào cuối năm 2018. Cisco dự kiến rằng con số này sẽ tăng lên đạt khoảng 50 tỷ thiết bị vào cuối năm 2020. Số lượng lớn các thiết bị kết nối này tạo ra một mạng lưới quy mô lớn để chia sẻ thông tin đã thu thập của họ và hợp tác cùng nhau để nâng cao các dịch vụ hiện có và tạo ra các ứng dụng mới có khả năng xử lý các vấn đề trong cuộc sống hàng ngày của người dùng IoT.
* Intelligent (trí thông minh): khái niệm tích hợp cảm biến, máy tính và mạng truyền thông để thu thập và quan sát thông tin đã được tìm thấy trong nhiều thập kỷ. Sự phát triển hiện đại nhằm mục đích làm cho các đối tượng IoT hoạt động một cách thông minh và đưa ra các quyết định tự chủ. Hầu hết các thiết bị IoT đều hoạt động theo các hành động được xác định trước của chúng, nhưng với sự hội tụ của các thuật toán phần cứng và phần mềm tinh vi, các đối tượng IoT có thể phản hồi một cách thông minh và chính xác theo các tình huống và ngữ cảnh khác nhau.
* Seising (cảm biến): Cảm biến là một trong những yếu tố chính của hệ thống IoT, được sử dụng để cảm nhận, nhận thức và thu thập thông tin về môi trường xung quanh. Thông tin thu thập được có thể là kết quả của quá trình ghi chép của họ hoặc sau sự tương tác của họ với môi trường. Các kỹ thuật cảm biến mang lại nhiều khả năng khác nhau để xem xét tính nhạy cảm của con người đối với môi trường xung quanh. Ngoài ra, tính năng cảm biến là khía cạnh quan trọng đối với nhận thức ngữ cảnh, cho phép các thiết bị tự điều chỉnh theo các tình huống và ngữ cảnh khác nhau tùy thuộc vào hoàn cảnh hoạt động của chúng.
* Unique identification (nhận dạng duy nhất): mỗi thiết bị IoT bao gồm một thẻ RFID cung cấp một danh tính duy nhất cho mỗi thiết bị. Các danh tính này được cung cấp cho các thiết bị IoT được các nhà sản xuất sử dụng để nâng cấp phần mềm của thiết bị. Hệ thống IoT với hàng tỷ thiết bị được kết nối cần có kiến trúc đặt tên cung cấp danh tính duy nhất cho các thiết bị IoT để thiết lập các đường dẫn giao tiếp giữa các loại thiết bị khác nhau.
* Dynamic Enviroment (môi trường động): về bản chất, IoT là một hệ thống năng động làm cho nhiều thứ khác nhau có thể thích ứng với những thay đổi của môi trường và hành động một cách thông minh dựa trên bối cảnh. Ngoài ra, các thiết bị IoT thu thập dữ liệu với việc xem xét các thay đổi động trong môi trường. Trạng thái của các thiết bị này thay đổi linh hoạt dựa trên các điều kiện xung quanh như được kết nối hoặc ngắt kết nối, đang ngủ hoặc đang chạy.
* Heterogeneily (tính không đồng nhất): có một số nhà sản xuất muốn sản xuất nhiều thiết bị để tận dụng khả năng kết nối qua Internet. Tuy nhiên, họ phải đối mặt với một vấn đề khi nói đến việc quản lý tính không đồng nhất của các thiết bị của họ. Hệ thống IoT liên quan đến một số thiết bị với các nền tảng phần cứng, mạng, giao thức truyền thông và hệ điều hành khác nhau. Mặc dù sự không đồng nhất của các thiết bị này gây ra nhiều vấn đề, chúng vẫn có thể liên lạc với nhau bằng các mạng truyền thông khác nhau.
* Conectivity (khả năng kết nối): Hệ thống IoT liên quan đến nhiều thiết bị cần được kết nối để chia sẻ thông tin của chúng. IoT có khả năng liên kết và kết nối các đối tượng khác nhau trong môi trường để mang lại cơ hội thị trường mới cho việc tạo ra các ứng dụng và dịch vụ mới nhằm trợ giúp con người trong các lĩnh vực khác nhau.
* Self-configuring (tự định cấu hình): Tính năng quy mô lớn của các thiết bị IoT tạo ra một vấn đề nghiêm trọng đối với các nhà cung cấp dịch vụ và nhà sản xuất khác nhau trong việc bảo trì và cập nhật thiết bị của họ. Với các tính năng tự định cấu hình cho IoT, các thiết bị có thể làm việc với nhau để thực hiện một hoạt động cụ thể. Ngoài ra, các thiết bị này có thể tự định cấu hình và tìm kiếm bản cập nhật phần mềm mới nhất cùng với nhà sản xuất thiết bị với những nỗ lực không đáng kể.

### Điện toán đám mây (cloud computing) và lưu trữ

#### Điện toán đám mây

Điện toán đám mây là việc phân phối, sử dụng tài nguyên theo nhu cầu qua Internet thay vì sử dụng các trung tâm dữ liệu và máy chủ vật lý.

Lợi ích của việc sử dụng điện toán đám mây:

* Nhanh chóng: cho phép nhanh chóng thu thập các tài nguyên khi cần từ các dịch vụ cơ sở hạ tầng, triển khai các dịch vụ công nghệ một cách nhanh chóng.
* Linh hoạt: không cần phải cung cấp tài nguyên quá mức để xử lý các hoạt động ở mức cao nhất, thay vào đó chỉ cần cung cấp những tài nguyên thực sự cần thiết.
* Tiết kiệm chi phí: thay thế các khoản chi phí cố định từ các trung tâm dữ liệu và máy chủ vật lý bằng các khoản chi phí biến đổi, chỉ cần phải tiêu tốn chi phí cho tài nguyên phải sử dụng.
* Triển khai trên toàn cầu: đám mây có thể mở rộng khu vực địa lý và triển khai trên toàn cầu trong vài phút, đặt các ứng dụng gần hơn với người dùng giúp giảm độ trễ và cải thiện trải nghiệm.

Các loại điện toán đám mây:

* Phần mềm dưới dạng dịch vụ (Software as a Service - SaaS): cung cấp sản phẩm hoản chỉnh được nhà cung cấp vận hành và quản lý: Email, CRM, Collaborative, ERP,…
* Nền tảng dưới dạng dịch vụ (Platform as a Service - PaaS): giúp người dùng tap trung vào công tác triển khai cũng như quản lý các ứng dụng mà không cần quản lý cơ sở hạ tầng ngầm (phần cứng và hệ điều hành): App Dev, Web, Decision Support, Streaming,…
* Cơ sở hạ tầng dưới dạng dịch vụ (Infrastructure as a Service - IaaS): chứa các khối xây dựng cơ bản cho đám mây, cung cấp quyền truy cập vào các tính năng mạng, máy tính và không gian lưu trữ dữ liệu. IaaS đem lại sự linh hoạt và khả năng kiểm soát quản lý ở mức cao nhất: Caching, Networking, Security, System-Mgmt,…

#### Ảo hóa

Ảo hoá là tạo một nền tảng mô phỏng phần cứng và cho phép nhiều phiên bản hệ điều hành sử dụng nền tảng đó. Hệ điều hành có đầy đủ quyền truy cập vào phần cứng bên dưới.

Lợi ích khi sử dụng ảo hoá:

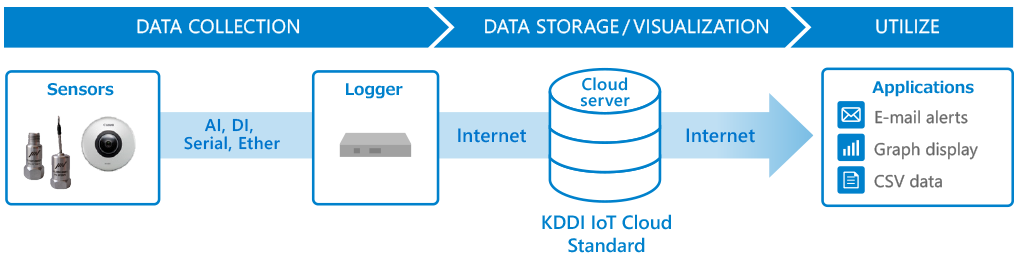
* Tiết kiệm phần cứng và năng lượng
* Khả năng phục hồi cao
* Dễ dàng kiểm tra và triển khai
* Tính ứng dụng cao

Những hạn chế:

* Yêu cầu giao dịch với nhiều nhà cung cấp
* Rủi ro bảo mật dữ liệu
* Khó nâng cấp và cập nhật các phần mềm

#### Mối quan hệ giữa IoT, Big Data và điện toán đám mây

Điện toán đám mây giúp lưu trữ và phân tích lượng dữ liệu khổng lồ mỗi giây để các công ty, tổ chức có thể tận dụng tối đa cảm biến, máy móc, thiết bị và cơ sở hạ tầng của IoT. Vì IoT tạo ra một lượng lớn dữ liệu nên nhiều nhà cung cấp đã cung cấp các dịch vụ truyền dữ liệu qua Internet giúp điều hướng dễ dàng hơn.



Hình 18 Mối quan hệ giữa IoT và big data, điện toán đám mây

Điện toán đám mây lưu giữ và điều khiển hàng nghìn cảm biến trong IoT và áp dụng các quy tắc, thuật toán phân tích cần thiết để cho ra kết quả mong đợi của dữ liệu. Nói cách khác IoT là nguồn dữ liệu, Big Data là công nghệ và nền tảng phân tích dữ liệu, đám mây là nơi lưu trữ các dữ liệu đã được phân tích và xử lý.

### Ứng dụng IOT

Hệ thống IoT có thể kết nối gần như tất cả các đối tượng vật lý và ảo trong môi trường của chúng ta để mang lại các dịch vụ và ứng dụng mới. Các ứng dụng này có thể được áp dụng trong các lĩnh vực khác nhau để nâng cao chất lượng cuộc sống của chúng ta. Phần này cung cấp một cuộc thảo luận về các ứng dụng IoT phổ biến.

#### Tự động hóa nhà

Nhà thông minh là một trong những ứng dụng phổ biến nhất của hệ thống IoT. Nhờ các công nghệ cảm biến và truyền động cùng với WSN, mọi người có thể kết nối nhiều thiết bị thông minh trong nhà để giải quyết sở thích của họ. Trong một ngôi nhà thông minh, có một số cảm biến để kích hoạt các dịch vụ thông minh và tự động hoạt động với nỗ lực tối thiểu của con người. Ngoài ra, các cảm biến được sử dụng để duy trì an ninh và an toàn.

Mặc dù những lợi ích được hỗ trợ bởi nhà thông minh là vô số, nó gây ra một số vấn đề liên quan đến bảo mật và quyền riêng tư vì tất cả các hành động và sự kiện xảy ra trong nhà đều được ghi lại. Nếu kẻ tấn công đã xâm nhập thành công hệ thống, nó có thể làm cho hệ thống hoạt động có hại. Vì vậy, ngôi nhà thông minh cần được bảo vệ theo cách cho phép các thiết bị thông minh thông báo cho chủ sở hữu về bất kỳ hành động bất thường nào. Ngoài ra, độ tin cậy cũng là một thách thức khác vì không tồn tại quản trị viên nào để quan sát hành vi của hệ thống.

#### Chăm sóc sức khỏe

IoT đã chứng minh rằng nó có thể cung cấp một số lợi ích cho lĩnh vực chăm sóc sức khỏe bằng cách tạo ra các ứng dụng và dịch vụ mới giúp bệnh nhân và giữ cho lĩnh vực này luôn đổi mới. Có nhiều thiết bị đeo được phát triển để theo dõi và theo dõi tình trạng sức khỏe của bệnh nhân. Những thiết bị này cho phép bệnh nhân lớn tuổi sống độc lập mà không sợ hãi. Ngoài ra, các thiết bị này có thể được sử dụng để liên tục quan sát và lưu trữ tình trạng sức khỏe của bệnh nhân và gửi các thông báo cảnh báo trong các tình huống bất thường. Nếu tình huống là Minor, bản thân thiết bị có thể đưa ra phương pháp điều trị cho bệnh nhân. Trong khi nếu đó là một tình huống nghiêm trọng, thiết bị có thể gửi tin nhắn khẩn cấp đến bệnh viện hoặc xe cấp cứu để được điều động ngay lập tức.

#### Nông nghiệp thông minh

Với sự tồn tại của nhiều cảm biến trong môi trường IoT, nông dân có thể sử dụng dữ liệu thu thập được để tạo ra lợi tức đầu tư tốt hơn. Các thông số của đất như độ ẩm, mức muối và nhiệt độ có thể được thu thập và đo lường bằng cách sử dụng các cảm biến có sẵn để tăng sản lượng nông nghiệp. Hơn nữa, với sự tồn tại của một số công nghệ không dây như hệ thống thông tin địa lý và viễn thám, có nhiều cơ hội thu thập thông tin liên quan về đất một cách nhanh chóng và hiệu quả, có thể giúp thay thế công sức của con người bằng máy móc tự động để tăng sản lượng nông nghiệp.

Có một sự tăng trưởng đáng kể trong việc áp dụng các thiết bị IoT trong lĩnh vực nông nghiệp. Dự đoán, số lượng thiết bị IoT trong nông nghiệp sẽ đạt khoảng 75 triệu thiết bị vào cuối năm 2020. Có một số lợi thế cho việc tích hợp các giải pháp IoT trong nông nghiệp. Ví dụ, các cảm biến có thể được sử dụng để theo dõi chất lượng đất, tiến độ phát triển của cây trồng và điều kiện thời tiết bên cạnh hiệu suất của nhân viên và hiệu quả của thiết bị. Ngoài ra, hệ thống IoT có thể giúp tự động hóa các hoạt động khác nhau trong vòng đời cây trồng và thực hiện quản lý tốt hơn phương pháp sản xuất và đảm bảo các tiêu chuẩn nâng cao về chất lượng cây trồng.

#### Chuỗi cung ứng và hậu cần

Hệ thống IoT cố gắng tạo điều kiện thuận lợi cho các hoạt động của thế giới thực trong hệ thống thông tin và kinh doanh. Sử dụng các công nghệ cảm biến như RFID và Giao tiếp trường gần (NFC), sản phẩm có thể được theo dõi từ nhà sản xuất đến địa điểm phân phối. Thẻ RFID gắn vào sản phẩm được sử dụng để nhận dạng duy nhất từng sản phẩm và tự động thu thập thông tin liên quan để truyền tải thông tin đó theo thời gian thực cùng với thông tin vị trí. Các thẻ này được sử dụng để truyền thông điệp hiển thị chính xác sản phẩm, kích thước và biến thể kiểu dáng cũng như nhiệt độ và độ ẩm của sản phẩm. Ngoài ra, tính năng thu thập dữ liệu tự động cung cấp khả năng hiển thị hàng tồn kho theo thời gian thực và tránh việc đếm thủ công cũng như các lỗi do con người gây ra. Nói cách đơn giản, IoT được thiết lập để cách mạng hóa chuỗi cung ứng với cả hiệu quả hoạt động và cơ hội doanh thu.

#### Thành phố thông minh

Khái niệm thành phố thông minh đề cập đến việc sử dụng các thiết bị IoT như cảm biến, đồng hồ đo, đèn chiếu sáng, v.v., để theo dõi và thu thập thông tin về thành phố xung quanh. Thông tin này được sử dụng để cải thiện các dịch vụ công cộng và cơ sở hạ tầng thành phố. Các giải pháp IoT tham gia vào nhiều lĩnh vực của thành phố thông minh như chiếu sáng đường phố thông minh, quản lý thùng rác, bãi đậu xe thông minh và quản lý giao thông. Đối với giao thông thông minh, thông tin cảm biến thu thập được về giao thông có thể được gửi đến điện thoại của công dân để giám sát giao thông trong thời gian thực và cho phép người lái xe chọn con đường tốt nhất để tiết kiệm công sức và thời gian lái xe. Ngoài ra, người lái xe có thể được cảnh báo trong trường hợp xảy ra tai nạn để chuyển hướng tránh ùn tắc. Để quản lý thùng rác, các cảm biến IoT được triển khai trên khắp các thùng rác để gửi tin nhắn đến các cơ quan chức năng cụ thể để báo cáo thùng rác cần được dọn sạch. Ngoài ra, các cảm biến này có thể được sử dụng để tối ưu hóa các xe chở rác nhằm giảm việc sử dụng rác thải.

#### Lưới thông minh

Sử dụng năng lượng hiệu quả và cuối cùng tiết kiệm nhiều tiền hơn có thể đạt được thông qua việc sử dụng các cảm biến IoT để thu thập thông tin liên quan về mức tiêu thụ năng lượng trong gia đình, chẳng hạn như đề xuất các cách tốt hơn để tiết kiệm năng lượng. Ngoài ra, thông tin cảm biến IoT có thể được sử dụng để cung cấp cho người tiêu dùng tất cả thông tin liên quan về các nhà cung cấp năng lượng khác nhau theo cách tự động để lựa chọn tốt nhất cho người tiêu dùng. Khái niệm về lưới điện thông minh bổ sung sự thông minh trong chu trình dòng điện từ nhà cung cấp đến người tiêu dùng. Loại hình thông minh này có thể được sử dụng để giúp người tiêu dùng nhận thức được mức tiêu thụ điện năng và giá cả năng động. Ngoài ra, một trong những ứng dụng chính của lưới điện thông minh là đồng hồ thông minh thu thập, ghi lại và phân tích điện năng tiêu thụ tại các thời điểm khác nhau trong ngày. Người tiêu dùng có thể sử dụng thông tin này để điều chỉnh mức tiêu thụ điện và thay đổi lối sống nhằm giảm chi phí.

#### Xe được kết nối

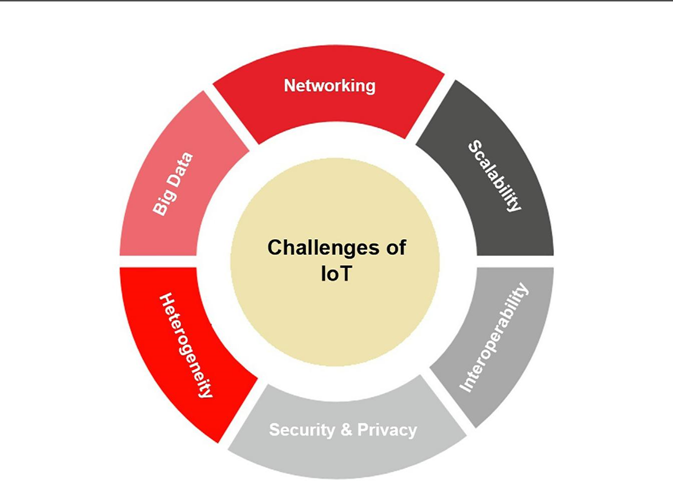
Ô tô thông minh hay còn gọi là ô tô kết nối bắt đầu được triển khai vào cộng đồng của chúng tôi. Loại ô tô này có thể truy cập Internet và chia sẻ dữ liệu của chúng với các thiết bị khác. Số lượng ô tô được trang bị tiện ích này đang tăng lên mỗi ngày, điều này sẽ cho phép sự xuất hiện của một số ứng dụng cho ô tô được kết nối trong tương lai gần. Chiếc xe được kết nối cung cấp một số lợi thế so với chiếc xe bình thường. Nó có thể làm giảm tai nạn ô tô và giảm lỗi của người lái xe ô tô bằng cách cho phép người lái xe điều khiển xe từ xa. Những chiếc xe không người lái này cũng có thể tiết kiệm thời gian và giảm bớt căng thẳng khi lái xe. Một số nhà sản xuất ô tô như BMW, Ford và Volvo đã xác nhận rằng sẽ có ô tô tự hành hoàn toàn vào cuối năm 2021.

#### Thiết bị đeo được

Thiết bị đeo được có sự quan tâm rất lớn trên các thị trường trên toàn thế giới. Nhiều công ty bắt đầu sản xuất những thiết bị này với số lượng khổng lồ để đáp ứng nhu cầu ngày càng cao như Google và Samsung. Theo Statista, số lượng thiết bị đeo được kết nối dự kiến sẽ đạt 830 triệu vào cuối năm 2020. Thiết bị đeo được trang bị cảm biến và có khả năng kết nối Internet để chia sẻ dữ liệu. Các cảm biến này thu thập dữ liệu về người dùng, dữ liệu này sau đó sẽ được xử lý để trích xuất thông tin có ý nghĩa. Hầu hết các thiết bị đeo thông dụng trong lĩnh vực thể dục, sức khỏe và giải trí.

### Những thách thức của IOT

Mặc dù các giải pháp IoT cung cấp vô số lợi ích, nhưng chúng đặt ra nhiều thách thức cần được giải quyết. Hầu hết các vấn đề phổ biến của hệ thống IoT bao gồm dữ liệu lớn, mạng, khả năng mở rộng, tính không đồng nhất, khả năng tương tác và bảo mật và quyền riêng tư được thảo luận trong phần này. Tất cả được tóm tắt như hình bên dưới.



Hình 19 Những thách thức của IoT

#### Dữ liệu lớn

Dữ liệu lớn là một cách diễn đạt khá mới lạ cho biết số lượng dữ liệu khổng lồ dù có cấu trúc hay không có cấu trúc, rất khó xử lý bằng các phương pháp cơ sở dữ liệu cổ điển và kỹ thuật phần mềm. Nó được đặc trưng bởi những gì được gọi là 5V, khối lượng, sự đa dạng, khả năng thay đổi, giá trị và vận tốc. Dữ liệu lớn nhận được sự quan tâm lớn từ nhiều tổ chức như một lĩnh vực công nghiệp mới như mạng xã hội trực tuyến (Twitter, Facebook và Instagram) vì có một lượng lớn dữ liệu được thu thập thông qua các mạng xã hội. Ví dụ, vào năm 2010, Twitter sản xuất trung bình khoảng 10 terabyte dữ liệu mỗi ngày.

Với hàng tỷ thiết bị và đối tượng, IoT là một trong những nguồn chính của dữ liệu lớn. Mặc dù Điện toán đám mây có thể được sử dụng để lưu trữ dữ liệu vĩnh viễn, việc xử lý lượng dữ liệu khổng lồ này là một vấn đề sâu rộng, đặc biệt là hiệu suất của các ứng dụng IoT khác nhau dựa trên dịch vụ quản lý dữ liệu. Ngoài ra, lượng dữ liệu khổng lồ này làm nảy sinh các vấn đề về bảo mật và quyền riêng tư vì đảm bảo tính toàn vẹn của dữ liệu sẽ là một nhiệm vụ rất khó đạt được.

#### Kết nối mạng

Động lực chính của hệ thống IoT là kết nối tất cả các đối tượng / thiết bị để chia sẻ thông tin của chúng. Các thiết bị này khác nhau về hình dạng và cấu trúc khiến nó sử dụng các giao thức mạng truyền thông khác nhau.

Việc triển khai một giao thức mạng cho IoT nên được xây dựng với việc cân nhắc đến hiệu suất và khả năng sử dụng của hệ thống. Điều này là do giao thức mạng có tác động lớn đến hoạt động của mạng. Vì vậy, việc lựa chọn giao thức mạng phù hợp là một vấn đề cần được quan tâm. Hơn nữa, việc lựa chọn cấu trúc liên kết mạng thích hợp cho giao thức là một thách thức khác.

#### Tính không đồng nhất

IoT là một trong những ví dụ phổ biến mô tả vấn đề không đồng nhất vì nó liên quan đến hàng tỷ thiết bị khác nhau về bản chất của chúng. Mục tiêu chính của hệ thống IoT là xây dựng một phương pháp chung để trừu tượng hóa tính không đồng nhất của các thiết bị này và hoàn thành việc khai thác tốt nhất chức năng của chúng.

Vì hệ thống IoT đang phát triển đáng kể, việc tìm kiếm các ứng dụng có thể tự thích ứng với các phần cứng và phần mềm khác nhau của các thiết bị IoT sẽ tiếp tục đạt được hiệu quả tối đa cho hệ thống IoT. Các nhà cung cấp dịch vụ phải cân nhắc đến sự đa dạng rộng rãi của các tùy chọn kết nối mạng, giao thức và phương thức truyền thông khi triển khai dịch vụ cho hệ thống IoT.

#### Khả năng tương tác

Khả năng tương tác đề cập đến khả năng của các thành phần hệ thống hợp tác với nhau một cách hiệu quả bất kể thông số kỹ thuật của chúng. Mặc dù sự kết nối với nhau của các thiết bị không đồng nhất IoT cho phép chia sẻ thông tin của chúng, dẫn đến việc tạo ra các dịch vụ mới, nhưng nó phải trả giá. Khi sự chấp nhận của hệ thống IoT tăng lên và số lượng các đối tượng và mạng được kết nối mở rộng, khả năng tương tác trở thành ưu tiên cơ bản để kết nối nhiều thứ khác nhau một cách hiệu quả

Bất chấp sự hiện diện của một số kết quả được đề xuất để giải quyết vấn đề về khả năng tương tác như khuôn khổ nguồn mở, công nghệ truyền dữ liệu và tạo lớp dịch vụ IoT chung, khả năng tương tác vẫn là một thách thức lớn cần được giải quyết.

#### Khả năng mở rộng

Khả năng mở rộng là một trong những thách thức quan trọng của hệ thống IoT đòi hỏi phải được xử lý để ngăn chặn sự gia tăng lớn của các thiết bị được kết nối. Khả năng mở rộng biểu thị khả năng của hệ thống để đối phó với sự phát triển tiềm năng của hệ thống một cách hiệu quả mà không ảnh hưởng đến hiệu suất của hệ thống.

Khả năng mở rộng là một hoạt động bắt buộc đối với hệ thống IoT để đáp ứng các yêu cầu khác nhau vì sự quan tâm của mọi người thay đổi theo thời gian và tình huống môi trường. Do đó, vấn đề khả năng mở rộng cần được nghiên cứu thêm để kiểm tra tiềm năng của hệ thống IoT khi số lượng thiết bị kết nối ngày càng tăng.

#### Bảo mật và quyền riêng tư

Sự gia tăng đáng kể của các thiết bị IoT trong môi trường của chúng ta dẫn đến việc tăng cơ hội tìm thấy các lỗ hổng bảo mật trong các thiết bị IoT được bảo mật kém mà không có bất kỳ biện pháp bảo mật tích hợp nào. Việc khai thác các lỗ hổng này dẫn đến việc đánh cắp thông tin người dùng và có thể gây nguy hiểm đến tính mạng của họ. Ngoài ra, vì các cảm biến IoT được phân phối trong môi trường xung quanh chúng ta, cho phép nó thu thập thông tin nhạy cảm, hành vi tiếp thị, thói quen và các thông tin khác vi phạm quyền riêng tư của chúng ta.

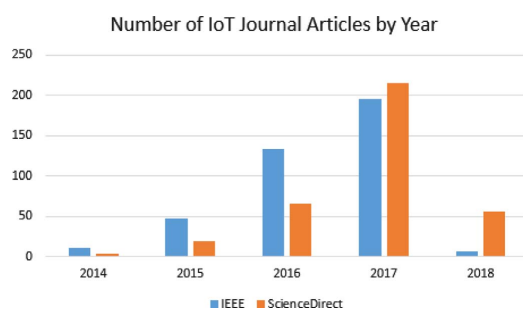
Do đó, xử lý các thách thức bảo mật trong hệ thống IoT nên là ưu tiên cơ bản để tăng cường áp dụng các ứng dụng IoT của người tiêu dùng. Ngoài ra, người dùng IoT cần hoàn toàn tự tin về tính bảo mật của các thiết bị IoT và các ứng dụng liên quan của họ, khi chúng trở nên tích hợp hơn vào các hoạt động cuộc sống hàng ngày của con người.

### 5G Internet of Things

#### Giới thiệu

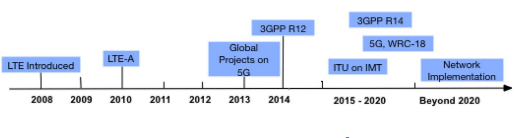
Theo báo của của International Data Corporation (IDC), những dịch vụ của mạng 5G sẽ khiến 70% công ty phải chi khoảng 1.2 tỉ đô cho các giải pháp kiểm soát kết nối. Những ứng dụng và mô hình kinh doanh mới trong tương lai về IoT sẽ có các khía cạnh quan trọng cốt lõi như là: massive connectivity, bảo mật, tin cậy, độ bao phủ của liên lạc không dây, độ trễ siêu thấp, ultra-realiable… cho số lượng khổng lồ các thiết bị IoT. Để đáp ứng các điều này, sự phát triển của Long Term Evolution (LTE) và công nghệ 5G được dự đoán sẽ là nền tảng cho các thiết bị IoT mới trong tương lai.

#### Thực trạng nghiên cứu của 5G và IOT

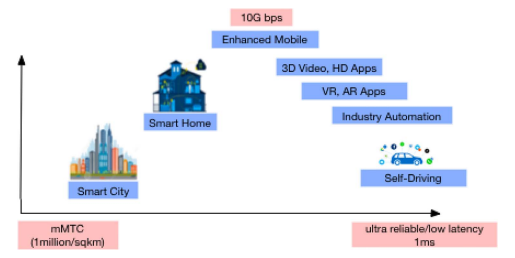


Hình 20 Số lượng bài báo về 5G-IoT theo năm

Kể từ năm 2012, “Long Term Evolution” (LTE) của kết nối 4G, trở thành sự đa dạng nhanh nhất và bền nhất của 4G so với các công nghệ cạnh tranh như BLE, WiMaxb, ZigBee, SigFox, LoRa. Theo kỳ vọng, 5G với tư cách là công nghệ của thế hệ kế tiếp, được kỳ vọng sẽ có các phương pháp giải quyết được các vướng mắt mà 4G đang gặp phải như là phương pháp giao tiếp phải phức tạp hơn, khả năng tính toán tốt hơn, trí thông minh… để phù hợp với những yêu cầu trong môi trường thông minh và công nghiệp 4.0…



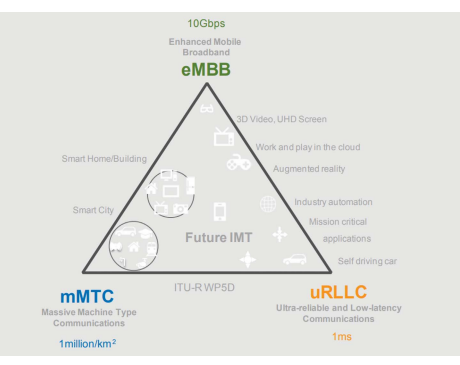
Hình 21 Dòng thời gian cho đến 5G



Hình 22 Machine type communication (MTC) trong 5G-IoT

Hình trên cho thấy sự khổng lồ trong việc liên lạc giữa các thiết bị IoT sẽ tạo nên nhu cầu về một mạng lưới kết nối khổng lồ. Trong hai thập kỷ qua, các phương pháp giao tiếp giữa máy với máy (M2M) đã được cài đặt rất nhiều như Zigbee, Wifi cho tầm ngắn, LPWA và Sigfox hoặc Lora cho tầm xa. Điều này đã gây phân hóa và là một thách thức cho 5G để đáp ứng các yêu cầu của các thiết bị IoT.

#### 5G-IoT Architecture



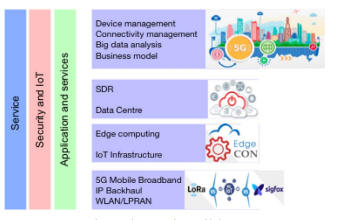
Hình 23 Kiến trúc của IMT

Hình trên cho thấy kiến trúc của thiết bị di động viễn thông quốc tế trong tương lai (IMT), trong đó mạng 5G dự kiến sẽ cung cấp:

* Băng thông rộng di động nâng cao (eMBB).
* Siêu tin cậy và giao tiếp độ trễ thấp (uRLLC).
* Cho liên lạc giữa các loại máy khổng lồ.

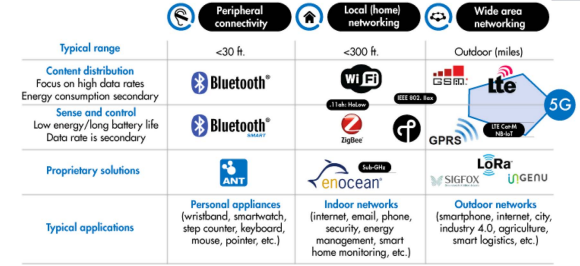
5G- IoT được dự kiến là sẽ cung cấp các ứng dụng với real-time, đáp ứng yêu cầu, luôn trực tuyến, có thể cấu hình lại và mang tính trải nghiệm xã hội. Những điều vốn bắt buộc kiến trúc 5G-IoT phải có thể kết hợp end-to-end, có tính năng hoạt động nhanh nhẹn, tự động và thông minh trong mỗi giai đoạn. Các kiến trúc 5G-IoT dự kiến sẽ cung cấp:

* Các mạng độc lập hợp lý theo nhiều yêu cầu của các ứng dụng.
* Sử dụng mạng truy cập vô tuyến dựa trên đám mây (CloudRAN) để xây dựng lại mạng truy cập vô tuyến (RAN) nhằm cung cấp các kết nối lớn theo nhiều tiêu chuẩn và triển khai RAN theo yêu cầu các chức năng như hình dưới.
* Đơn giản hóa kiến trúc mạng lõi để thực hiện điều khiển theo yêu cầu.



Hình 24 Các yêu cầu mà 5G cần đáp ứng

#### Các công nghệ cho phép chính trong 5G-IOT



Hình 25 các công nghệ liên hệ với 5G-IoT

Kiến trúc 5G-IoT là một chủ đề chính. Hình dưới cho thấy một nguyên mẫu của ngôi nhà thông minh tích hợp cơ sở hạ tầng 5G, trong đó 5G-IoT kết nối một số thiết bị IoT hạn chế tài nguyên với các ứng dụng dựa trên đám mây từ xa bằng cách sử dụng nhiều giao thức truyền thông không dây. 5G-IoT chủ yếu sẽ dựa trên các hệ thống không dây 5G, vì vậy kiến trúc thường bao gồm hai mặt phẳng:

* Mặt phẳng dữ liệu, tập trung vào cảm biến dữ liệu thông qua mạng fronthaul do phần mềm xác định.
* Mặt phẳng điều khiển, bao gồm các công cụ quản lý mạng và các nhà cung cấp dịch vụ (ứng dụng) có thể cấu hình lại.



Hình 26 Ví dụ về kiến trúc 5G-IoT thực tế

Kiến trúc 5G-IoT phải có thể đáp ứng các yêu cầu về dịch vụ từ các khía cạnh sau:

* Khả năng mở rộng, đám mây hóa / ảo hóa chức năng mạng (NFV).
* Khả năng ảo hóa mạng.
* Quản lý mạng phức tạp, bao gồm kiểm soát tính di động, kiểm soát access và ảo hóa mạng tối ưu về tài nguyên.

Nhà cung cấp dịch vụ thông minh, kiến trúc sẽ có thể cung cấp các dịch vụ thông minh dựa trên phân tích dữ liệu lớn.

# PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG

## Mục tiêu của đồ án

Mấy năm trở lại đây, công nghệ blockchain nổi lên như một hiện tượng công nghệ với những ưu điểm tuyệt vời có thể hỗ trợ cho cuộc sống của con người trở nên dễ dàng hơn. Đặc biệt trong hệ thống bầu cử, công nghệ blockchain hoàn toàn có thể khắc phục được những nhược điểm của các hệ thống bầu cử cũ. Khi sử dụng blockchain, tất cả dữ liệu của quá trình bầu cử sẽ được lưu lại trực tuyến và có thể kiểm chứng một cách công khai mặc dù vẫn duy trì được tính ẩn danh của cử tri. Việc sử dụng công nghệ Blockchain – IOT vào bỏ phiếu, bầu cử nhằm mục đích làm cho các quy trình bỏ phiếu của chính phủ trở nên an toàn, chính xác và minh bạch hơn bao giờ hết.

## Thiết kế hệ thống

### Thiết kế phần cứng

Thiết bị hệ thống nhúng sử dụng phần cứng là ESP8266 và computer để làm sever cho blockchain.

#### Giới thiệu ESP8266

ESP8266 là một mạch vi điều khiển có thể giúp chúng ta điều khiển các thiết bị điện tử.Thêm vào đó nó được tích hợp wi-fi 2.4GHz có thể dùng cho lập trình.

#### Thông số kĩ thuật

* WiFi: 2.4 GHz hỗ trợ chuẩn 802.11 b/g/n
* Điện áp hoạt động: 3.3V
* Điện áp vào: 5V thông qua cổng USB
* Số chân I/O: 11 (tất cả các chân I/O đều có Interrupt/PWM/I2C/One-wire, trừ chân D0)
* Số chân Analog Input: 1 (điện áp vào tối đa 3.3V)
* Bộ nhớ Flash: 4MB
* Giao tiếp: Cable Micro USB ( tương đương cáp sạc điện thoại )
* Hỗ trợ bảo mật: WPA/WPA2
* Tích hợp giao thức TCP/IP
* Lập trình trên các ngôn ngữ: C/C++, Micropython,…



Hình 27 ESP8266 Pinout

### Thiết kế phần mềm

#### NodeJS

Nodejs là một mã nguồn được xây dựng dựa trên nền tảng Javascript V8 Engine. Nodejs sử dụng rộng bởi hàng ngàn lập trình viên trên toàn thế giới. NodeJS có thể chạy trên nhiều nền tảng hệ điều hành khác nhau từ Windows cho tới Linux, MacOs nên đó cũng là một lợi thế. NodeJS cung cấp các thư viện phong phú ở dạng Javascript Module khác nhau giúp đơn giản hóa việc lập trình và giảm thời gian ở mức thấp nhất.



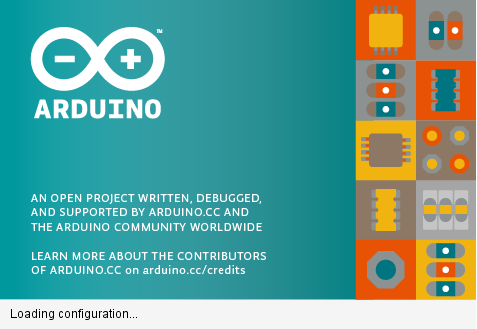
Hình 28 Node JS

Các tính năng vượt trội của Nodejs:

* Không đồng bộ: Tất cả các API của Nodejs đều không đồng bộ (none-blocking), nó chủ yếu dựa trên nền của Nodejs Server và chờ đợi Server trả dữ liệu về. Việc di chuyển máy chủ đến các API tiếp theo sau khi gọi và cơ chế thông báo các sự kiện của Node.js giúp máy chủ để có được một phản ứng từ các cuộc gọi API trước (Realtime).
* Chạy rất nhanh: Nodejs được xây dựng dựa vào nền tảng V8 Javascript Engine nên việc thực thi chương trình rất nhanh.
* Đơn luồng nhưng khả năng mở rộng cao: Node.js sử dụng một mô hình luồng duy nhất với sự kiện lặp. cơ chế tổ chức sự kiện giúp các máy chủ để đáp ứng một cách không ngăn chặn và làm cho máy chủ cao khả năng mở rộng như trái ngược với các máy chủ truyền thống mà tạo đề hạn chế để xử lý yêu cầu. Node.js sử dụng một chương trình đơn luồng và các chương trình tương tự có thể cung cấp dịch vụ cho một số lượng lớn hơn nhiều so với yêu cầu máy chủ truyền thống như Apache HTTP Server.
* Không đệm: Nodejs không đệm bất kì một dữ liệu nào và các ứng dụng này chủ yếu là đầu ra dữ liệu.
* Có giấy phép: Nodejs đã được cấp giấy phép bởi MIT License.

#### ArduinoIDE

Arduino IDE là một phần mềm với một mã nguồn mở, được sử dụng chủ yếu để viết và biên dịch mã vào module Arduino. Nó bao gồm phần cứng và phần mềm. Phần cứng chứa đến 300,000 board mạch được thiết kế sẵn với các cảm biến, linh kiện. Phần mềm giúp bạn có thể sử dụng các cảm biến, linh kiện ấy của Arduino một cách linh hoạt phù hợp với mục đích sử dụng.



Hình 29 Arduino IDE

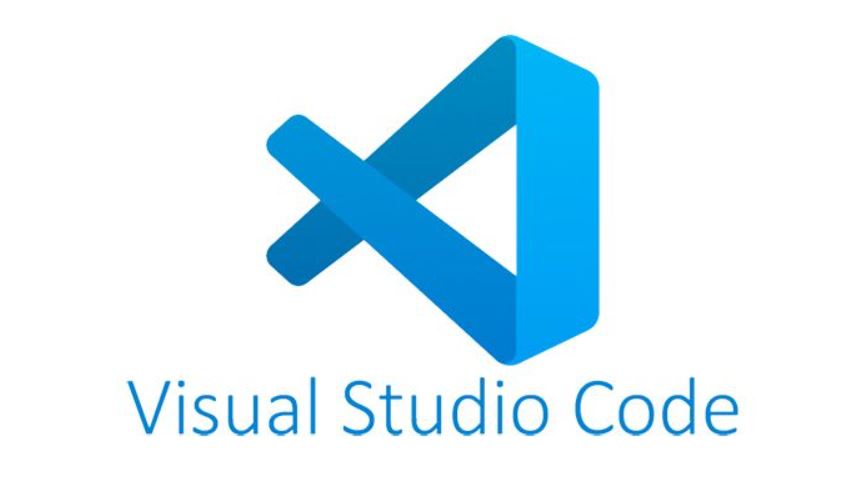
IDE trong Arduino IDE là phần có nghĩa là mã nguồn mở. Nghĩa là phần mềm này miễn phí cả về phần tải về lẫn phần bản quyền. Người dùng có quyền sửa đổi, cải tiến, phát triển, nâng cấp theo một số nguyên tắc chung được nhà phát hành cho phép mà không cần xin phép ai, điều mà họ không được phép làm đối với các phần mềm nguồn đóng.

Arduino IDE sử dụng ngôn ngữ lập trình C/C++ rất phổ biến trong giới lập trình. Bất kỳ đoạn code nào của C/C++ thì Arduino IDE đều có thể nhận dạng, giúp các lập trình viên thuận tiện trong việc thiết kế chương trình lập cho các bo mạch Arduino.

Arduino có một module quản lý bo mạch, nơi người dùng có thể chọn bo mạch mà họ muốn làm việc cùng và có thể thay đổi bo mạch thông qua Menu. Quá trình sửa đổi lựa chọn cũng liên tục tự động cập nhật để các dữ liệu có sẵn trong bo mạch và dữ liệu sửa đổi đồng nhất với nhau. Bên cạnh đó, Arduino IDE cũng giúp bạn tìm ra lỗi từ code mà bạn viết, qua đó giúp bạn sửa lỗi kịp thời tránh tình trạng bo mạch Arduino làm việc với code lỗi quá lâu dẫn đến hư hỏng hoặc tốc độ xử lý bị giảm sút.

#### Visual Studio Code

Visual Studio Code là một trình soạn thảo mã nguồn được phát triển bởi Microsoft dành cho Windows, Linux và macOS. Nó hỗ trợ chức năng debug, đi kèm với Git, có chức năng nổi bật cú pháp (syntax highlighting), tự hoàn thành mã thông minh, snippets, và cải tiến mã nguồn. Nó cũng cho phép tùy chỉnh, do đó, người dùng có thể thay đổi theme, phím tắt, và các tùy chọn khác. Nó miễn phí và là phần mềm mã nguồn mở theo giấy phép MIT, mặc dù bản phát hành của Microsoft là theo giấy phép phần mềm miễn phí.

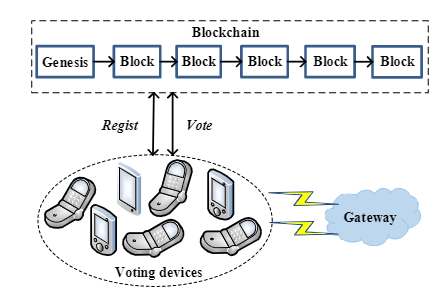


Hình 30 Visual Studio Code

Visual Studio Code là một trình biên tập mã. Nó hỗ trợ nhiều ngôn ngữ và chức năng tùy vào ngôn ngữ sử dụng theo như trong bảng sau. Nhiều chức năng của Visual Studio Code không hiển thị ra trong các menu tùy chọn hay giao diện người dùng. Thay vào đó, chúng được gọi thông qua khung nhập lệnh hoặc qua một tập tin .json (ví dụ như tập tin tùy chỉnh của người dùng). Khung nhập lệnh là một giao diện theo dòng lệnh. Tuy nhiên, nó biến mất khi người dùng nhấp bất cứ nơi nào khác, hoặc nhấn tổ hợp phím để tương tác với một cái gì đó ở bên ngoài đó. Tương tự như vậy với những dòng lệnh tốn nhiều thời gian để xử lý. Khi thực hiện những điều trên thì quá trình xử lý dòng lệnh đó sẽ bị hủy.

### Thiết kế phần chức năng

#### Thiết kế tổng quan



Hình 31 Sơ đồ tổng quan hệ thống

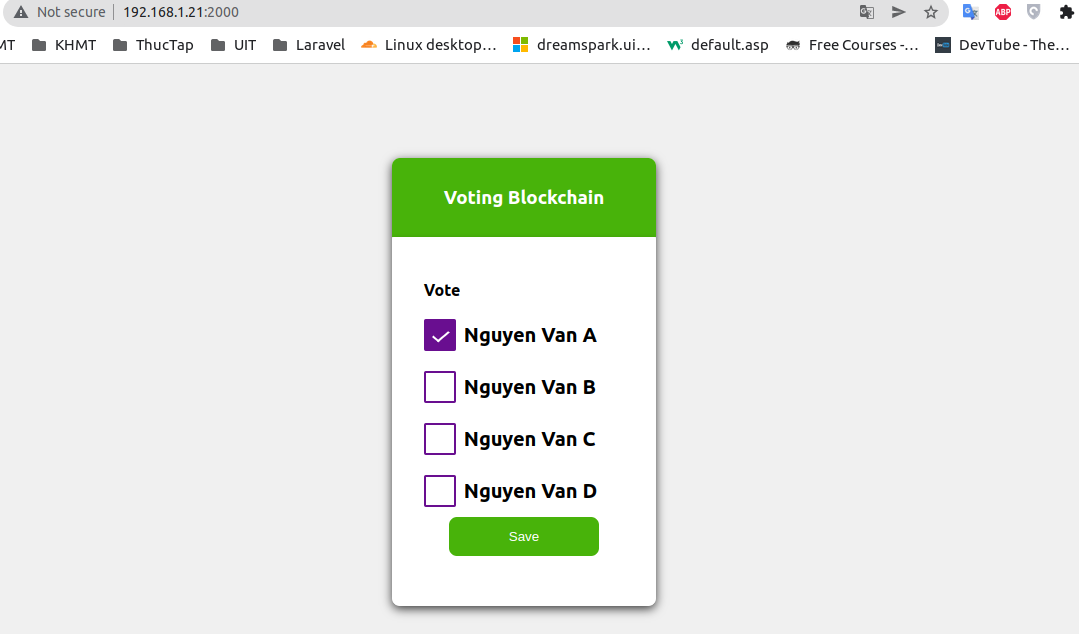
* Voting device: Ở đây, các thiết bị IOT sẽ đóng vai trò là client người dùng sẽ thực hiện vote trên giao diện mỗi thiết bị sẽ chứa một id để định danh thiết bị đó
* Blockchain: Hệ thống backend Blockchain sẽ được xây dựng bằng NodeJS, nơi lưu trữ thông tin vote từ người dùng.
* Vote: Các thiết bị IOT sẽ thực hiện giao thức post gửi request tới server Blockchain để tại block mới có chứa dữ liệu là thông tin vote.

#### Thiết kế giao diện trên Webserver sử dụng ESP8266

Vi xử lý ESP8266 sử dụng webserver để thực hiện chạy lệnh html để hiển thị giao diện. Giao diện bao gồm 4 checkbox dành cho 4 người được bầu cử và 1 nút bấm để thực hiện ghi dữ liệu từ checkbox vào blockchain

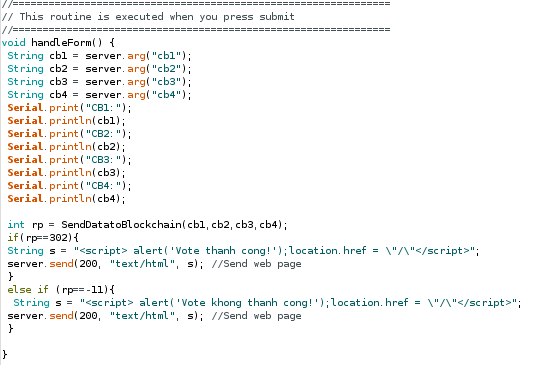


Hình 32 Mã html hiển thị 4 checkbox và nút bấm

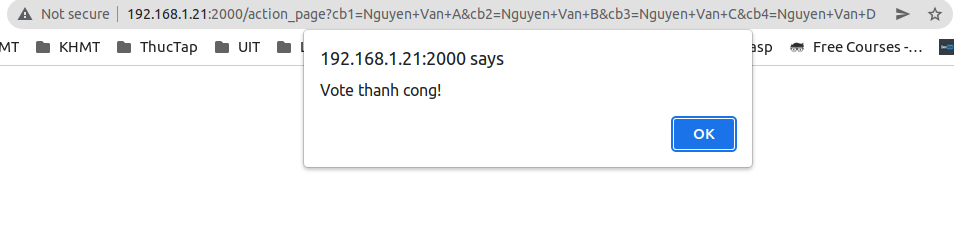


Hình 33 Giao diện Voting

Sau khi bấm nút button, server sẽ tạo thêm một alert để xuất thông tin dữ liệu có được ghi vào blockchain hay chưa



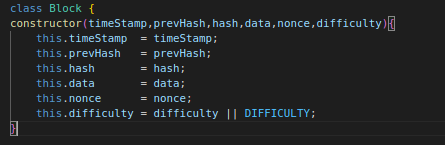
Hình 34 Mã html hiển thị thông báo



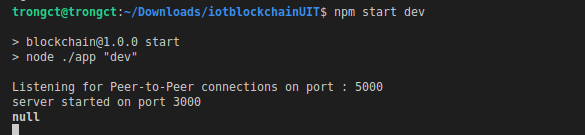
Hình 35 Giao diện hiển thị thông báo

#### Thiết kế mạng Blockchain

Như đã phân tích blockchain ở phần trên, cấu trúc một block bao gồm timestamp, prevHash, Hash, data (transaction), nonce, difficulty. Hình dưới là cấu trúc của một block được viết bằng javascript



Hình 36 Cấu trúc một block



Hình 37 Khởi tạo server

Nodejs là một nền tảng để phát triển, xây dựng backend và Expressjs là một framework được xây dựng trên nền tảng của Nodejs. Nó cung cấp các tính năng mạnh mẽ để phát triển web hoặc mobile. Expressjs hỗ trợ các method HTTP và midleware tạo ra API. Đoạn dưới là API nơi mà thiết bị IOT gửi request đến và thực hiện các phương thức GET/POST/PUT/...



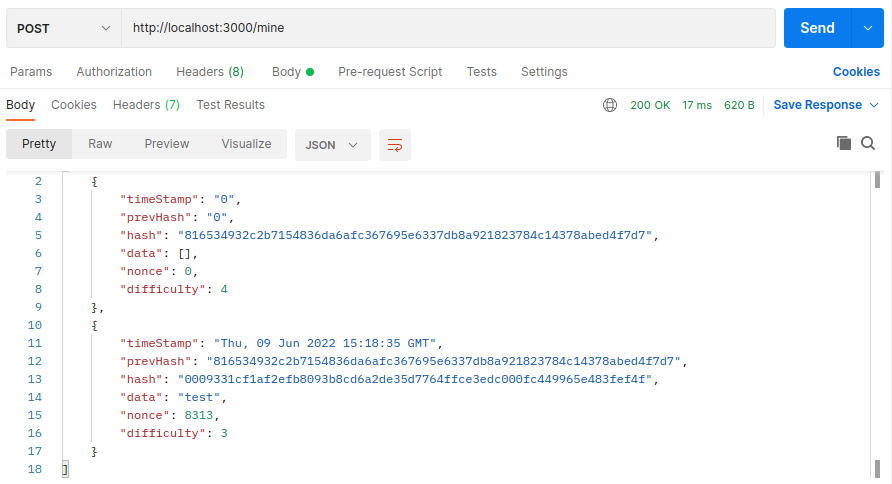
Hình 38 API tạo một block mới

# KẾT QUẢ THỰC NGHIỆM

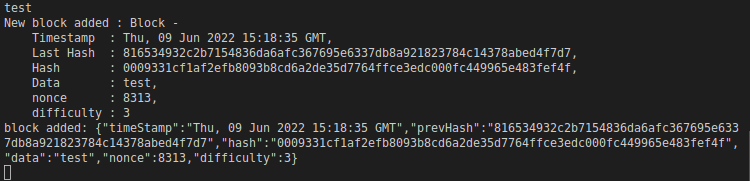
## Kết quả đạt được

Postman là một công cụ cho phép chúng ta thao tác với API, phổ biến nhất là REST. Postman hiện là một trong những công cụ phổ biến nhất được sử dụng trong thử nghiệm các API. Với Postman, ta có thể gọi Rest API mà không cần viết dòng code nào. Postman hỗ trợ tất cả các phương thức HTTP (GET, POST, PUT, PATCH, DELETE, …). Bên cạnh đó, nó còn cho phép lưu lại lịch sử các lần request, rất tiện cho việc sử dụng lại khi cần.

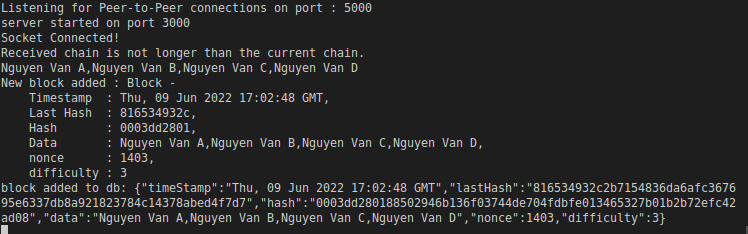
Hình bên dưới là kết quả trả về sau khi gọi API từ server blockchain



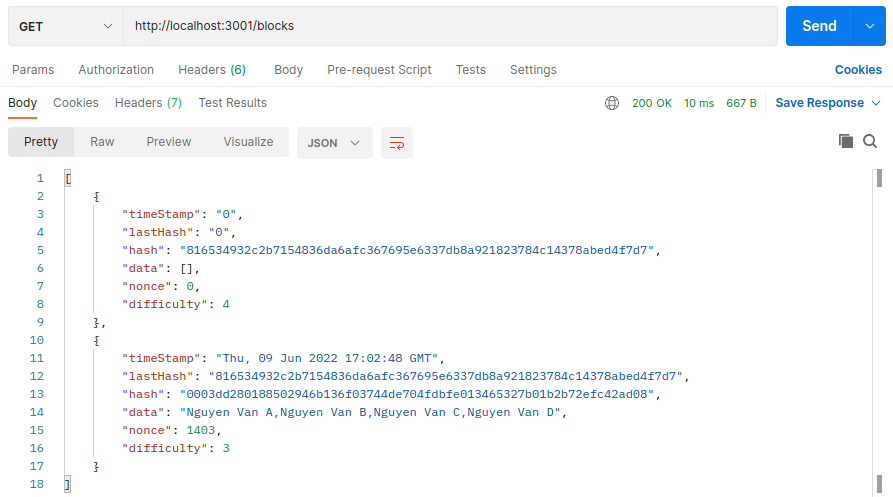
Hình 39 Kết quả khi gọi API tạo mới block sử dụng Postman



Hình 40 Kết quả khi tạo mới block trên terminal



Hình 41 Kết quả khi truyền dữ liệu voting từ thiết bị IOT



Hình 42 Kết quả khi goi API hiển thị dữ liệu voting từ port P2P trên Postman

## Đánh giá hệ thống

Ưu điểm: Đáp ứng được tính chất minh bạch của hệ thống voting. Xây dựng được blockchain cơ bản và ứng dụng iot vào blockchain

Hạn chế:

Kỹ thuật xây dựng dừng ở mức khá đơn giản.

Mô hình dành cho cơ bản, chưa hướng đến những hệ thống có độ phức tạp lớn hơn.

# KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

## Kết kuận

### Những khó khăn

* Do phải làm việc online nên tương tác, hoạt động trong nhóm còn hạn chế, giải quyết các lỗi xảy ra chậm.
* Vì nhiều vấn đề nên nhóm còn nhiều hạn chế trong việc phát triển, sáng tạo về thiết kế trong hệ thống.

### Kết quả và những kinh nghiệm tích lũy

* Cơ bản xây dựng được một hệ thống blockchain kết hợp IOT có các chức năng phục vụ cho hệ thống bỏ phiếu.
* Hiểu thêm được kiến thức làm việc với các công nghệ mới và kinh nghiệm thiết kế hệ thống IoT.

## Hướng phát triển

* Mở rộng mô hình cho những hệ thống bầu cử lớn hơn.
* Phát triển thêm hệ thống backend để nâng cao bảo mật.
* Phát triển thêm tính năng về giao diện

TÀI LIỆU THAM KHẢO

Theo chuẩn IEEE