

ĐẠI HỌC BÁCH KHOA HÀ NỘI
KHOA TOÁN - TIN



BÀI TẬP LỚN
MẬT MÃ VÀ ĐỘ PHỨC TẠP THUẬT TOÁN

TÊN ĐỀ TÀI: ỨNG DỤNG CỦA BLOCKCHAIN TRONG
BẢO MẬT HỆ THỐNG IOT

Giảng viên hướng dẫn: PGS. TS. Nguyễn Đình Hân
TS. Ngô Thị Hiền

Nhóm sinh viên thực hiện: Nguyễn Thế Phong 20216868
Triệu Hoàng Long 20216849
Khổng Nguyên Thiêm 20210814

Mã lớp học: 150342

Hà Nội, tháng 6 năm 2024

Bảng đánh giá thành viên trong nhóm

| STT | Họ và Tên | MSSV | Chức vụ | Công Việc Thực Hiện | Điểm |
|-----|--------------------|----------|-------------|--|------|
| 1 | Nguyễn Thế Phong | 20216868 | Trưởng nhóm | <ul style="list-style-type: none"> - Tìm hiểu nội dung chương 3,4,5 - Mô phỏng 2 ứng dụng - Làm slides thuyết trình - Kiểm tra và hoàn thiện báo cáo, slides - Thuyết trình | ... |
| 2 | Triệu Hoàng Long | 20216849 | Thành viên | <ul style="list-style-type: none"> - Tìm hiểu nội dung chương 1 - Làm slides thuyết trình - Kiểm tra và hoàn thiện báo cáo, slides - Thuyết trình | ... |
| 3 | Khổng Nguyên Thiêm | 20216832 | Thành viên | <ul style="list-style-type: none"> - Tìm hiểu nội dung chương 2 - Làm báo cáo - Kiểm tra và hoàn thiện báo cáo, slides - Thuyết trình | ... |

Mục lục

| | |
|--|-----------|
| Lời nói đầu | 2 |
| 1 Tổng quan về hệ thống IoT | 4 |
| 1.1 Khái niệm IoT | 4 |
| 1.2 Cấu trúc của hệ thống IoT | 5 |
| 1.3 Kiến trúc hướng dịch vụ của hệ thống IoT | 5 |
| 1.3.1 Lớp cảm biến | 6 |
| 1.3.2 Lớp mạng | 7 |
| 1.3.3 Lớp dịch vụ | 8 |
| 1.3.4 Lớp giao diện | 8 |
| 1.4 Các thành phần cơ bản của hệ thống IoT | 8 |
| 1.5 Nguyên lý hoạt động của IoT | 10 |
| 1.6 Các đặc tính cơ bản của IoT | 11 |
| 2 Tổng quan về công nghệ Blockchain | 12 |
| 2.1 Công nghệ Blockchain | 12 |
| 2.2 Hệ thống chuỗi khối (Blockchain system) | 13 |
| 2.3 Sổ cái phân tán (Distributed ledger) | 14 |
| 2.4 Mạng ngang hàng và giao thức đồng thuận | 15 |
| 2.4.1 Mạng ngang hàng (Peer-to-Peer Network) | 15 |
| 2.4.2 Giao thức đồng thuận | 16 |
| 2.5 Hàm băm | 17 |
| 2.5.1 Hàm băm mật mã học (Cryptographic hash function) . . | 17 |
| 2.5.2 Hàm băm SHA-256 | 17 |
| 2.6 Đặc tính của Blockchain | 18 |
| 2.6.1 Tính phi tập trung | 18 |
| 2.6.2 Tính bảo mật | 19 |
| 2.6.3 Tính ổn định | 19 |
| 2.6.4 Tính khắc phục | 19 |

| | | |
|----------|---|-----------|
| 3 | Hệ bảo mật của hệ thống IoT | 20 |
| 3.1 | Vấn đề bảo mật cấp thấp | 21 |
| 3.2 | Vấn đề bảo mật cấp trung | 21 |
| 3.3 | Vấn đề bảo mật cấp cao | 21 |
| 4 | Blockchain trong hệ thống IoT | 23 |
| 4.1 | Tổng quan về công nghệ Blockchain trong IoT | 23 |
| 4.1.1 | Lợi ích của việc hợp nhất IoT và Blockchain | 26 |
| 4.1.2 | Nền tảng Blockchain cho Công nghiệp Internet of Things (BPIIoT) | 27 |
| 4.1.3 | Chăm sóc sức khỏe thông minh trong IoT với Blockchain | 27 |
| 4.1.4 | Thành phố thông minh dựa trên Blockchain (BC) | 27 |
| 4.1.5 | Nhà thông minh dựa trên Blockchain (BC) | 28 |
| 4.1.6 | Mô hình thương mại điện tử (eBusiness) IoT sử dụng Blockchain | 30 |
| 4.1.7 | Quản lý chuỗi cung ứng (SCM) sử dụng Blockchain | 31 |
| 4.2 | Lợi ích của công nghệ Blockchain trong hệ bảo mật IoT | 31 |
| 4.2.1 | Tốc độ thay đổi dữ liệu nhanh chóng | 31 |
| 4.2.2 | Tăng cường bảo mật | 32 |
| 4.2.3 | Mạng lưới cung cấp hiệu quả | 33 |
| 4.2.4 | Giảm chi phí | 34 |
| 4.2.5 | Kế toán minh bạch | 34 |
| 5 | Mô phỏng công nghệ Blockchain trong hệ bảo mật IoT | 36 |
| 5.1 | Mô phỏng hàm băm sử dụng thuật toán SHA-256 trong chuỗi khối Blockchain | 36 |
| 5.1.1 | Nội dung | 36 |
| 5.1.2 | Các lớp trong chương trình | 36 |
| 5.1.3 | Lớp Block: Lưu các dữ liệu | 37 |
| 5.1.4 | Kết quả | 38 |
| 5.2 | Mô phỏng kiến trúc cửa sổ trượt Blockchain cho IoT | 40 |
| | Tổng kết | 45 |
| | Tài liệu tham khảo | 49 |
| | Phụ lục | 50 |

Lời nói đầu

Tầm quan trọng của đề tài

Trong thời đại công nghệ số, bảo mật hệ thống IoT (Internet of Things) trở nên vô cùng quan trọng do sự gia tăng số lượng và đa dạng của các thiết bị kết nối. Các thiết bị này hiện diện trong nhiều lĩnh vực từ nhà thông minh, y tế, đến công nghiệp. Tuy nhiên, chúng cũng đối mặt với nhiều mối đe dọa bảo mật phức tạp.

Việc áp dụng công nghệ blockchain vào bảo mật hệ thống IoT không chỉ là một giải pháp tiềm năng mà còn là một bước tiến quan trọng. Blockchain, với đặc tính phân tán, không thể thay đổi và an toàn, giúp cải thiện tính toàn vẹn và bảo mật dữ liệu, đồng thời giải quyết các vấn đề về xác thực và quản lý quyền truy cập.

Nghiên cứu về sự kết hợp này không chỉ thúc đẩy phát triển công nghệ tiên tiến mà còn mang lại lợi ích thực tiễn, tạo ra các hệ thống thông minh, an toàn và đáng tin cậy hơn, góp phần vào sự phát triển bền vững và nâng cao chất lượng cuộc sống.

Mục tiêu đề tài

Mục tiêu của đề tài này là nghiên cứu và đánh giá tiềm năng ứng dụng công nghệ blockchain trong việc tăng cường bảo mật cho hệ thống IoT. Đầu tiên, đề tài sẽ cung cấp cái nhìn toàn diện về hệ thống IoT và công nghệ blockchain, bao gồm các thành phần, nguyên lý hoạt động và các đặc tính nổi bật. Tiếp theo, nghiên cứu sẽ phân tích các thách thức bảo mật hiện tại của hệ thống IoT và cách blockchain có thể giải quyết chúng, như bảo mật truyền thông, quản lý danh tính và xác thực, và chống tấn công giả mạo. Cuối cùng, đề tài sẽ mô phỏng việc áp dụng blockchain trong hệ bảo mật IoT, đánh giá hiệu quả và tính khả thi của các giải pháp được đề xuất, nhằm cải thiện an ninh, nâng cao hiệu quả và đảm bảo tính bền vững cho các hệ thống IoT trong thực tế.

Phương pháp nghiên cứu

Phương pháp nghiên cứu của đề tài này bao gồm việc kết hợp giữa nghiên cứu lý thuyết và thực nghiệm. Đầu tiên, nghiên cứu sẽ tiến hành thu thập và tổng hợp các tài liệu, bài báo khoa học và báo cáo liên quan đến hệ thống IoT và công nghệ blockchain. Tiếp theo, phân tích các thách thức bảo mật trong hệ thống IoT và các giải pháp blockchain tiềm năng thông qua việc xem xét các mô hình lý thuyết và các nghiên cứu trước đây. Cuối cùng, đề tài sẽ thực hiện mô phỏng các giải pháp blockchain trong hệ bảo mật IoT bằng cách sử dụng các công cụ phần mềm chuyên dụng, từ đó đánh giá hiệu quả, tính khả thi và đưa ra các đề xuất cụ thể để cải thiện an ninh và hiệu suất của hệ thống IoT.

Nội dung đề tài

Chương 1: Tổng quan về hệ thống IoT

Chương 2: Tổng quan về công nghệ Blockchain

Chương 3: Hệ bảo mật của hệ thống IoT

Chương 4: Blockchain trong hệ thống IoT

Chương 5: Mô phỏng công nghệ Blockchain trong hệ bảo mật IoT

Chương 1

Tổng quan về hệ thống IoT

1.1 Khái niệm IoT

IoT là viết tắt của cụm từ tiếng Anh *Internet of Things* hay *Internet vạn vật*. Trong cụm Internet of Things ta có thể hiểu như sau:

- **Internet:** đây là chỉ một hệ thống trung gian giúp tiếp nhận, xử lý và truyền đi những thông tin, dữ liệu giữa thiết bị này và thiết bị khác.
- **Things (vạn vật):** có thể hiểu là tất cả những thiết bị có vai trò phục vụ và cung cấp thông tin, nhu cầu cho hệ thống vận hành Internet ở trên. Rất nhiều ví dụ thực tế quanh chúng ta có thể được coi là các thiết bị trong “vạn vật” của hệ thống IoT từ những cảm biến đơn giản cho đến những cấu trúc phức tạp như nhà thông minh, đồng hồ đeo tay điện tử,...

Vậy có thể kết luận rằng hệ thống IoT là một mạng lưới khổng lồ với các thiết bị được kết nối với nhau thông qua Internet. Các thiết bị này có chức năng thu thập và chia sẻ dữ liệu về cách chúng được sử dụng cũng như môi trường chúng được vận hành. Tất cả dữ liệu được thu thập bằng các cảm biến được gắn trong mọi thiết bị mà chúng ta đang sử dụng.

Ý tưởng về một mạng lưới các thiết bị thông minh đã được thảo luận vào năm 1982, tại đại học Đại học Carnegie Mellon đã nghiên cứu ra những khái niệm IoT đầu tiên [3]. Họ đã tiến hành thử nghiệm bằng cách kết nối Internet vào một máy bán nước tự động và lập trình nó tự động báo cáo kiểm kho cũng như độ lạnh của từng chai nước khi bỏ vào máy.[2]

Năm 1999, Kevin Ashton - người sáng lập ra Trung tâm Auto-ID ở đại học MIT đã đưa ra cụm từ *Internet of Things* [1] để mô tả một hệ thống mà Internet được kết nối với thế giới vật chất thông qua các cảm biến.

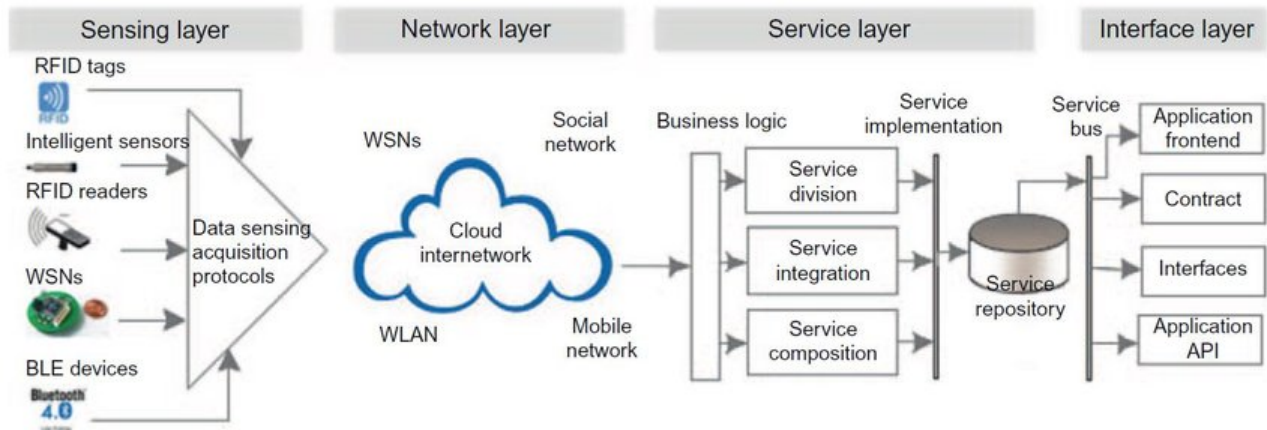
1.2 Cấu trúc của hệ thống IoT

Một hệ thống IoT sẽ có 4 thành phần chính như sau:

- **Thiết bị (Things)** là thành phần quan trọng trong hệ thống, bao gồm các cảm biến như nhiệt độ, áp suất, ánh sáng, và nhiều loại cảm biến khác nhau. Nhiệm vụ của chúng không chỉ là cảm nhận tín hiệu từ môi trường xung quanh mà còn chuyển đổi chúng thành dữ liệu số. Điều này mở ra khả năng theo dõi và kiểm soát các yếu tố như thời tiết, môi trường làm việc, hay sự hiện diện của một đối tượng nào đó.
- **Trạm kết nối (Gateways)** đóng vai trò quan trọng trong việc thu thập và truyền tải dữ liệu từ các thiết bị tới hạ tầng mạng. Chúng giúp cầu nối giữa thiết bị và mạng, có thể là trạm trung gian hoặc các thiết bị truyền thông chính.
- **Hạ tầng mạng (Network and Cloud)** chịu trách nhiệm về việc chuyển đổi, lưu trữ, và quản lý lượng lớn dữ liệu từ các thiết bị. Dữ liệu này thường được chuyển đến đám mây để lưu trữ và phân tích. Hạ tầng mạng đảm bảo tính liên tục và an toàn cho toàn bộ quá trình truyền tải thông tin.
- **Bộ phân tích và xử lý dữ liệu (Services-creation and Solution Layers)** là nơi dữ liệu được biến đổi thành thông tin hữu ích. Các giải pháp thông minh và ứng dụng được tạo ra từ quá trình này, giúp tối ưu hóa và tăng cường trải nghiệm người dùng. Các ứng dụng trên điện thoại hay máy tính thường là kết quả của bước này, mang lại sự thuận tiện và linh hoạt trong việc quản lý và kiểm soát các thiết bị IoT.

1.3 Kiến trúc hướng dịch vụ của hệ thống IoT

Một yêu cầu quan trọng của IoT là các vật trong mạng phải được kết nối với nhau. Kiến trúc hệ thống IoT phải đảm bảo các hoạt động của IoT, giúp thu hẹp khoảng cách giữa thế giới vật lý và thế giới ảo. Thiết kế kiến trúc IoT liên quan đến nhiều yếu tố như mạng, truyền thông, mô hình kinh doanh và quy trình, và bảo mật. Trong việc thiết kế kiến trúc IoT, khả năng mở rộng, khả năng tương thích và khả năng tương tác giữa các thiết bị khác nhau và các mô hình của chúng cần được xem xét. Do thực tế là các vật có thể di chuyển vật lý và cần tương tác với nhau trong chế độ thời gian thực, kiến trúc IoT cần phải linh hoạt để các thiết bị có thể tương tác với các vật khác một cách động và hỗ trợ giao tiếp sự kiện một cách rõ ràng [9].



Hình 1.1: Caption

Kiến trúc hướng dịch vụ (SoA), bao gồm bốn lớp với các chức năng khác nhau, cung cấp khả năng tương tác giữa các thiết bị theo nhiều cách. Các lớp này bao gồm:

- **Lớp cảm biến:** Tích hợp với tất cả các đối tượng (vật) có sẵn để cảm nhận trạng thái của chúng.
- **Lớp mạng:** Là cơ sở hạ tầng hỗ trợ các kết nối không dây hoặc có dây giữa các vật.
- **Lớp dịch vụ:** Tạo và quản lý các dịch vụ cần thiết cho người dùng hoặc ứng dụng.
- **Lớp giao diện:** Bao gồm các phương thức tương tác với người dùng hoặc ứng dụng.

1.3.1 Lớp cảm biến

IoT được kỳ vọng là một mạng lưới vật lý kết nối rộng rãi, trong đó các vật được kết nối liên tục và có thể được kiểm soát từ bất kỳ đâu. Trong lớp cảm biến, các hệ thống thông minh trên các thẻ hoặc cảm biến có khả năng tự động cảm nhận môi trường và trao đổi dữ liệu giữa các thiết bị. Các vật có thể được nhận dạng duy nhất và môi trường xung quanh có thể được giám sát cho nhiều mục đích và ứng dụng khác nhau. Mỗi đối tượng trong IoT đều có một danh tính kỹ thuật số và có thể dễ dàng theo dõi trong miền kỹ thuật số. Kỹ thuật gán danh tính duy nhất cho một đối tượng được gọi là định danh duy nhất toàn cầu (UUID). UUID là một số 128-bit được sử dụng để nhận dạng duy nhất một đối tượng hoặc thực thể trên Internet.

Khi xác định lớp cảm biến của IoT, cần xem xét các khía cạnh sau:

- *Chi phí, kích thước, tài nguyên và tiêu thụ năng lượng:* Các vật có thể được trang bị các thiết bị cảm biến như thẻ RFID, nút cảm biến. Do số lượng cảm biến lớn trong các ứng dụng, các thiết bị thông minh nên được thiết kế để giảm thiểu tài nguyên và chi phí cần thiết.
- *Triển khai:* Các vật cảm biến (thẻ RFID, cảm biến, v.v.) có thể được triển khai một lần, từng bước, hoặc ngẫu nhiên tùy theo yêu cầu.
- *Giao tiếp:* Các cảm biến phải có khả năng giao tiếp để làm cho các vật có thể truy cập và truy xuất được.
- *Mạng:* Các vật được tổ chức thành các mạng đa bước, lưới hoặc tự phát.

1.3.2 Lớp mạng

Lớp mạng trong IoT kết nối tất cả các vật và cho phép chúng nhận biết môi trường xung quanh. Thông qua lớp mạng, các vật có thể chia sẻ dữ liệu với các vật kết nối khác, điều này rất quan trọng cho việc quản lý và xử lý sự kiện thông minh trong IoT. Để chia sẻ dữ liệu và cung cấp dịch vụ, một mạng mạnh mẽ là cần thiết. Mạng cũng nên tự động phát hiện và ánh xạ các vật. Các vật cần được gán vai trò tự động để triển khai, quản lý và lập lịch hành vi của các vật và nên có khả năng chuyển đổi vai trò bất cứ lúc nào khi cần thiết. Điều này cho phép các thiết bị thực hiện các nhiệm vụ một cách hợp tác.

Trong lớp mạng, cần giải quyết các vấn đề sau:

- Công nghệ quản lý mạng: Bao gồm quản lý các mạng cố định, không dây, di động.
- Yêu cầu về QoS (Chất lượng dịch vụ).
- Công nghệ tìm kiếm và xử lý dữ liệu
- Bảo mật và quyền riêng tư

Trong số các vấn đề này, bảo mật thông tin và quyền riêng tư của con người là rất quan trọng vì IoT kết nối nhiều vật dụng cá nhân, mang lại nguy cơ tiềm ẩn liên quan đến quyền riêng tư. Các công nghệ bảo mật mạng hiện có có thể cung cấp nền tảng cho quyền riêng tư và bảo mật trong IoT, nhưng vẫn cần thực hiện nhiều công việc hơn.

1.3.3 Lớp dịch vụ

Lớp dịch vụ cho phép các dịch vụ và ứng dụng trong IoT. Đây là một nền tảng tiết kiệm chi phí, nơi phần mềm và phần cứng có thể được tái sử dụng. Các dịch vụ trong lớp dịch vụ chạy trực tiếp trên mạng để định vị hiệu quả các dịch vụ mới cho một ứng dụng và truy xuất dữ liệu động về các dịch vụ. Hầu hết các đặc tả được thực hiện bởi các tiêu chuẩn khác nhau do các tổ chức khác nhau phát triển. Một lớp dịch vụ được chấp nhận toàn cầu là quan trọng đối với IoT. Một lớp dịch vụ thực tế bao gồm một tập hợp tối thiểu các ứng dụng, giao diện lập trình ứng dụng (API), và các giao thức hỗ trợ các ứng dụng và dịch vụ cần thiết. Tất cả các hoạt động hướng dịch vụ, chẳng hạn như trao đổi và lưu trữ thông tin, quản lý dữ liệu, công cụ tìm kiếm và giao tiếp, đều được thực hiện tại lớp dịch vụ.

Các nhiệm vụ được thực hiện bởi lớp dịch vụ bao gồm:

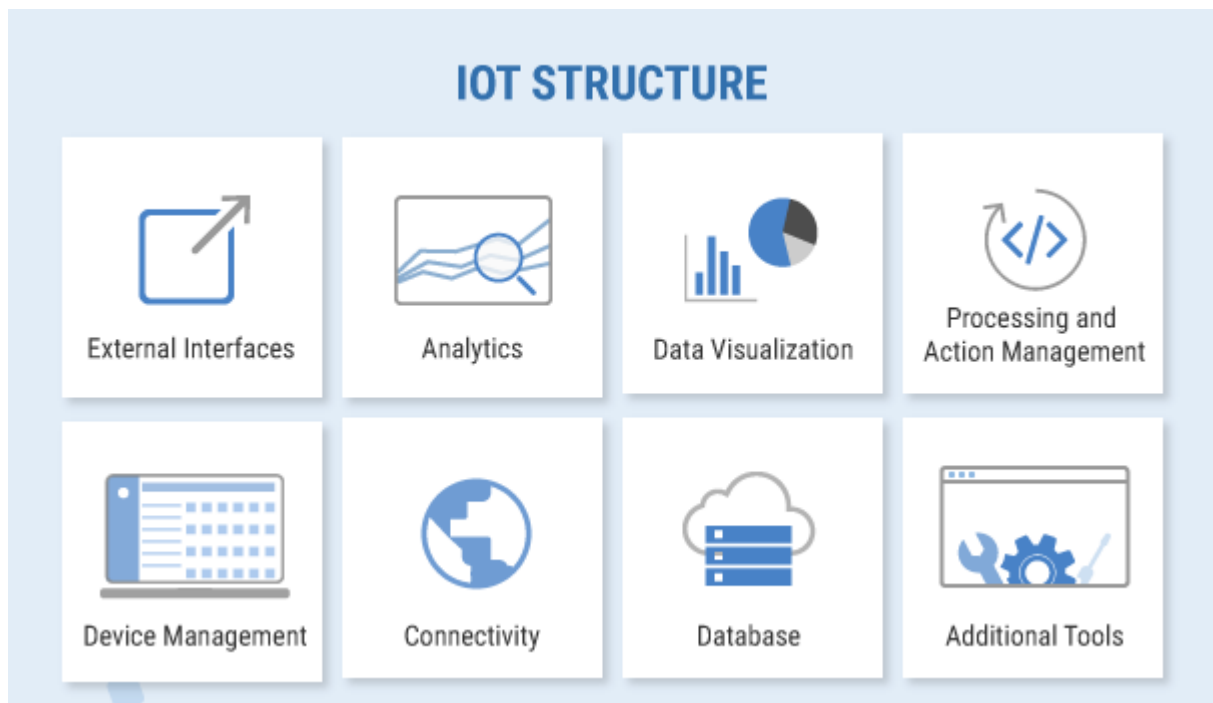
- *Khám phá dịch vụ*: Tìm các đối tượng có thể cung cấp dịch vụ và thông tin cần thiết một cách hiệu quả.
- *Thành phần dịch vụ*: Cho phép tương tác giữa các vật kết nối và mô tả mối quan hệ giữa các vật để cung cấp dịch vụ mong muốn.
- *API dịch vụ*: Cung cấp giao diện giữa các dịch vụ mà người dùng yêu cầu.

1.3.4 Lớp giao diện

Trong IoT, có một số lượng lớn các thiết bị được kết nối; các thiết bị này thuộc sở hữu của những người khác nhau và do đó không phải lúc nào cũng tuân theo cùng một tiêu chuẩn. Vấn đề tương thích giữa các vật cần phải được giải quyết để các vật có thể tương tác với nhau. Tính tương thích liên quan đến việc trao đổi thông tin, giao tiếp và xử lý sự kiện. Có một nhu cầu mạnh mẽ về một cơ chế giao diện hiệu quả để đơn giản hóa việc quản lý và kết nối các vật. Cơ bản là lớp giao diện hoạt động ở phần giao diện người dùng của ứng dụng hoặc API (Giao diện Chương trình Ứng dụng).

1.4 Các thành phần cơ bản của hệ thống IoT

Về kiến trúc chung của mô hình IoT phổ biến nhất hiện nay, được tạo từ 8 thành phần [20] sau đây:



Hình 1.2: Các thành phần cơ bản của mô hình IoT

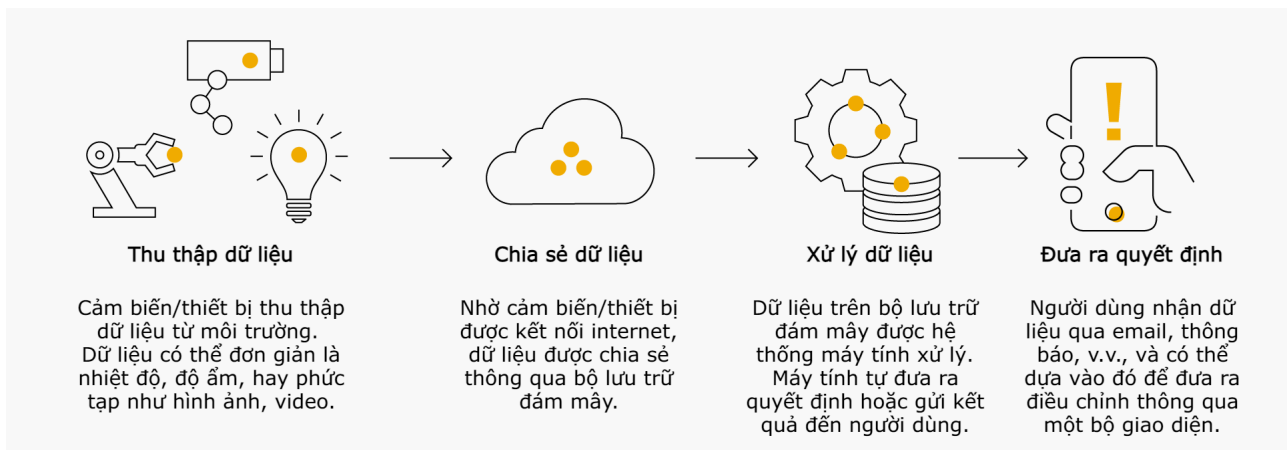
- **Kết nối và đồng bộ hóa:** Thành phần này có chức năng tích hợp đồng bộ các giao thức và các định dạng dữ liệu khác nhau vào một giao diện “phần mềm” đảm bảo việc truyền dữ liệu chính xác và tương tác với tất cả các thiết bị.
- **Quản lý thiết bị:** Đây là thành phần đảm bảo kết nối các thiết bị hoạt động bình thường, chạy các bản vá và cập nhật phần mềm cũng như ứng dụng đang chạy trên thiết bị hoặc các gateways ngoại biên (EDGE gateway).
- **Cơ sở dữ liệu:** Đây là thành phần được coi quan trọng của một nền tảng. Ngoài lưu trữ dữ liệu quan trọng của thiết bị, nó phải có khả năng mở rộng đáp ứng các yêu cầu cho các cơ sở dữ liệu dựa trên đám mây. Thành phần này phải có khả năng mở rộng khối lượng, đảm bảo sự đa dạng, vận tốc và độ tin cậy của dữ liệu.
- **Quản lý và xử lý hoạt động:** Chức năng đưa dữ liệu vào hoạt động dựa trên nguyên tắc Event-Action-Triggers cho phép thực thi các hoạt động “thông minh” dựa trên dữ liệu từ cảm biến cụ thể.
- **Phân tích:** Đây có thể được coi là bộ não của nền tảng IoT. Thành phần này có chức năng thực hiện hàng loạt các phân tích phức tạp từ việc phân

cụm dữ liệu cơ bản và khả năng tự học để tự phân tích, dự đoán, trích xuất những dữ liệu giá trị nhất trong luồng dữ liệu IoT.

- **Giao diện biểu diễn dữ liệu trực quan:** Cho phép con người xem xét các mẫu và quan sát các xu hướng từ bảng điều khiển trực quan, nơi dữ liệu được miêu tả sinh động qua biểu đồ đường thẳng, hình họa mô phỏng.
- **Công cụ bổ sung:** Thành phần này cho phép các nhà phát triển IoT thử nghiệm và trước khi đưa sản phẩm ra thị trường với các trường hợp sử dụng được biểu diễn trên hệ sinh thái mô phỏng dùng để hiển thị, quản lý và kiểm soát thiết bị kết nối.
- **Các giao thức kết nối với hệ thống khác bên ngoài:** Đây là nơi cho phép tích hợp với các hệ thống của bên thứ ba và phần còn lại của hệ thống CNTT như phần mềm quản trị nguồn lực doanh nghiệp ERP, hệ thống quản lý sản xuất MES thông qua các giao diện lập trình ứng dụng (API), các bộ phát triển phần mềm (SDK) và các gateways.

1.5 Nguyên lý hoạt động của IoT

Mọi hệ thống IoT hoàn chỉnh đều có 4 bước: Thu thập dữ liệu, chia sẻ dữ liệu, xử lý dữ liệu và đưa ra quyết định.



Hình 1.3: Sơ đồ nguyên lý hoạt động của hệ thống IoT

Hệ thống IoT bao gồm các thiết bị thông minh hỗ trợ web sử dụng hệ thống nhúng, như bộ xử lý, cảm biến và phần cứng truyền thông, để thu thập, gửi và xử lý trên dữ liệu mà chúng thu thập được. Các thiết bị IoT chia sẻ dữ liệu cảm biến thu thập được bằng cách kết nối với cổng IoT hoặc thiết bị biên khác, nơi dữ liệu được gửi đến đám mây để phân tích hoặc phân tích cục bộ.

1.6 Các đặc tính cơ bản của IoT

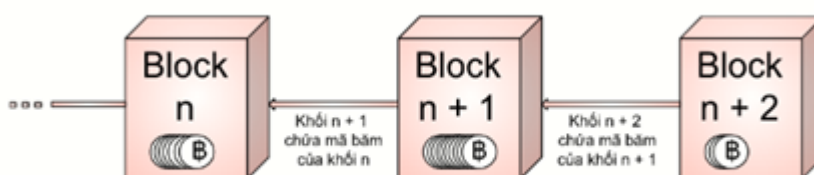
- **Tính kết nối liên thông (interconnectivity):** với IoT, bất cứ điều gì cũng có thể kết nối với nhau thông qua mạng lưới thông tin và cơ sở hạ tầng liên lạc tổng thể.
- **Những dịch vụ liên quan đến “Things”:** hệ thống IoT có khả năng cung cấp các dịch vụ liên quan đến “Things”, chẳng hạn như bảo vệ sự riêng tư và nhất quán giữa Physical Thing và Virtual Thing. Để cung cấp được dịch vụ này, cả công nghệ phần cứng và công nghệ thông tin(phần mềm) sẽ phải thay đổi.
- **Tính không đồng nhất:** Các thiết bị trong IoT là không đồng nhất vì nó có phần cứng khác nhau, và network khác nhau. Các thiết bị giữa các network có thể tương tác với nhau nhờ vào sự liên kết của các network.
- **Thay đổi linh hoạt:** Status của các thiết bị tự động thay đổi, ví dụ, ngủ và thức dậy, kết nối hoặc bị ngắt, vị trí thiết bị đã thay đổi, và tốc độ đã thay đổi... Hơn nữa, số lượng thiết bị có thể tự động thay đổi.
- **Quy mô lớn:** Sẽ có một số lượng rất lớn các thiết bị được quản lý và giao tiếp với nhau. Số lượng này lớn hơn nhiều so với số lượng máy tính kết nối Internet hiện nay. Số lượng các thông tin được truyền bởi thiết bị sẽ lớn hơn nhiều so với được truyền bởi con người.

Chương 2

Tổng quan về công nghệ Blockchain

2.1 Công nghệ Blockchain

Blockchain hay **Chain of blocks** (chuỗi các khối), một cách đơn giản, có thể hình dung đây là một chuỗi các bản ghi (một khối) không thể chỉnh sửa gắn kết với một tem thời gian được quản lý bởi một chuỗi các máy tính (không thuộc sở hữu của một thực thể đơn lẻ) [18].



Hình 2.1: Cấu trúc dữ liệu của một chuỗi khối

Công nghệ Blockchain là một cơ chế cơ sở dữ liệu tiên tiến cho phép chia sẻ thông tin minh bạch trong một mạng lưới kinh doanh. Mỗi khối (block) đều chứa thông tin về thời gian khởi tạo và được liên kết với khối trước đó, kèm theo đó là một mã thời gian và dữ liệu giao dịch. Dữ liệu khi đã được mạng lưới chấp nhận thì sẽ không có cách nào thay đổi được. Blockchain được thiết kế để chống lại việc gian lận, thay đổi của dữ liệu .

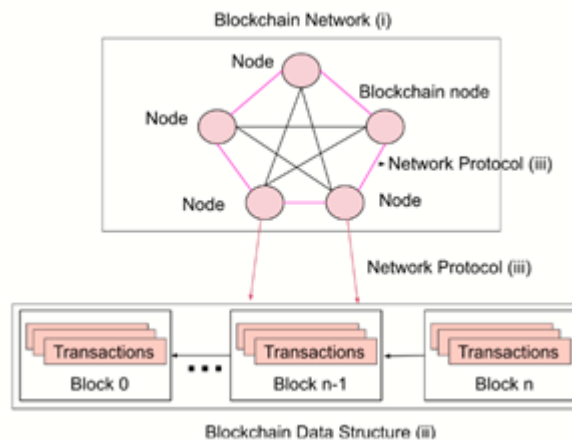
Do đó, ta có thể sử dụng công nghệ chuỗi khối để tạo một sổ cấu trúc không thể chỉnh sửa hay biến đổi để theo dõi các đơn đặt hàng, khoản thanh toán, tài khoản và những giao dịch khác. Hệ thống có những cơ chế tích hợp để ngăn

chặn các mục nhập giao dịch trái phép và tạo ra sự nhất quán trong chế độ xem chung của các giao dịch này.

2.2 Hệ thống chuỗi khối (Blockchain system)

Một hệ thống chuỗi khối bao gồm [7]:

- **Mạng lưới chuỗi khối:** Đây là hệ thống các nút trong chuỗi khối. Mỗi nút là một máy tính hoặc thiết bị kết nối với mạng và tham gia vào việc xác minh và xây dựng chuỗi khối. Các nút này liên lạc với nhau qua giao thức mạng để chia sẻ thông tin và đạt được sự đồng thuận về trạng thái của chuỗi khối.
- **Cấu trúc dữ liệu chuỗi khối:** Sổ cái phân tán không thể thay đổi được sao chép và lưu trữ trên toàn bộ mạng lưới blockchain. Các nút trong mạng được cấu hình để chứa một bản sao đầy đủ của sổ cái, gọi là các nút đầy đủ (full nodes).
- **Giao thức mạng:** Giao thức mạng đặt ra các quy tắc và trách nhiệm của các nút trong mạng lưới. Nó xác định cách các nút liên lạc, truyền tải thông tin và thực hiện các hoạt động như xác minh, xác thực và đạt được sự đồng thuận. Điều này đảm bảo việc ủy quyền và xác thực các giao dịch mới, cơ chế thêm các khối mới vào chuỗi khối và các cơ chế khuyến khích.

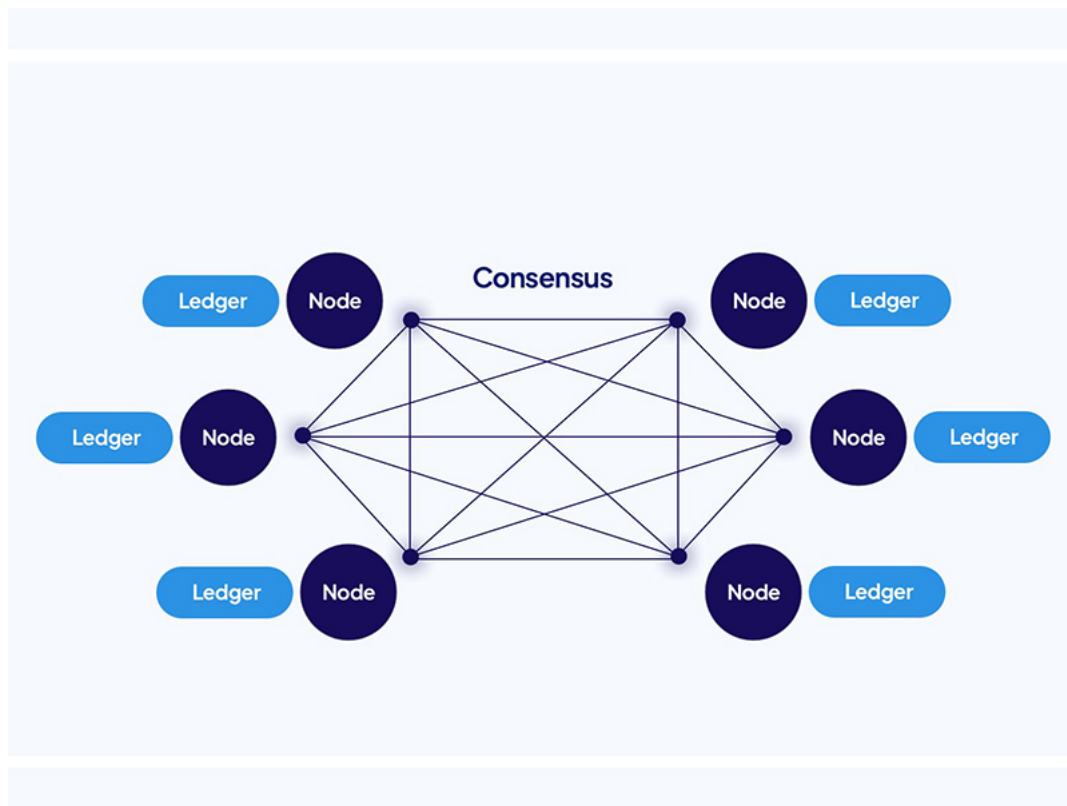


Hình 2.2: Sơ đồ cấu trúc một hệ thống chuỗi khối

2.3 Sổ cái phân tán (Distributed ledger)

Công nghệ sổ cái phân tán (Distributed ledger technology - DLT) [17] là một hệ thống lưu trữ dữ liệu phi tập trung. Trong đó, các thông tin cũng như bản ghi được phân phối trên nhiều máy chủ hoặc nút mạng khác nhau. Nó cho phép người dùng truy cập đồng thời, xác thực và cập nhật bản ghi trên một cơ sở dữ liệu có kết nối mạng.

DLT cho phép lưu trữ thông tin một cách bảo mật hơn, chính xác hơn bằng tiền mã hóa. Dữ liệu được truy cập bởi “chìa khóa” và chữ ký crypto. Một khi thông tin được lưu trữ, nó sẽ trở thành cơ sở dữ liệu cố định, không thể thay đổi. Trong đó, các quy tắc của mạng lưới bên trong nó sẽ được lập trình nhằm quản trị sổ cái đó.



Hình 2.3: Cơ chế hoạt động của công nghệ sổ cái phân tán

Chỉ cần một thông tin không thể thay đổi thì dữ liệu khi cùng nó sẽ bất biến. Sổ cái phân tán chỉ bất biến khi chúng được lập trình theo cách này. Còn đối với công nghệ blockchain, toàn bộ dữ liệu đều không thể thay đổi nên nó còn có một cách gọi khác là sổ cái tập trung - ngược lại với sổ cái phân tán.

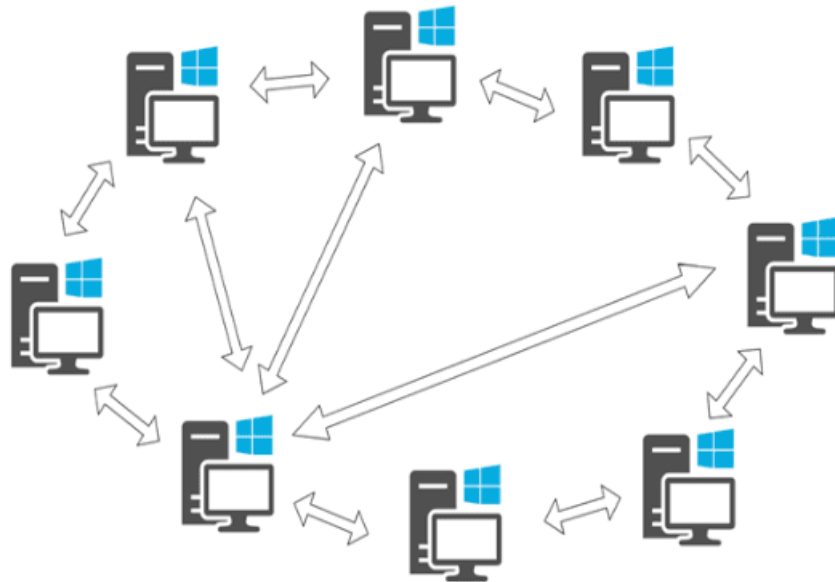
Sổ cái phân tán cho phép các nút bên trong mạng lưới trao đổi và chia sẻ dữ

liệu một cách an toàn và minh bạch. Với việc dữ liệu được phân tán trên nhiều máy tính, nó tăng tính bảo mật và khả năng chống lại các cuộc tấn công từ một điểm duy nhất. Ngoài ra, tính phân tán cũng tạo ra tính toàn vẹn và khả năng chịu lỗi cao hơn, vì một lỗi ở một nút mạng không làm ảnh hưởng đến hoạt động của toàn bộ hệ thống.

2.4 Mạng ngang hàng và giao thức đồng thuận

2.4.1 Mạng ngang hàng (Peer-to-Peer Network)

Mạng ngang hàng hay Peer-to-Peer (P2P) [22] là một hệ thống máy tính kết nối với nhau thông qua Internet, và chia sẻ dữ liệu mà không cần máy chủ trung tâm. Các mạng máy tính ngang hàng sử dụng cấu trúc phân tán (phi tập trung). Nói theo cách khác, mạng P2P không có phân biệt máy chủ (server) và máy khách (client).



Hình 2.4: Cấu trúc mạng ngang hàng

Cơ chế hoạt động

Mạng ngang hàng không có máy chủ (server) và máy khách (client). Thay vào đó mỗi nút giữ một bản sao của các tệp, đóng vai trò là máy khách và máy

chủ cho các nút khác. Vậy về bản chất, mạng ngang hàng được duy trì bởi một mạng lưới người dùng phân tán.

Trên mạng P2P, các thiết bị sử dụng các ứng dụng phần mềm được thiết kế để làm trung gian cho việc chia sẻ dữ liệu. Khi muốn tìm và tải các tệp, người dùng có thể gửi yêu cầu tìm kiếm đến các thiết bị khác trên mạng. Và khi đã tải xuống một tệp, họ có thể đóng vai trò là nguồn của tệp đó.

Nói theo một cách khác, thì khi tải xuống một tệp từ nút A, thì nút B sẽ đóng vai trò như máy khách. Còn khi nút A tải xuống một tệp từ nút B thì nút B sẽ đóng vai trò là máy chủ.

Vai trò của P2P trong Blockchain

Cấu trúc mạng ngang hàng (P2P) trong Blockchain là yếu tố giúp cho việc giao dịch các loại tiền điện tử không cần phải thông qua bên trung gian.

Vì vậy, không có ngân hàng nào hoặc máy chủ trung tâm nào có thể kiểm soát các giao dịch. Thay vào đó là sử dụng một sổ cái gọi là Blockchain để ghi lại công khai tất cả các giao dịch.

Bên cạnh đó, các nút sẽ đảm nhận các vai trò khác nhau. Ví dụ, các nút đầy đủ (full node) giúp duy trì bảo mật mạng. Điều này được thực hiện thông qua việc xác minh các giao dịch theo các quy tắc đồng thuận.

2.4.2 Giao thức đồng thuận

Giao thức đồng thuận là 1 tập hợp các quy tắc, phương pháp để các máy tính trong mạng lưới cần tuân theo, để từ đó đạt được sự đồng thuận trên toàn mạng lưới. Các node không tuân theo sẽ tự bị đào thải nếu dữ liệu nó gửi đến node khác không hợp lệ.

Trong blockchain, có rất nhiều loại giao thức đồng thuận khác nhau được đưa vào sử dụng. Các giao thức phổ biến có thể kể đến:

- Mô hình đồng thuận bằng chứng công việc.
- Mô hình đồng thuận bằng chứng cổ phần.
- Mô hình đồng thuận bằng chứng thời gian đã trôi qua.

2.5 Hàm băm

2.5.1 Hàm băm mật mã học (Cryptographic hash function)

Hàm băm là các thuật toán không sử dụng khóa để mã hóa, nó có nhiệm vụ băm thông điệp được đưa vào theo một thuật toán hàm một chiều nào đó, rồi đưa ra một bản băm – văn bản đại diện – có kích thước cố định. Do đó người nhận không biết được nội dung hay độ dài ban đầu của thông điệp đã được băm bằng hàm băm.

Giá trị của hàm băm là duy nhất, và không thể suy ngược lại được nội dung thông điệp từ giá trị băm này.

Một hàm băm được mô tả theo cấu trúc sau:

$$h : M \rightarrow \{0, 1\}^n, h(m) = \tilde{m}$$

Trong đó:

- m : một dữ liệu cho trước có kích thước bất kì
- M : dãy kí tự biểu diễn tóm tắt của m
- n : kích thước được cung cấp

Tính chất của hàm băm

1. Tính chống tiền ảnh (Preimage resistant - one-way property):
Cho trước giá trị băm h việc tìm x sao cho $H(x) = h$ là rất khó
2. Tính chống tiền ảnh thứ hai (Second preimage resistant - weak collision resistant - Tính chống trùng yếu):
Cho thông điệp đầu vào x , việc tìm một thông điệp x' với ($x' \neq x$) sao cho $h(x') = h(x)$ là rất khó
3. Tính chống trùng mạnh (Strong Collision resistant):
Không thể tính toán để tìm được hai thông điệp đầu vào $x_1 \neq x_2$ sao cho chúng có cùng giá trị băm (Nghịch lý ngày sinh – Birthday paradox)

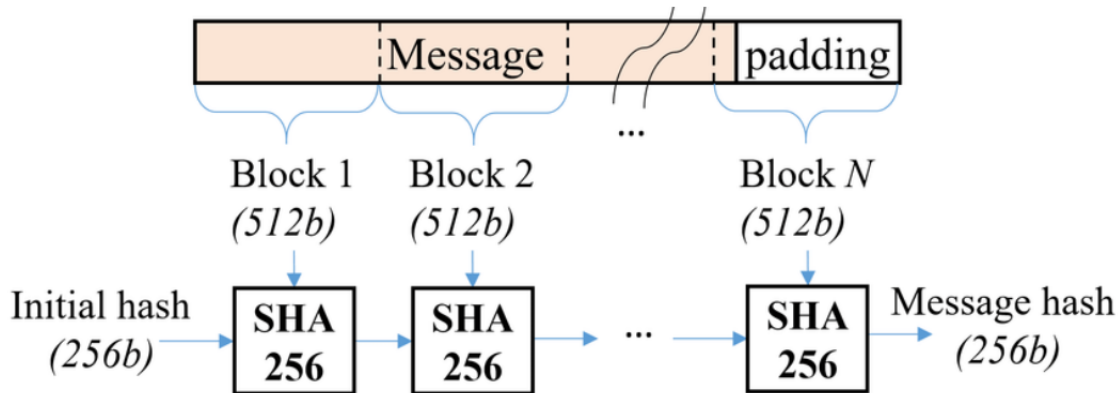
2.5.2 Hàm băm SHA-256

Trong kỹ thuật số, chúng ta sử dụng "dấu vân tay" được biểu diễn dưới dạng giá trị mật mã băm, cụ thể là giá trị băm được sinh ra bởi thuật toán SHA-256.

Họ SHA-2 là một tập hợp các hàm băm mật mã được thiết kế và công bố bởi

Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) vào năm 2002. SHA-2 bao gồm những thay đổi đáng kể so với tiền nhiệm của nó SHA-1 và vẫn đang là một trong những hàm băm mạnh nhất được sử dụng ngày nay. Họ SHA-2 sử dụng các phép tính logic, phép xoay và phép trộn bit để xử lý dữ liệu đầu vào và tính toán giá trị băm tương ứng.

Thuật toán SHA-256 [16] được phát triển bởi NSA (Cơ quan An ninh quốc gia Mỹ). SHA-256 là một hàm băm đại diện cho họ SHA-2. Nó tính toán giá trị băm 256 bit cho một dữ liệu đầu vào tối đa là $2^{64} - 1$ bit.



Hình 2.5: Tính toán hàm băm cho dữ liệu đầu vào có kích thước lớn

Tổng quan các bước xử lý của thuật toán SHA-256 bao gồm hai quy trình: message expander (ME) và message compressor (MC).

Thuật toán này rất an toàn và được nhiều nơi trên thế giới sử dụng nó để lưu trữ mật khẩu, kiểm tra các tài liệu kỹ thuật số. Trên thực tế, trong Blockchain, nó cũng đã được áp dụng và đóng vai trò là một trong những thành phần cốt lõi của chuỗi khối. Điều quan trọng là thuật toán này được áp dụng không chỉ cho tập tài liệu hoặc văn bản, mà nó còn được áp dụng cho bất kỳ tài liệu kỹ thuật số nào. Vì vậy, ta có thể đưa một đoạn video, một văn bản, âm thanh, một tệp lệnh vào trong thuật toán, nó sẽ trả về một giá trị đặc biệt và duy nhất cho từng đối tượng dữ liệu.

2.6 Đặc tính của Blockchain

2.6.1 Tính phi tập trung

Công nghệ phi tập trung cung cấp cho bạn khả năng lưu trữ tài sản (như các hợp đồng, tài liệu,...) vào trong hệ thống thông qua Internet. Chủ sở hữu

sẽ có quyền kiểm soát trực tiếp hệ thống và chuyển giao tài sản của mình sang bất kỳ một người nào khác thông qua một chiếc chìa khóa riêng (chìa khóa ảo).

Công nghệ Blockchain đã và đang chứng minh được khả năng của mình trong công cuộc phi tập trung hóa các trang web và sở hữu sức mạnh đem lại thay đổi to lớn cho tất cả các nền công nghiệp.

2.6.2 Tính bảo mật

Dữ liệu trên mạng lưới Blockchain gần như không thể bị sửa đổi, bởi vì mỗi khối trong Blockchain có thể được truy ngược về khối đầu tiên của mạng. Thường khi xảy ra các hoạt động lừa đảo, việc tìm ra dấu vết gian lận là rất khó và tốn nhiều thời gian. Lịch sử dữ liệu có thể bị thay đổi đến mức không thể phát hiện các giao dịch và hoạt động lừa đảo.

2.6.3 Tính ổn định

Tạo dựng một nền tảng sổ cái (ledgers) ổn định là mục tiêu cốt lõi của Blockchain. Bất kỳ nền tảng tập trung nào đều cũng có thể dễ dàng bị xâm nhập bởi các hacker và đòi hỏi sự tin tưởng từ bên thứ ba. Tuy nhiên, hệ thống Blockchain như Bitcoin luôn giữ cho dữ liệu sổ cái của mình trong trạng thái luôn được chuyển tiếp ổn định.

Chúng ta sẽ luôn cần đạt được sự đồng thuận giữa các miners (người dùng Bitcoin), exchange (giao dịch) và nodes operator (nút toán tử) trong Bitcoin để có thể thay đổi được dữ liệu của Blockchain.

2.6.4 Tính khắc phục

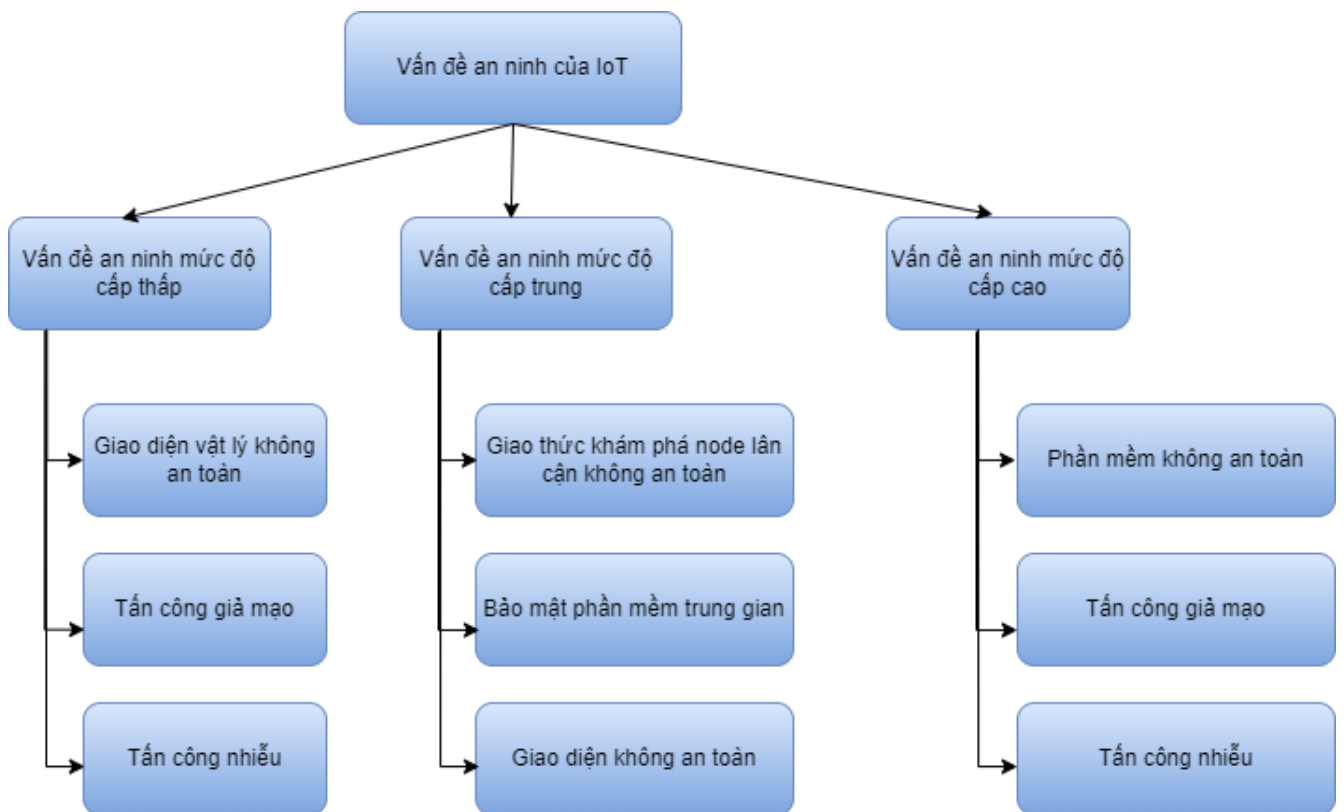
Nhờ có công nghệ của Blockchain, chúng ta sẽ có thể giải quyết được những vấn đề rắc rối liên quan đến việc gian lận. Đặc biệt, ở những quốc gia nơi mà sự tin tưởng của người dùng đối với các tính năng công nghệ vẫn còn thấp - sẽ là “vùng đất hy vọng” cho sự phát triển của phần mềm Blockchain.

Chương 3

Hệ bảo mật của hệ thống IoT

Các vấn đề bảo mật của IoT có thể được phân loại thành ba loại [12] :

1. Vấn đề bảo mật cấp thấp (Low-level security issues)
2. Vấn đề bảo mật cấp trung (Intermediate-level security issues)
3. Vấn đề bảo mật cấp cao (High-level security issues)



Hình 3.1: Phân loại các vấn đề bảo mật cho IoT

3.1 Vấn đề bảo mật cấp thấp

- Giao diện vật lý không an toàn (Insecure Physical Interface): Các thiết bị IoT thường có các giao diện vật lý như cổng USB, GPIO, và các giao diện không dây. Những giao diện này có thể dễ dàng bị tấn công nếu không được bảo mật đúng cách, chẳng hạn như bị truy cập trái phép hoặc bị can thiệp [14].
- Tấn công giả mạo (Spoofing Attacks) [11]: Kẻ tấn công có thể giả mạo thiết bị IoT để truy cập vào mạng hoặc dữ liệu nhạy cảm. Điều này có thể dẫn đến việc truy cập trái phép, làm gián đoạn dịch vụ hoặc đánh cắp thông tin.
- Gây nhiễu (Jamming Adversaries) [24]: Các thiết bị IoT sử dụng sóng vô tuyến để giao tiếp có thể bị gây nhiễu bởi các thiết bị khác, làm gián đoạn giao tiếp và ảnh hưởng đến hoạt động của hệ thống.

3.2 Vấn đề bảo mật cấp trung

- Khám phá láng giềng không an toàn (Insecure Neighbor Discovery): Trong mạng IoT, các thiết bị cần phát hiện và giao tiếp với các thiết bị lân cận. Nếu quá trình này không được bảo mật, kẻ tấn công có thể chen vào mạng các thiết bị giả mạo để thu thập thông tin hoặc gây rối loạn hệ thống.
- Tấn công đặt chỗ bộ đệm (Buffer Reservation Attack) [8]: Kẻ tấn công có thể gửi một lượng lớn yêu cầu để chiếm dụng bộ đệm của các thiết bị IoT, gây ra tình trạng từ chối dịch vụ hoặc làm giảm hiệu suất của hệ thống.
- Tấn công Sybil (Sybil Attacks) [13]: Kẻ tấn công tạo ra nhiều danh tính giả để chiếm quyền kiểm soát một phần lớn của mạng IoT, gây ra các vấn đề về bảo mật và sự tin cậy.

3.3 Vấn đề bảo mật cấp cao

- Phần mềm không an toàn (Insecure Software): Các ứng dụng và phần mềm chạy trên thiết bị IoT có thể chứa các lỗ hổng bảo mật. Những lỗ hổng này có thể bị khai thác để thực hiện các cuộc tấn công như chiếm quyền điều khiển, đánh cắp dữ liệu hoặc phá hoại hệ thống.

- Bảo mật phần mềm trung gian (Middleware Security): Phần mềm trung gian kết nối các thiết bị IoT với nhau và với các dịch vụ mạng khác cần được bảo mật để ngăn chặn các cuộc tấn công như truy cập trái phép hoặc giả mạo dữ liệu.
- Giao diện không an toàn (Insecure Interface): Các giao diện giữa thiết bị IoT và người dùng hoặc các hệ thống khác có thể thiếu các biện pháp bảo mật, dẫn đến nguy cơ bị tấn công và làm giảm độ tin cậy của hệ thống.

Chương 4

Blockchain trong hệ thống IoT

4.1 Tổng quan về công nghệ Blockchain trong IoT

Blockchain có thể cải thiện IoT bằng cách cung cấp dịch vụ an toàn, nơi dữ liệu đáng tin cậy và có thể truy cập được [12].

Dữ liệu được lưu trữ không thay đổi theo thời gian, giúp tăng cường tính bảo mật của nó. Vị trí của dữ liệu luôn được biết rõ ràng.

Các tương tác giữa Blockchain và IoT có thể được phân loại thành ba loại:

1. **IoT-IoT:** Thiết lập tương tác giữa các thiết bị IoT với nhau.
2. **IoT-Blockchain:** Cho phép các thiết bị IoT giao tiếp với mạng Blockchain.
3. **Hybrid approach:** Kết hợp giữa IoT-IoT và IoT-Blockchain

Hình dưới đây minh họa Tổng quan về ứng dụng Blockchain trong IoT.

Hệ sinh thái Internet of Things (IoT) hiện đại dựa vào các **mô hình tập trung**, còn được gọi là mô hình máy khách/máy chủ (client/server).

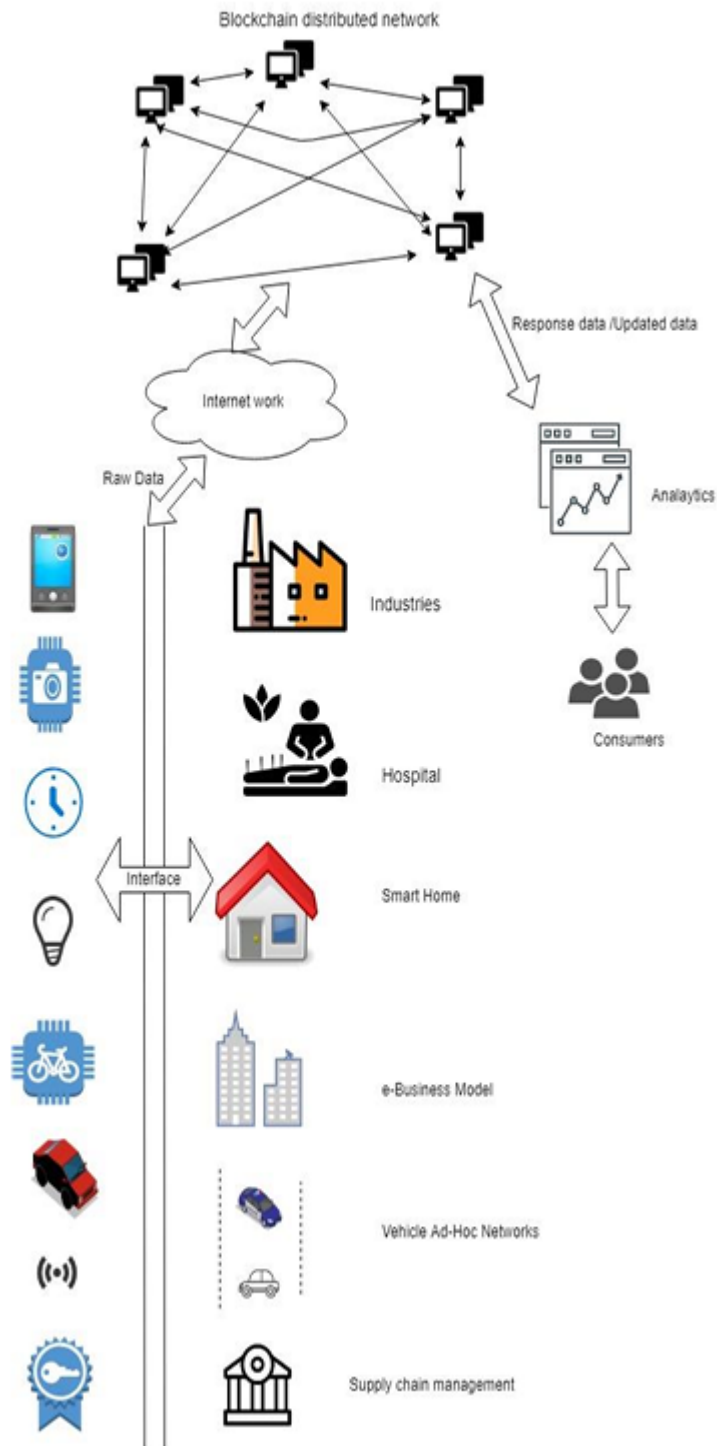
Tất cả các thiết bị đều được nhận dạng, xác thực và tham gia thông qua các máy chủ có dung lượng lưu trữ và sức mạnh xử lý khổng lồ.

Điểm yếu của mô hình IoT hiện tại là rủi ro hỏng hóc một điểm (single point of failure). Nghĩa là nếu máy chủ trung tâm gặp sự cố, toàn bộ hệ thống có thể bị ảnh hưởng [12].

-> Để giải quyết vấn đề này, mô hình IoT được tích hợp với công nghệ Blockchain.

Công nghệ Blockchain sử dụng phương thức **phi tập trung (decentralized)** cho mạng lưới IoT.

Điều này có nghĩa là không có một máy chủ trung tâm nào kiểm soát mọi thứ, thay vào đó, dữ liệu được phân tán trên nhiều nút (node) khác nhau trong mạng.



Hình 4.1: Tổng quan về ứng dụng Blockchain trong IoT

Ý nghĩa của mô hình ngang hàng (peer-to-peer model) trong IoT với Blockchain [12] :

- Việc áp dụng mô hình giao tiếp ngang hàng (peer-to-peer) để xử lý hàng triệu hoặc hàng tỷ giao dịch giữa các thiết bị sẽ **giảm đáng kể chi phí** liên quan đến việc xây dựng và duy trì các trung tâm dữ liệu lớn tập trung.
- Mô hình này **ngăn chặn sự cố ở một nút riêng lẻ** trong mạng làm tê liệt toàn bộ mạng (single point of failure).

Vai trò của các thành phần trong hệ thống:

- Thiết bị IoT: Sinh ra một lượng lớn dữ liệu và cần sức mạnh tính toán theo thời gian thực.
- Nút giao diện (interface node): Có khả năng tính toán thấp, thực hiện xử lý sơ bộ dữ liệu thô do thiết bị người dùng cuối tải lên để lọc dữ liệu và thu thập thông tin có giá trị.
- Raw data: Được truyền đến mạng phân tán blockchain để xử lý hoặc cập nhật.
- Nút đào (miner node): Kiểm tra khối dữ liệu thô trong mạng phân tán blockchain. Nếu khối hợp lệ, dữ liệu sẽ được cập nhật trong mạng blockchain phân tán.
- Consumers: Truy cập dữ liệu có sẵn trong mạng phân tán bằng cách sử dụng các thiết bị phân tích hoặc phần mềm.

| Blockchain | IoT |
|--|---|
| Tiêu tốn tài nguyên | Hầu hết các thiết bị có nguồn lực hạn chế |
| Quá trình đào block phức tạp | Tính toán phức tạp |
| Hệ thống BC bị hạn chế với mạng lưới lớn | IoT chứa một số lượng lớn các nút |
| Blockchain tiêu tốn nhiều băng thông | Băng thông và tài nguyên hạn chế |

Mặc dù việc sử dụng Blockchain (BC) trong lĩnh vực IoT (Internet of Things) còn tương đối mới mẻ, nhưng đã có một số lượng lớn các ứng dụng hiện hữu. BC được áp dụng theo những cách thức độc đáo để cải thiện công nghệ IoT.

4.1.1 Lợi ích của việc hợp nhất IoT và Blockchain

Việc xây dựng các ứng dụng IoT dựa trên nền tảng Blockchain mang lại một số lợi ích rõ ràng [6]:

1. Cải thiện tính bảo mật:

- Các ứng dụng IoT có thể trao đổi thông tin giữa nhiều hệ thống khác nhau do các công ty hoặc chính phủ khác nhau sở hữu và quản lý, điều này gây ra các vấn đề về bảo mật.
- Bản ghi Blockchain vốn dĩ đơn giản - bất kỳ ai được phép giao tiếp với hệ thống đều có thể theo dõi và phân tích các hoạt động.

2. Tính toàn vẹn của dữ liệu: Với Blockchain (lúc này sẽ được nắm giữ bởi các thiết bị), không có con người nào có khả năng ghi đè lên bản ghi bằng dữ liệu sai.

3. Nâng cao tính bảo mật cho dữ liệu nhạy cảm của IoT:

- Một phần đáng kể thông tin do IoT tạo ra có tính chất cá nhân

Ví dụ, các thiết bị gia đình thông minh thu thập thông tin chi tiết về cuộc sống và lịch trình hàng ngày của chúng ta. Đây là thông tin cần được chia sẻ với các thiết bị và dịch vụ khác để có giá trị đối với chúng ta. Tuy nhiên, điều đó cũng có nghĩa là có nhiều lỗ hổng hơn để kẻ tấn công có thể khai thác.

Doanh nghiệp và chính phủ đầu tư vào IoT cũng cần phải chiến đấu với nguy cơ gia tăng về việc bị tin tặc, đối thủ cạnh tranh hoặc kẻ thù bên ngoài đánh cắp thông tin.

Cho phép kiểm soát quyền truy cập vào thông tin từ các thiết bị IoT thông qua Blockchain sẽ tạo thêm một lớp bảo mật mà mọi kẻ tấn công trực tuyến đều phải vượt qua - lớp bảo mật được neo giữ bởi các giao thức mã hóa mạnh mẽ nhất hiện có.

Những thách thức đối với việc áp dụng Blockchain trong IoT:

Các giao thức đồng thuận hiện được sử dụng như PoW (Proof of Work), PoS (Proof of Stake) và giao thức đồng thuận dựa trên biểu quyết không phù hợp với môi trường IoT vì chúng có ít sức mạnh xử lý hơn. Nếu cố gắng sử dụng các giao thức đồng thuận nêu trên trong môi trường IoT, nó sẽ dẫn đến việc giao dịch bị trễ và không phù hợp với môi trường IoT thời gian thực. Hầu hết các thiết bị IoT đều được sử dụng trong máy chủ đám mây trung tâm.

4.1.2 Nền tảng Blockchain cho Công nghiệp Internet of Things (BPI-IoT)

1. Nền tảng Blockchain cho Công nghiệp Internet of Things (BPIIoT) có thể cải thiện hoạt động của sản xuất trên nền tảng đám mây (CBM) bằng cách cung cấp một mạng ngang hàng phi tập trung và đáng tin cậy cho môi trường sản xuất.

CBM là một nguyên mẫu công nghiệp hướng đến dịch vụ. Người dùng sử dụng các dịch vụ để cấu hình các thiết bị sản xuất theo nhu cầu của họ bằng cách sử dụng mô hình CBM.

2. BPIIoT [10] dựa trên mạng BC (Blockchain) nơi các hợp đồng thông minh được triển khai.

Hợp đồng thông minh hoạt động như các thỏa thuận giữa người mua dịch vụ và các thiết bị sản xuất để cung cấp dịch vụ sản xuất theo yêu cầu.

3. BPIIoT cho phép kết hợp các máy móc cũ trên xưởng sản xuất vào môi trường đám mây và cho phép củng cố phần mềm sản xuất ngang hàng và phi tập trung.

Các thành phần IoT sản xuất trong ngành có thể truy cập vào các dịch vụ phân phối điều khiển để tạo ra sản phẩm hoàn chỉnh tại thời điểm đó, cần thiết lập lòng tin giữa các thành phần IoT sản xuất và các dịch vụ phân phối điều khiển. Để giải quyết vấn đề này, việc tích hợp công nghệ BC với các thiết bị IoT là một quá trình phức tạp trong BPIIoT

4.1.3 Chăm sóc sức khỏe thông minh trong IoT với Blockchain

Chăm sóc sức khỏe thông minh sẽ là ứng dụng IoT hàng đầu. Các ứng dụng và dịch vụ chăm sóc sức khỏe thông minh có thể thực hiện theo dõi và kích hoạt theo thời gian thực cho các nhu cầu chăm sóc sức khỏe của bệnh nhân và sử dụng phân tích dữ liệu trên đám mây để cải thiện chất lượng chăm sóc sức khỏe và trải nghiệm cho bệnh nhân đồng thời giảm chi phí cung cấp dịch vụ chăm sóc sức khỏe [23].

Bảo mật trong chăm sóc sức khỏe thông minh bao gồm nhiều tính năng dựa trên tính toàn vẹn của Hồ sơ sức khỏe được lưu trữ tại bệnh viện

4.1.4 Thành phố thông minh dựa trên Blockchain (BC)

- Thành phố thông minh [21] sử dụng các thiết bị IoT thông minh để thu thập dữ liệu.

- Lượng dữ liệu khổng lồ này được tạo ra từ nhiều nguồn khác nhau.
- BC có thể giúp phân chia mạng lưới thành phố thông minh (SC) thành hai nhóm riêng biệt: mạng lõi và mạng biên (sử dụng công nghệ BC)
 1. Mạng lõi có các nút khai thác (miner node) với sức mạnh tính toán và dung lượng lớn, trong khi các thiết bị có dung lượng và sức mạnh xử lý hạn chế. Các nút khai thác cạnh tranh để tạo ra các khối (block) và xác minh bằng chứng công việc (PoW).
- Mỗi nút được cấp quyền truy cập vào bộ điều khiển SDN (Software-Defined Networking) để mang lại tính linh hoạt và bảo mật cao, giảm chi phí quản lý thiết bị và đơn giản hóa việc triển khai hệ thống tổ chức thành phố thông minh.
- Trong một thành phố thông minh dựa trên BC, mỗi nút hoạt động như một máy chủ trung tâm cho một khung mở cụ thể để cung cấp các dịch vụ ban đầu và đạt được các hạn chế.
- Nó lưu trữ các phương pháp và quyền truy cập của các thực thể được đăng ký riêng tư trong cơ sở dữ liệu của nó, đồng thời đạt được độ trễ thấp và giảm dung lượng truyền băng thông.
- Bản chất phân tán của BC có thể làm cho toàn bộ hoạt động linh hoạt hơn và hạn chế tác động của các cuộc tấn công ngay cả khi một nút bị tấn công. Tuy nhiên, nếu một nút bị hack, thiệt hại phải được giới hạn trong khu vực địa phương.

Những thách thức:

- Giảm thiểu độ trễ (latency).
- Giảm thiểu việc sử dụng băng thông.
- Cải thiện bảo mật, quyền riêng tư và khả năng mở rộng.

4.1.5 Nhà thông minh dựa trên Blockchain (BC)

Khác biệt so với nhà thông minh IoT thông thường:

- Nhà thông minh dựa trên BC [4] có tiêu chuẩn thiết kế riêng, bao gồm một ACL (Access Control List - Danh sách kiểm soát truy cập) cho phép chủ sở hữu kiểm soát tất cả các hoạt động diễn ra trong nhà.

- Miner cấp phát khóa (chia sẻ - shared key) giữa các thiết bị tương ứng theo chính sách do chủ sở hữu đặt ra trong giao tiếp giữa các thiết bị.
- Hệ thống nhà thông minh dựa trên BC cung cấp quyền truy cập được kiểm soát vào thông tin IoT. Ngoài ra, nó còn bảo vệ tính toàn vẹn, tính sẵn có và tính bảo mật của tin nhắn cùng với khả năng chống lại các cuộc tấn công DDoS (Distributed Denial-of-Service).

Mục tiêu chính:

- Giải quyết các vấn đề của BC như tài nguyên tính toán, độ trễ và sử dụng năng lượng bằng cách không sử dụng Proof of Work (Bằng chứng công việc) trong khai thác khối.
- Để giảm chi phí sức mạnh xử lý (bao gồm cả năng lượng), mỗi khối được khai thác mà không cần thuật toán bổ sung.
- Giảm độ trễ trong xác thực khối bằng cách loại bỏ các giao dịch không được khai thác vào khối.
- Mô hình chuỗi khối dựa trên hypergraph phù hợp với nhà thông minh và có thể hỗ trợ duy trì các yêu cầu bảo mật và bảo vệ quyền riêng tư.

Hạn chế:

- **Điểm lỗi đơn (SPF - Single Point of Failure):** Mặc dù bản chất của BC là hệ thống phi tập trung, nhưng trong mô hình này, Home-Miner (Máy đào gia đình), Cluster Heads (Các đầu nhóm) và lưu trữ đám mây lại là các SPF ở các lớp riêng biệt.
- **Quyết định tập trung:** Hầu hết các nguyên tắc BC yêu cầu tất cả các nút trong mạng phải đồng ý về các giao dịch và khối. Tuy nhiên, trong trường hợp này, Cluster Heads lại có trách nhiệm quyết định giữ lại một khối hay từ chối nó.
- **Bảo mật bằng Proof of Work (PoW):** Chỉ có Home Miner đào khối mà không cần Proof of Work, trong khi PoW đóng vai trò quan trọng trong việc bảo vệ BC chống lại chi tiêu trùng lặp và gian lận thông tin.

4.1.6 Mô hình thương mại điện tử (eBusiness) IoT sử dụng Blockchain

Cải thiện doanh thu doanh nghiệp:

- Sử dụng các kỹ thuật IoT dựa trên Blockchain để cải thiện doanh thu cho doanh nghiệp.
- Kỹ thuật này nhằm mục đích bán và mua tài sản cá nhân như ô tô, xe máy, nhà cửa và các thiết bị điện tử bằng cách sử dụng ý tưởng về Decentralized Autonomous Corporations (DAC - Tổ chức tự trị phi tập trung) [5].
- Chức năng chính của DAC là tự động, không cần sự can thiệp của con người và sử dụng các bản ghi kỹ thuật số để đưa ra quyết định.
- Nó cho phép trao đổi dữ liệu nhanh chóng giữa tất cả các bên liên quan, chẳng hạn như thiết bị, máy tính, cá nhân, người tiêu dùng, nhà cung cấp, v.v.

Bảo mật thiết bị IoT:

- Các thiết bị IoT được sử dụng trong mô hình kinh doanh phải được bảo mật vì chúng hoạt động như một nhà cung cấp dịch vụ cho người tiêu dùng.
- Loại bỏ trung gian trong mô hình thương mại điện tử bằng cách tích hợp công nghệ Blockchain với các thiết bị IoT sẽ giúp cải thiện hiệu quả.
- Thiết bị thông minh cài đặt mô hình DAC để mua và bán một số dịch vụ như nguồn điện, linh kiện bổ sung và cập nhật ứng dụng.

Hạn chế:

- **Quản lý thiết bị IoT khó khăn:** Thiết bị IoT thường có sức mạnh xử lý hạn chế, bộ nhớ nhỏ và mức tiêu thụ điện năng thấp, gây khó khăn trong việc quản lý.
- **Rủi ro bảo mật:** Việc tích hợp BC với IoT có thể dẫn đến vi phạm bảo mật của người tiêu dùng.

4.1.7 Quản lý chuỗi cung ứng (SCM) sử dụng Blockchain

Lợi ích:

- Blockchain là nền tảng mẫu để xác nhận tính xác thực và minh bạch của sản phẩm trong suốt toàn bộ chuỗi cung ứng [19].
- Nó hỗ trợ theo dõi sản phẩm từ đầu đến cuối trong thời gian thực bằng cách sử dụng sổ cái kỹ thuật số.
- Các thiết bị IoT được sử dụng trong văn phòng, xe tải hàng hóa, kho lạnh được kết nối với sổ cái kỹ thuật số phi tập trung trong SCM để tìm ra lịch sử sản phẩm, vị trí hiện tại và trạng thái môi trường như độ ẩm và nhiệt độ.

Hạn chế:

- **Kết nối với giao diện vật lý:** Bất kể việc ứng dụng thực tế của Blockchain trong SCM, vẫn tồn tại vấn đề nội tại về việc kết nối BC với các loại giao diện vật lý khác nhau.

Ngoài ra, việc cập nhật vị trí hiện tại và tình trạng của sản phẩm khi di chuyển từ địa điểm này sang địa điểm khác vẫn được thực hiện thủ công trong SCM hiện tại.

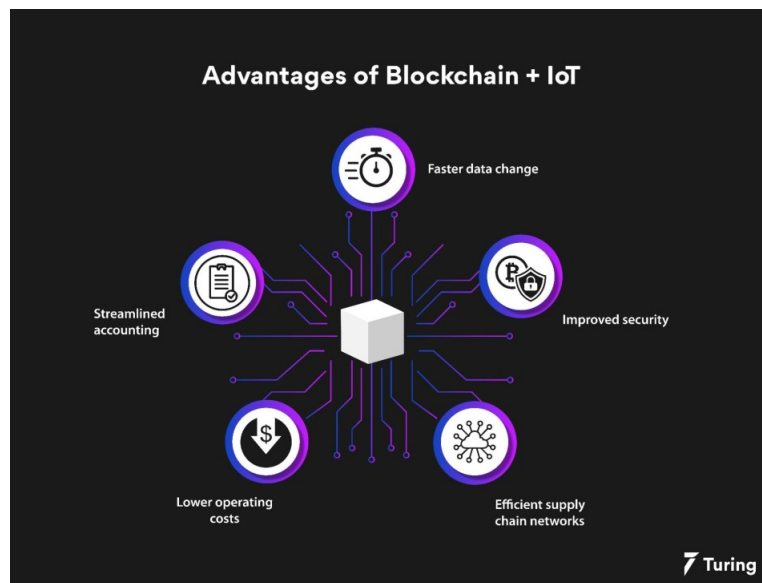
- **Tình trạng phi tập trung:**

- Trong môi trường phi tập trung, không có nút cảm biến nào khác xác định được trạng thái chính xác của mặt hàng này sau khi nó đến kho, ngoại trừ nút báo cáo về nó.
- Do đó, cần bảo mật nhiều nút cảm biến được sử dụng trong SCM để tiết lộ trạng thái sản phẩm, nhằm đảm bảo SCM an toàn.
- Công nghệ Blockchain không cần tích hợp với các thiết bị IoT nếu các nút được sử dụng trong SCM là đáng tin cậy. Ngược lại, nếu các nút trong SCM không duy trì được sự tin cậy, thì toàn bộ SCM sẽ bị tin tặc tấn công và chúng có thể dễ dàng đưa thông tin giả mạo vào SCM.

4.2 Lợi ích của công nghệ Blockchain trong hệ bảo mật IoT

4.2.1 Tốc độ thay đổi dữ liệu nhanh chóng

Aftrex Market Research xếp thay đổi dữ liệu nhanh chóng là một trong những lợi ích hàng đầu. Tuy nhiên, Michael Leone, một nhà phân tích cấp cao



Hình 4.2: Lợi ích của Blockchain trong hệ thống bảo mật IoT

tại Enterprise Strategy Group (ESG), cho rằng việc triển khai blockchain hiện tại có giới hạn trong lĩnh vực này vì nó hạn chế số giao dịch mỗi giây. "Để quản lý lượng dữ liệu, số lượng thiết bị IoT và tốc độ tương tác giữa hai bên, một phương pháp phù hợp với doanh nghiệp như blockchain dựa trên quyền hạn là rất cần thiết", theo lời Leone. "Để đáp ứng nhu cầu về hiệu suất của IoT, một blockchain có thể giảm thời gian xác nhận giao dịch bằng cách sử dụng các nút đáng tin cậy là rất quan trọng, cũng như một blockchain có thể xử lý được tốc độ trao đổi dữ liệu của IoT

4.2.2 Tăng cường bảo mật

Một trong những đặc tính thiết yếu của blockchain là khả năng xác thực dữ liệu và xác minh rằng nó có nguồn gốc từ một nguồn đáng tin cậy. Với số lượng lớn thiết bị trong IoT, điều này rất hữu ích. Blockchain cung cấp một cách để lưu trữ và quản lý dữ liệu một cách an toàn thông qua việc sử dụng các khối mã hóa chứa thông tin về các giao dịch. Mỗi khối đều chứa dấu thời gian và liên kết với khối trước đó, tạo thành một chuỗi liên tục mà không thể bị thay đổi một cách dễ dàng. Điều này giúp ngăn chặn các cuộc tấn công giả mạo dữ liệu và đảm bảo rằng thông tin lưu trữ là chính xác và không bị thay đổi.

Sự kết hợp giữa blockchain và IoT có tiềm năng cải thiện việc truyền thông an toàn và đồng thời tăng cường các thỏa thuận về quyền riêng tư. Trong một hệ thống IoT, hàng triệu thiết bị kết nối và trao đổi thông tin với nhau, việc quản lý và bảo mật dữ liệu trở thành một thách thức lớn. Blockchain có thể

cung cấp một nền tảng để các thiết bị này có thể xác thực và trao đổi thông tin một cách an toàn mà không cần sự can thiệp của bên thứ ba. Mỗi giao dịch được ghi lại trong sổ cái phân tán và chỉ những người có quyền mới có thể truy cập và thực hiện giao dịch.

Việc có một sổ cái đáng tin cậy cho thấy ai có quyền truy cập và đang thực hiện giao dịch là một lợi ích lớn. Trong các hệ thống truyền thống, việc xác định và quản lý quyền truy cập có thể phức tạp và dễ bị tấn công. Tuy nhiên, với blockchain, mỗi hành động và giao dịch đều được ghi lại một cách minh bạch và không thể thay đổi. Điều này không chỉ giúp tăng cường an ninh mà còn cung cấp một cách để theo dõi và giám sát mọi hoạt động trong hệ thống IoT. Các nhà quản lý có thể dễ dàng kiểm tra và xác minh các hoạt động, từ đó giảm thiểu rủi ro và đảm bảo rằng hệ thống hoạt động một cách hiệu quả và an toàn.

4.2.3 Mạng lưới cung cấp hiệu quả

Nâng cao hiệu suất của mạng lưới cung ứng là một ưu tiên hàng đầu của nhiều doanh nghiệp. Quá trình này, tuy nhiên, bị cản trở bởi một loạt các vấn đề kinh tế và toàn cầu. Blockchain và IoT có thể tăng cường hiệu quả chuỗi cung ứng bằng cách loại bỏ trung gian, tăng tốc độ giao dịch và giảm chi phí. Nâng cao hiệu suất của mạng lưới cung ứng là một ưu tiên hàng đầu của nhiều doanh nghiệp. Quá trình này, tuy nhiên, bị cản trở bởi một loạt các vấn đề kinh tế và toàn cầu như chi phí vận chuyển tăng, thiếu hụt nguyên liệu, và yêu cầu về minh bạch và truy xuất nguồn gốc sản phẩm. Blockchain và IoT có thể tăng cường hiệu quả chuỗi cung ứng bằng cách loại bỏ trung gian, tăng tốc độ giao dịch và giảm chi phí.

Blockchain cung cấp một sổ cái phân tán và minh bạch, nơi mọi giao dịch và thay đổi trong chuỗi cung ứng được ghi lại một cách chi tiết và không thể thay đổi. Điều này không chỉ giúp loại bỏ sự cần thiết của các bên trung gian mà còn đảm bảo rằng mọi bước trong quy trình từ sản xuất đến giao hàng đều có thể được theo dõi và xác minh một cách dễ dàng. Với công nghệ blockchain, các doanh nghiệp có thể quản lý chuỗi cung ứng một cách tự động và minh bạch, giảm thiểu thời gian và chi phí liên quan đến việc quản lý dữ liệu và giao dịch.

Khi kết hợp với IoT, blockchain còn có thể mang lại nhiều lợi ích hơn nữa cho chuỗi cung ứng. Các thiết bị IoT có thể giám sát và thu thập dữ liệu trong thời gian thực về tình trạng của hàng hóa, điều kiện vận chuyển, và hiệu suất của các máy móc trong quá trình sản xuất. Dữ liệu này sau đó có thể được ghi lại trên blockchain, đảm bảo rằng thông tin là chính xác, minh bạch và không thể bị thay đổi. Điều này giúp tăng cường khả năng truy xuất nguồn gốc và

đảm bảo chất lượng của sản phẩm, từ đó nâng cao niềm tin của khách hàng và đối tác.

Một ứng dụng cụ thể của blockchain trong bảo mật hệ thống IoT là trong việc quản lý quyền truy cập và xác thực thiết bị. Trong một chuỗi cung ứng, có rất nhiều thiết bị IoT tham gia vào quá trình giám sát và quản lý. Blockchain có thể cung cấp một phương pháp bảo mật để xác thực và quản lý quyền truy cập của từng thiết bị này. Mỗi thiết bị có thể được gán một danh tính duy nhất trên blockchain, và mọi hoạt động của nó đều được ghi lại và kiểm tra. Điều này không chỉ ngăn chặn các cuộc tấn công giả mạo mà còn giúp phát hiện và khắc phục sự cố nhanh chóng.

Ngoài ra, blockchain còn giúp giảm rủi ro về an ninh thông qua việc phân tán dữ liệu. Trong các hệ thống truyền thống, dữ liệu thường được lưu trữ tập trung, tạo ra một điểm yếu dễ bị tấn công. Tuy nhiên, với blockchain, dữ liệu được phân tán trên nhiều nút mạng, làm cho việc tấn công và thay đổi dữ liệu trở nên khó khăn hơn nhiều. Điều này không chỉ bảo vệ dữ liệu mà còn đảm bảo tính liên tục và đáng tin cậy của hệ thống IoT trong chuỗi cung ứng.

Tóm lại, sự kết hợp giữa blockchain và IoT không chỉ tăng cường hiệu quả của mạng lưới cung ứng mà còn cải thiện đáng kể khả năng bảo mật, quản lý dữ liệu và quyền truy cập trong hệ thống. Điều này giúp các doanh nghiệp không chỉ tối ưu hóa chi phí và thời gian mà còn đảm bảo chất lượng và an toàn của sản phẩm từ sản xuất đến tay người tiêu dùng.

4.2.4 Giảm chi phí

Khả năng giảm chi phí hoạt động là một trong những lợi ích được ca ngợi nhiều nhất đối với các doanh nghiệp. Dữ liệu được gửi trực tiếp từ người gửi đến người nhận mà không cần quản lý tập trung, tiết kiệm tiền của công ty và loại bỏ các điểm thất bại [10].

4.2.5 Kế toán minh bạch

Phòng kế toán sẽ là một trong những bộ phận đầu tiên trong một tổ chức được hưởng lợi từ tính minh bạch gia tăng mà blockchain và IoT mang lại. Leone nói: “Chỉ cần biết ai đang chia sẻ/gửi tiền/dữ liệu qua một chuỗi tuyến tính, được đánh dấu thời gian là bạn đã chiến thắng

Kết luận: Như chúng ta có thể thấy, công nghệ blockchain chắc chắn mang lại lợi ích cho IoT. Lý do chính là vì IoT có giới hạn trong việc cung cấp an ninh hiệu quả khi kết nối tất cả các thiết bị trên mọi loại mạng. Ngược lại, công

nghe blockchain có lợi thế chính là cung cấp an ninh xuất sắc. Sự kết hợp giữa hai công nghệ này có thể tạo ra những điều kỳ diệu!

Chương 5

Mô phỏng công nghệ Blockchain trong hệ bảo mật IoT

5.1 Mô phỏng hàm băm sử dụng thuật toán SHA-256 trong chuỗi khối Blockchain

5.1.1 Nội dung

Bước 1: Tạo ra các Block có chứa dữ liệu, hàm băm sử dụng thuật toán SHA-256, lưu hàm băm của khối trước.

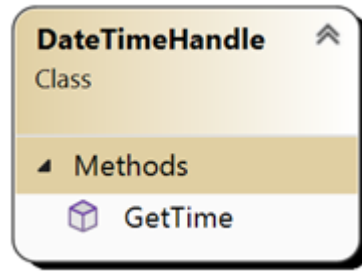
Bước 2: Kiểm tra tính bảo mật của các khối, thay đổi, sửa đổi thông tin các Block.

Bước 3: Có thể thêm Block sau khi chạy chương trình.

5.1.2 Các lớp trong chương trình

Lớp `DateTimeHandle`

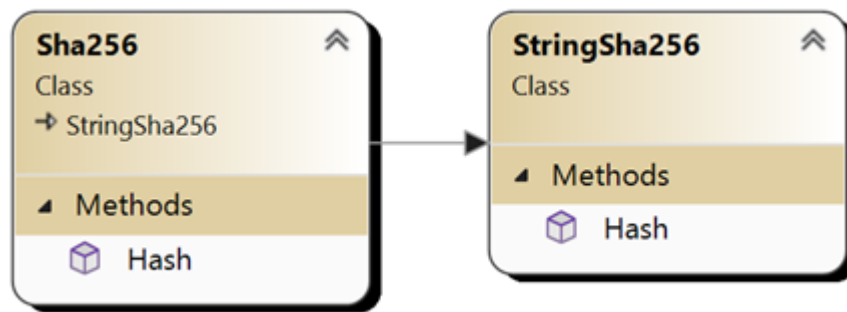
Lấy thời gian từ 1 mốc cố định cho trước. Đơn vị: Mili Giây (ms)



Hình 5.1

2.2. Lớp StringSha256 và lớp Sha256

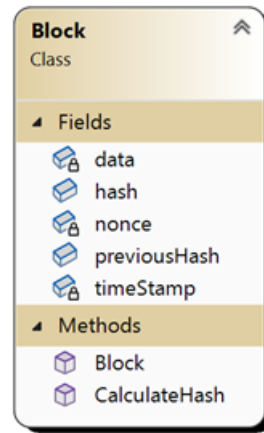
- Lớp Sha256: Mã hóa bằng thuật toán Sha256
- Lớp StringSha256: Trả về hàm băm sau khi mã hóa



Hình 5.2

5.1.3 Lớp Block: Lưu các dữ liệu

Dữ liệu (data), Hàm băm khối hiện tại (hash), Hàm băm khối trước (previousHash).



Hình 5.3

5.1.4 Kết quả

- Mốc thời gian: 1/1/2002
- Dữ liệu các khối:
 1. Khối 1: Nguyen The Phong
 2. Khối 2: Mat ma va do phuc tap thuat toan
 3. Khối 3: Khoa Toán Tin
 4. Khối 4: Dai hoc Bach khoa Ha Noi

```

C:\WINDOWS\system32\cmd. x + v
Blockchain is valid: True
[{"hash": "ee9bdb0a6778ab4ee6313c2cad361195a225dd4f4ead1dbe61bb2a3baf7efa80", "previousHash": "0"}, {"hash": "2dcff7e313f1052720a217e18637e08228b64dfbad1885dedb49cd44bacd5049", "previousHash": "ee9bdb0a6778ab4ee6313c2cad361195a225dd4f4ead1dbe61bb2a3baf7efa80"}, {"hash": "10de48d3faa61def6493a967d8f3a5d4d756cfedfaf630d2b902cb06d703bd05", "previousHash": "2dcff7e313f1052720a217e18637e08228b64dfbad1885dedb49cd44bacd5049"}, {"hash": "89337a1e352e81ff12658993d50d7f7cb71c6409c7cb9cd8b5d0afb548f139c5", "previousHash": "10de48d3faa61def6493a967d8f3a5d4d756cfedfaf630d2b902cb06d703bd05"}]

New Block
Data:
    
```

Hình 5.4: Kết quả của từng block

Lưu thêm 1 khối:

- Dữ liệu: Nhóm 3
- previous Hash: Trieu Hoang Long va Khong Nguyen Thiem

Kết quả: Giá trị previousHash của Block mới không giống Hàm Băm của Block cũ.

```

C:\WINDOWS\system32\cmd. x + v
Blockchain is valid: True
[{"hash": "ee9bdb0a6778ab4ee6313c2cad361195a225dd4f4ead1dbe61bb2a3baf7efa80", "previousHash": "0"}, {"hash": "2dcff7e313f1052720a217e18637e08228b64dfbad1885dedb49cd44bacd5049", "previousHash": "ee9bdb0a6778ab4ee6313c2cad361195a225dd4f4ead1dbe61bb2a3baf7efa80"}, {"hash": "10de48d3faa61def6493a967d8f3a5d4d756cfedfaf630d2b902cb06d703bd05", "previousHash": "2dcff7e313f1052720a217e18637e08228b64dfbad1885dedb49cd44bacd5049"}, {"hash": "89337a1e352e81ff12658993d50d7f7cb71c6409c7cb9cd8b5d0afb548f139c5", "previousHash": "10de48d3faa61def6493a967d8f3a5d4d756cfedfaf630d2b902cb06d703bd05"}]

New Block
Data: Nhom 3
Previous Hash: Trieu Hoang Long va Khong Nguyen Thiem
[{"hash": "ee9bdb0a6778ab4ee6313c2cad361195a225dd4f4ead1dbe61bb2a3baf7efa80", "previousHash": "0"}, {"hash": "2dcff7e313f1052720a217e18637e08228b64dfbad1885dedb49cd44bacd5049", "previousHash": "ee9bdb0a6778ab4ee6313c2cad361195a225dd4f4ead1dbe61bb2a3baf7efa80"}, {"hash": "10de48d3faa61def6493a967d8f3a5d4d756cfedfaf630d2b902cb06d703bd05", "previousHash": "2dcff7e313f1052720a217e18637e08228b64dfbad1885dedb49cd44bacd5049"}, {"hash": "89337a1e352e81ff12658993d50d7f7cb71c6409c7cb9cd8b5d0afb548f139c5", "previousHash": "10de48d3faa61def6493a967d8f3a5d4d756cfedfaf630d2b902cb06d703bd05"}, {"hash": "23f873a1d977b2a4952f1e1ff606a47047cee8b069659a150f09b2956a474cef", "previousHash": "Trieu Hoang Long va Khong Nguyen Thiem"}]
Previous Hashes not equal
Blockchain is valid: False
  
```

Hình 5.5: Kết quả của từng block sau khi thêm khối dữ liệu

Trong chuỗi khối, mỗi Block liên kết với Block trước thông qua giá trị previousHash. Giá trị này là Hàm Băm (hash) của Block trước, được tạo ra bằng thuật toán mã hóa mạnh mẽ.

Nếu giá trị previousHash của Block mới giống Hàm Băm của Block cũ, nghĩa là dữ liệu trong Block cũ không thay đổi. Tuy nhiên, trong thực tế, dữ liệu trong hệ thống IoT thường xuyên thay đổi, ví dụ như thông tin về trạng thái thiết bị, dữ liệu cảm biến, v.v.

Do đó, sự khác biệt giữa giá trị previousHash của Block mới và Hàm Băm của Block cũ chỉ ra rằng đã có thay đổi trong dữ liệu. Điều này giúp phát hiện các hành vi sửa đổi dữ liệu trái phép hoặc các nỗ lực tấn công vào hệ thống.

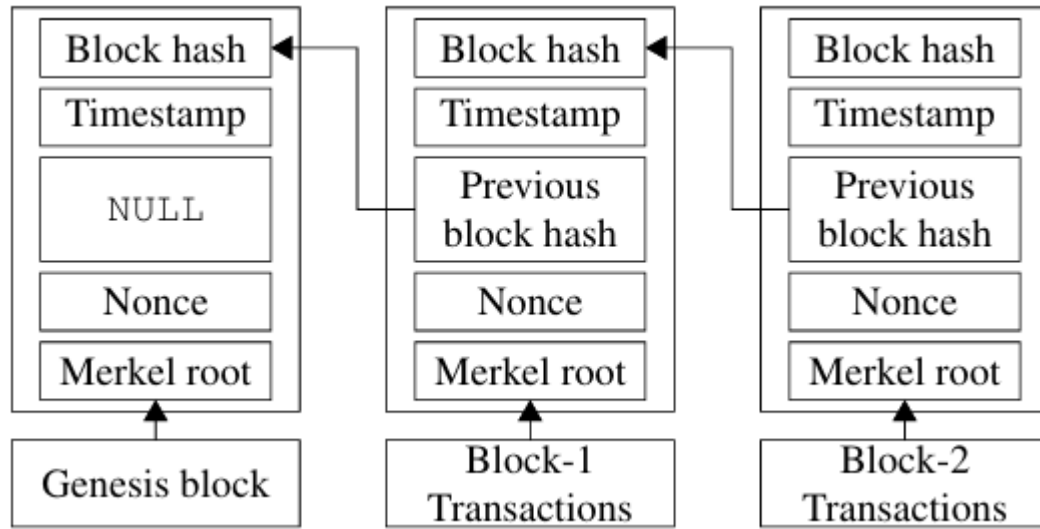
Ví dụ trong thực tế

Giả sử một kẻ tấn công cố gắng thay đổi thông tin về trạng thái của một thiết bị IoT trong Block cũ. Sau khi thay đổi, kẻ tấn công cần tạo ra một Block mới với giá trị previousHash giống Hàm Băm của Block cũ để che giấu hành vi của mình.

Tuy nhiên, do giá trị previousHash được tạo ra bằng thuật toán mã hóa mạnh mẽ, việc tạo ra một giá trị previousHash giống Hàm Băm của Block cũ mà không thay đổi dữ liệu trong Block cũ là gần như không thể.

Do đó, khi giá trị previousHash của Block mới khác Hàm Băm của Block cũ, hệ thống sẽ phát hiện ra sự thay đổi và có thể thực hiện các biện pháp để ngăn chặn các hành vi xâm hại.

5.2 Mô phỏng kiến trúc của sổ trượt Blockchain cho IoT



Hình 5.6: Kiến trúc Blockchain truyền thống

Hiện trạng và lý do chọn SWBC :

- IoT đang cách mạng hóa môi trường sống, do đó cần thiết phải bảo mật dữ liệu thu thập được từ các thiết bị này [15].
- Các thuật toán bảo mật tập trung truyền thống không phù hợp do những hạn chế về CPU, bộ nhớ và năng lượng của thiết bị IoT.

Mục đích:

- Cung cấp giải pháp bảo mật cho dữ liệu thu thập từ các thiết bị Internet of Things (IoT).
- Đề xuất kiến trúc chuỗi khối cửa sổ trượt (SWBC) thích hợp với các thiết bị IoT có tài nguyên hạn chế.

Đóng góp chính:

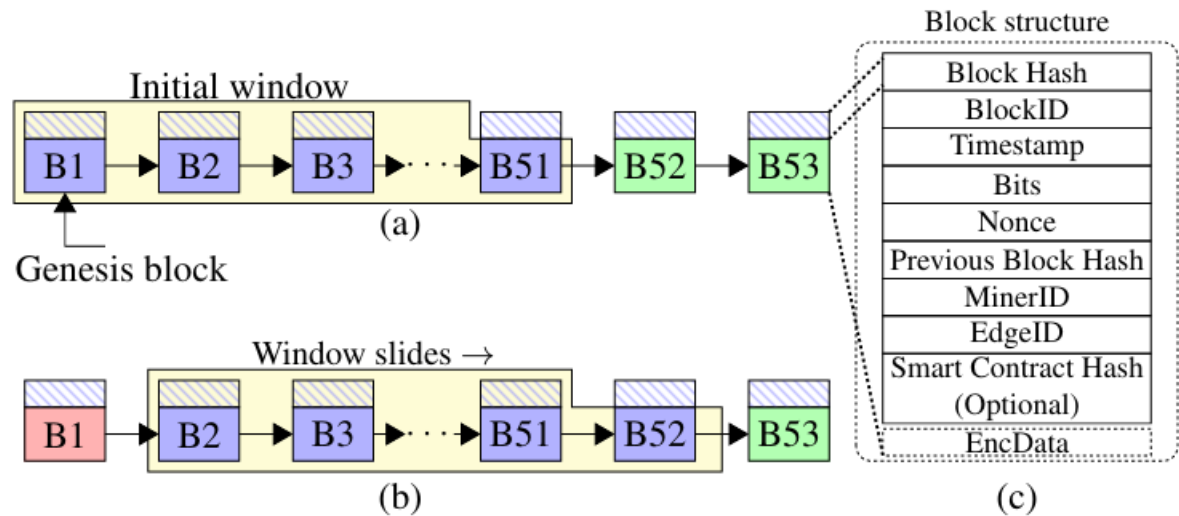
- Đề xuất kiến trúc SWBC mới để bảo mật cho IoT, tính đến hạn chế về tài nguyên.
- Thiết lập môi trường thử nghiệm nhà thông minh để triển khai và phân tích hiệu suất của kiến trúc đề xuất.

Mô phỏng :

- SWBC là một sổ cái phân tán, lưu trữ một phần chuỗi khối trong bộ nhớ thiết bị IoT và toàn bộ chuỗi khối trên đám mây riêng.
- Cửa sổ trượt cải thiện tính bất biến của dữ liệu chuỗi khối.
- Kích thước cửa sổ (n) được giữ bí mật và chỉ gửi cho thợ đào cùng với khối genesis (khối khởi tạo).
- Khối SWBC chứa các thông tin như hash block, ID block, timestamp, bits, nonce, previous block hash, minerID, and edgeID.
- Kích thước khối linh hoạt với giới hạn tối đa 1MB.
- Độ khó đào được chọn ngẫu nhiên giữa 1 và 5 để giảm tổng thời gian đào khối.
- Dữ liệu cảm biến được mã hóa bằng thuật toán AES với PBKDF2.

So sánh với Bitcoin Blockchain:

- Bitcoin Blockchain không phù hợp với IoT do độ khó đào cao và kích thước khối cố định.
- SWBC khắc phục hạn chế này bằng cách sử dụng cửa sổ trượt và kích thước khối linh hoạt.



Hình 5.7: Kiến trúc cửa sổ trượt Blockchain

Mô tả:

Cấu trúc bao gồm các thành phần như Genesis block, Initial window, EncData, Block structure, Smart Contract Hash (Optional), EdgeID, MinerID, Previous Block Hash, Nonce, Bits, Timestamp, BlockID, Block Hash.

Giải thích từng thành phần

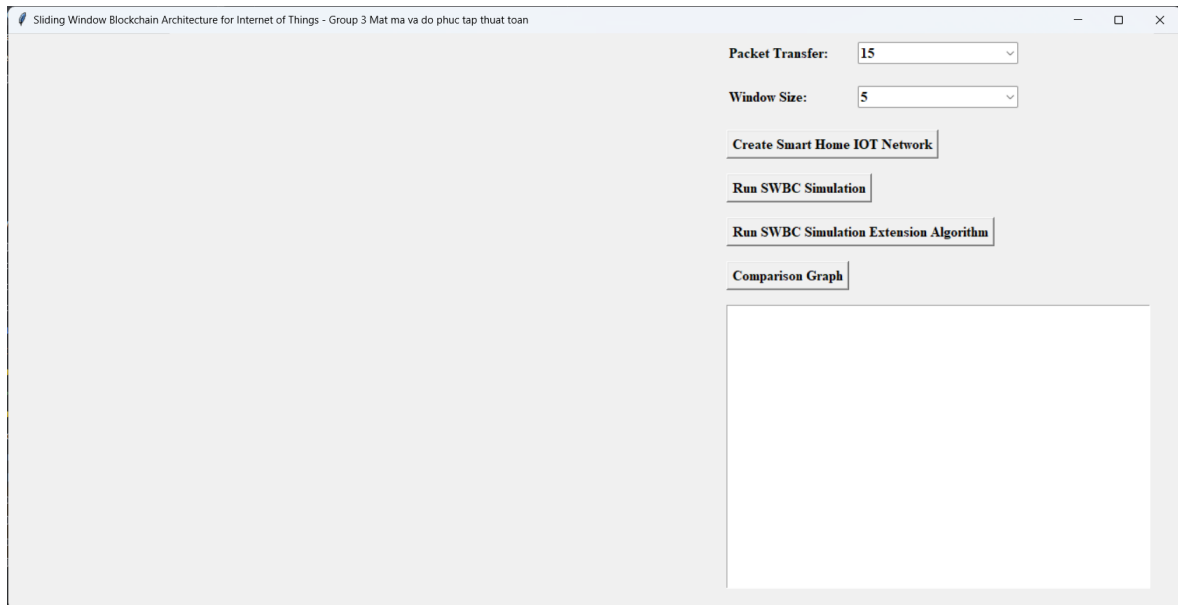
1. Genesis Block: Đây là khối đầu tiên trong chuỗi blockchain, chứa thông tin cần thiết như kích thước của cửa sổ trượt.
2. Initial Window: Cửa sổ ban đầu bao gồm một số lượng khối nhất định (thường là một khối).
3. EncData: Dữ liệu được mã hóa trước khi lưu trữ trong blockchain, đảm bảo tính bảo mật của thông tin.
4. Block Structure: Cấu trúc của mỗi khối trong blockchain, bao gồm các trường như Smart Contract Hash (tùy chọn), EdgeID, MinerID, Previous Block Hash, Nonce, Bits, Timestamp, BlockID, Block Hash.
5. Smart Contract Hash (Optional): Một trường tùy chọn trong cấu trúc khối, chứa mã băm của hợp đồng thông minh liên quan đến giao dịch.
6. EdgeID: Định danh của thiết bị IoT hoặc cạnh mạng mà khối đang được tạo ra từ.
7. MinerID: Định danh của người đào (miner) tạo ra khối.
8. Previous Block Hash: Giá trị băm của khối trước đó trong chuỗi blockchain.
9. Nonce: Giá trị ngẫu nhiên được thay đổi để tạo ra một khối với giá trị băm thỏa mãn yêu cầu khó khăn (Proof-of-Work).
10. Bits: Một trường trong khối chứa thông tin về yêu cầu khó khăn cho quá trình đào.
11. Timestamp: Thời gian khi khối được tạo ra.
12. BlockID: Định danh của khối trong chuỗi blockchain.
13. Block Hash: Giá trị băm của khối hiện tại, được tạo ra bằng cách băm các trường dữ liệu khác trong khối.

Chức năng:

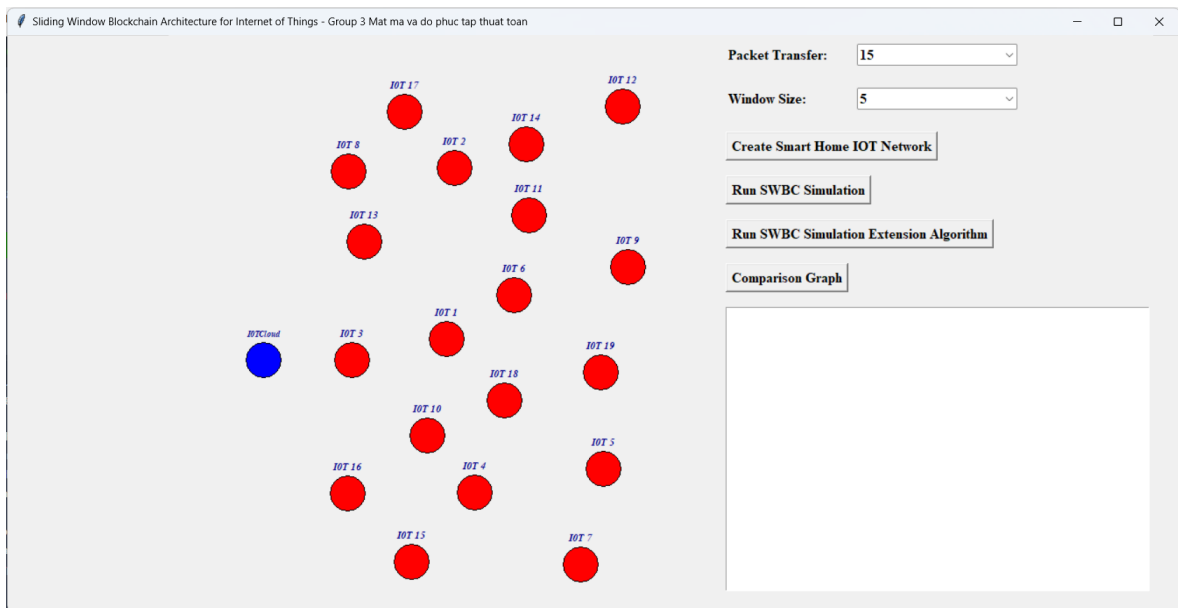
- Sliding Window Blockchain sử dụng cửa sổ trượt để cải thiện tính không thể thay đổi của các bản ghi blockchain.

CHƯƠNG 5. MÔ PHỎNG CÔNG NGHỆ BLOCKCHAIN TRONG HỆ BẢO MẬT IOT43

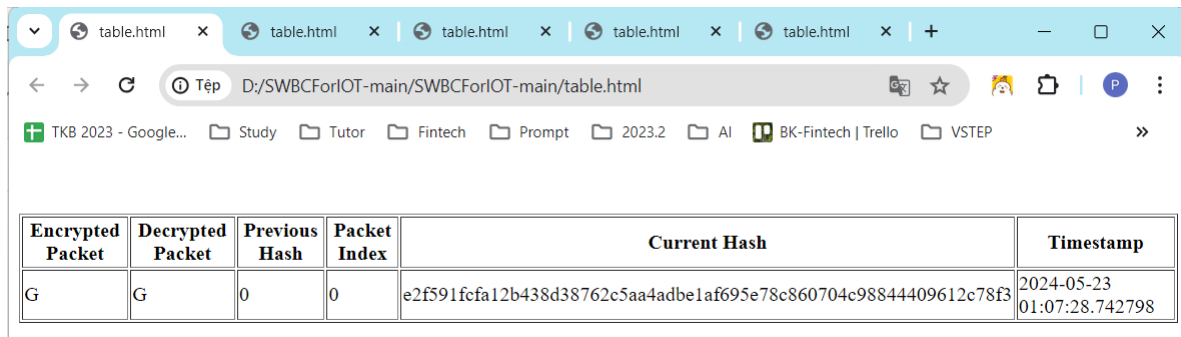
- Một miner giả mạo cần các khối trước đó (n-1) và kích thước cửa sổ n để đào một khối.
- Khi cửa sổ trượt, các khối cũ sẽ bị loại khỏi cửa sổ và được xóa khỏi bộ nhớ thiết bị IoT, giảm tải bộ nhớ cần thiết.



Hình 5.8: Bước 1: Tạo Packet Transfer và Window Size



Hình 5.9: Bước 2: Create smart home IoT Network



| Encrypted Packet | Decrypted Packet | Previous Hash | Packet Index | Current Hash | Timestamp |
|------------------|------------------|---------------|--------------|--|----------------------------|
| G | G | 0 | 0 | e2f591fcfa12b438d38762c5aa4adbe1af695e78c860704c98844409612c78f3 | 2024-05-23 01:07:28.742798 |

Hình 5.10: Bước 3

Khi chạy mô phỏng và thấy các file liên tiếp với các thông tin như Encrypted Packet, Decrypted Packet, Previous Hash, Packet Index, Current Hash, Timestamp và chỉ thay đổi ở mỗi Current Hash, điều này có ý nghĩa và mục đích nhất định trong việc bảo mật cho môi trường IoT. Dưới đây là một số lý do và ý nghĩa của việc này:

Bảo mật dữ liệu:

Việc mã hóa (encryption) và giải mã (decryption) dữ liệu trong các gói tin (packets) giúp đảm bảo tính bảo mật của thông tin truyền tải trong mạng IoT. Điều này ngăn chặn người ngoài cuộc truy cập trái phép vào dữ liệu quan trọng. Previous Hash và Current Hash:

Previous Hash là giá trị băm của gói tin trước đó, đóng vai trò quan trọng trong việc xác thực tính toàn vẹn của dữ liệu. Current Hash là giá trị băm của gói tin hiện tại, thay đổi ở mỗi gói tin để đảm bảo tính duy nhất và không thể thay đổi của từng gói tin. Timestamp:

Thời gian (Timestamp) ghi lại thời điểm mà gói tin được tạo ra hoặc xử lý, giúp trong việc theo dõi và xác định chuỗi thời gian của các sự kiện trong mạng IoT. Liên tiếp và thay đổi Current Hash:

Việc các file xuất hiện liên tiếp và chỉ thay đổi ở mỗi Current Hash có thể đại diện cho việc tạo ra các gói tin mới liên tục và duy trì chuỗi dữ liệu an toàn và bảo mật. Sự liên tục này có thể phản ánh quá trình truyền tải dữ liệu liên tục trong môi trường IoT mà không bị gián đoạn. Tóm lại, việc thấy các file liên tiếp với các thông tin như Encrypted Packet, Decrypted Packet, Previous Hash, Packet Index, Current Hash, Timestamp và sự thay đổi ở mỗi Current Hash trong quá trình mô phỏng có ý nghĩa quan trọng trong việc bảo mật dữ liệu và duy trì tính toàn vẹn của thông tin trong môi trường IoT.

Tổng kết

Trong bối cảnh cách mạng công nghiệp 4.0, Internet of Things (IoT) đang phát triển mạnh mẽ, mang lại nhiều tiện ích và cải tiến cho cuộc sống. Tuy nhiên, cùng với sự phát triển này là những thách thức về bảo mật do sự kết nối của hàng tỷ thiết bị. Blockchain, với các đặc tính bảo mật và phân quyền của nó, được xem là giải pháp tiềm năng để bảo vệ hệ thống IoT khỏi các cuộc tấn công và lỗ hổng bảo mật.

Tổng Quan về Blockchain và IoT

Blockchain là một công nghệ sổ cái phân tán cho phép lưu trữ dữ liệu một cách an toàn và không thể sửa đổi. Các đặc điểm nổi bật của blockchain bao gồm:

- Tính phi tập trung: Không có một thực thể trung tâm nào kiểm soát toàn bộ mạng lưới.
- Tính minh bạch: Mọi giao dịch được ghi lại công khai và dễ dàng kiểm tra.
- Tính bất biến: Một khi dữ liệu đã được ghi vào blockchain, rất khó để thay đổi nó.
- Tính bảo mật: Dữ liệu được mã hóa và phân phối trên nhiều node, làm giảm nguy cơ bị tấn công.
- IoT là mạng lưới các thiết bị kết nối với nhau qua internet, thu thập và trao đổi dữ liệu. Sự kết nối này tạo ra cơ hội nhưng cũng đưa đến nhiều rủi ro về bảo mật, như các cuộc tấn công DDoS, truy cập trái phép, và giả mạo dữ liệu.

Ứng Dụng của Blockchain trong Bảo Mật Hệ Thống IoT

• Xác Thực Thiết Bị:

Blockchain có thể cung cấp một hệ thống xác thực an toàn cho các thiết bị IoT. Thay vì sử dụng các chứng chỉ số tập trung, blockchain cho phép xác thực phân tán, giảm nguy cơ giả mạo.

- Quản Lý Dữ Liệu:

Dữ liệu từ các thiết bị IoT có thể được ghi vào blockchain để đảm bảo tính toàn vẹn và bất biến. Điều này giúp ngăn chặn việc thay đổi dữ liệu và đảm bảo tính chính xác của thông tin. Bảo Mật Giao Dịch:

Blockchain cho phép ghi lại mọi giao dịch giữa các thiết bị IoT một cách minh bạch và không thể thay đổi. Điều này giúp theo dõi và kiểm soát các hoạt động trong mạng lưới IoT.

- Quản Lý Quyền Truy Cập:

Sử dụng smart contracts, blockchain có thể tự động quản lý quyền truy cập của các thiết bị và người dùng, đảm bảo rằng chỉ những đối tượng có quyền mới có thể truy cập vào dữ liệu và tài nguyên.

- Phòng Chống Tấn Công:

Với cơ chế phi tập trung và mã hóa mạnh mẽ, blockchain làm giảm nguy cơ bị tấn công DDoS và các loại tấn công mạng khác. Mỗi node trong mạng lưới đều có bản sao của sổ cái, giúp phân tán rủi ro.

Tài liệu tham khảo

- [1] Rob van Kranenburg Thorsten Kramp and Sebastian Lange. “Introduction to the Internet of Things”. In: (2013), p. 1.
- [2] InformationWeek. “Internet of Things Done Wrong Stifles Innovation”. In: (2014).
- [3] Carnegie Mellon University. “The "Only" Coke Machine on the Internet”. In: (2014).
- [4] Ali Dorri et al. “Blockchain for IoT security and privacy: The case study of a smart home”. In: *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE. 2017, pp. 618–623.
- [5] Yu Zhang and Jiangtao Wen. “The IoT electric business model: Using blockchain technology for the internet of things”. In: *Peer-to-Peer Networking and Applications* 10 (2017), pp. 983–994.
- [6] Hany F Atlam et al. “Blockchain with internet of things: Benefits, challenges, and future directions”. In: *International Journal of Intelligent Systems and Applications* 10.6 (2018), pp. 40–48.
- [7] Rafael Bettín-Díaz, Alix E Rojas, and Camilo Mejía-Moncayo. “Methodological approach to the definition of a blockchain system for the food industry supply chain traceability”. In: *International Conference on Computational Science and Its Applications*. Springer. 2018, pp. 19–33.
- [8] Minhaj Ahmad Khan and Khaled Salah. “IoT security: Review, blockchain solutions, and open challenges”. In: *Future generation computer systems* 82 (2018), pp. 395–411.
- [9] Sagar Bhat Pradyumna Gokhale Omkar Bhat. “Introduction to IoT”. In: (2018), pp. 42–43.

- [10] Li Bai et al. “BPIIoT: A light-weighted blockchain-based platform for industrial IoT”. In: *IEEE Access* 7 (2019), pp. 58381–58393.
- [11] Rui Han et al. “Blockchain-based GNSS spoofing detection for multiple UAV systems”. In: *Journal of Communications and Information Networks* 4.2 (2019), pp. 81–88.
- [12] P Karthikeyyan, S Velliangiri, et al. “Review of Blockchain based IoT application and its security issues”. In: *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*. Vol. 1. IEEE. 2019, pp. 6–11.
- [13] P Swathi, Chirag Modi, and Dhiren Patel. “Preventing sybil attack in blockchain using distributed behavior monitoring of miners”. In: *2019 10th international conference on computing, communication and networking technologies (ICCCNT)*. IEEE. 2019, pp. 1–6.
- [14] Poornima M Chanal and Mahabaleshwar S Kakkasageri. “Security and privacy in IoT: a survey”. In: *Wireless Personal Communications* 115.2 (2020), pp. 1667–1693.
- [15] Prescilla Koshy, Sarath Babu, and BS Manoj. “Sliding window blockchain architecture for internet of things”. In: *IEEE Internet of Things Journal* 7.4 (2020), pp. 3338–3348.
- [16] Raffaele Martino and Alessandro Cilardo. “Designing a SHA-256 processor for blockchain-based IoT applications”. In: *Internet of Things* 11 (2020), p. 100254.
- [17] Ali Sunyaev and Ali Sunyaev. “Distributed ledger technology”. In: *Internet computing: Principles of distributed systems and emerging internet-based technologies* (2020), pp. 265–299.
- [18] Lorenzo Ghiro et al. “What is a Blockchain? A Definition to Clarify the Role of the Blockchain in the Internet of Things”. In: *arXiv preprint arXiv:2102.03750* (2021).
- [19] Muzammil Hussain et al. “Blockchain-based IoT devices in supply chain management: a systematic literature review”. In: *Sustainability* 13.24 (2021), p. 13646.
- [20] iFACTORY. “Tìm hiểu về các thành phần cơ bản của mô hình IoT phổ biến nhất hiện nay”. In: (2021), p. 42.
- [21] Umer Majeed et al. “Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges”. In: *Journal of Network and Computer Applications* 181 (2021), p. 103007.

- [22] Taotao Wang et al. “Ethna: Analyzing the underlying peer-to-peer network of ethereum blockchain”. In: *IEEE Transactions on Network Science and Engineering* 8.3 (2021), pp. 2131–2146.
- [23] Endale Mitiku Adere. “Blockchain in healthcare and IoT: A systematic literature review”. In: *Array* 14 (2022), p. 100139.
- [24] Gyungmin Kim and Yonggang Kim. “The Threat of Disruptive Jamming to Blockchain-Based Decentralized Federated Learning in Wireless Networks”. In: *Sensors* 24.2 (2024), p. 535.

Code C# Lớp DateTimeHandle

```
using System;

namespace VdBlockchain.Classes
{
    public class DateTimeHandle
    {
        public static long GetTime()
        {
            long result = 0;
            var st = new DateTime(2002, 1, 1);
            TimeSpan t = (DateTime.Now.ToUniversalTime() - st);
            result = (Int64)(t.TotalMilliseconds + 0.5);
            return result;
        }
    }
}
```

Listing 5.1: DateTimeHandle class in C#

Code C# Lớp StringSha256

```
namespace VdBlockchain.Classes
{
    class StringSha256
    {
        public virtual string Hash(string strInput)
        {
            return strInput;
        }
    }
}
```

Listing 5.2: StringSha256 class in C#

Code C# Lớp HashSha256

```
using System;
using System.Text;

namespace VdBlockchain.Classes
{
    class Sha256 : StringSha256
    {
        public override string Hash(string strInput)
        {
            try
            {
                var crypt = new System.Security.Cryptography.SHA256Managed();
                var hash = new System.Text.StringBuilder();
                byte[] crypto = crypt.ComputeHash(Encoding.UTF8.GetBytes(strInput));
                foreach (byte theByte in crypto)
                {
                    hash.Append(theByte.ToString("x2"));
                }
                return hash.ToString();
            }
            catch (Exception e)
            {
                throw e;
            }
        }
    }
}
```

Listing 5.3: HashSha256 class in C#

Code C# Lớp Block

```
using System;
using VdBlockchain.Classes;
```

```

namespace VdBlockchain
{
    class Block
    {
        public String hash;
        public String previousHash;
        private String data;

        private long timeStamp;
        private int nonce = 0;

        public Block(String data, String previousHash)
        {
            this.data = data;
            this.previousHash = previousHash;
            this.timeStamp = DateTimeHandle.GetTime();
            this.hash = CalculateHash();
        }

        public String CalculateHash()
        {
            Sha256 sha256 = new Sha256();
            String calculatedhash = sha256.Hash(previousHash + timeStamp.ToString() +
nonce.ToString() + data);
            return calculatedhash;
        }
    }
}

```

Listing 5.4: Block class in C#

Code C# Lớp Program

```

using System;
using System.Collections.Generic;
using System.Linq;

```

```

namespace VdBlockchain
{
    class Program
    {
        public static List<Block> blockchain = new List<Block>();
        static void Main(string[] args)
        {
            blockchain.Add(new Block("Mat Ma", "0"));
            blockchain.Add(new Block("Do phuc tap thuat toan",
blockchain.ElementAt(blockchain.Count - 1).hash));
            blockchain.Add(new Block("Toan Tin", blockchain.ElementAt(blockchain.Count -
1).hash));

            Console.WriteLine("Blockchain is valid: " + IsChainValid());

            string printBlockChain = new
System.Web.Script.Serialization.JavaScriptSerializer().Serialize(blockchain);
            Console.WriteLine(printBlockChain);

            string data, previousHash;
            Console.WriteLine();
            Console.WriteLine("New Block");
            Console.Write("Data: ");
            data = Console.ReadLine();
            Console.Write("Previous Hash: ");
            previousHash = Console.ReadLine();
            blockchain.Add(new Block(data, previousHash));
            string printBlockChain1 = new
System.Web.Script.Serialization.JavaScriptSerializer().Serialize(blockchain);
            Console.WriteLine(printBlockChain1);
            Console.WriteLine("Blockchain is valid: " + IsChainValid());
            Console.ReadLine();
        }

        public static Boolean IsChainValid()
        {
            Block currentBlock;

```



```

        Block previousBlock;

        for (int i = 1; i < blockchain.Count; i++)
        {
            currentBlock = blockchain.ElementAt(i);
            previousBlock = blockchain.ElementAt(i - 1);

            if (!currentBlock.hash.Equals(currentBlock.CalculateHash()))
            {
                Console.WriteLine("Current Hashes not equal");
                return false;
            }

            if (!previousBlock.hash.Equals(currentBlock.previousHash))
            {
                Console.WriteLine("Previous Hashes not equal");
                return false;
            }
        }
        return true;
    }
}

```

Listing 5.5: Program class in C#