BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

HUỲNH THANH TÂM

NỀN TẢNG ĐẢM BẢO AN TOÀN BẢO MẬT DỰA TRÊN BLOCKCHAIN CHO LIÊN MẠNG VẠN VẬT

LUẬN ÁN TIẾN SĨ KỸ THUẬT

HÀ NỘI - 2022

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

HUỲNH THANH TÂM

NỀN TẢNG ĐẢM BẢO AN TOÀN BẢO MẬT DỰA TRÊN BLOCKCHAIN CHO LIÊN MẠNG VẠN VẬT

Chuyên ngành: **Hệ thống thông tin**

Mã số: 9.48.01.04

LUẬN ÁN TIẾN SĨ KỸ THUẬT

Người hướng dẫn khoa học:

1. **PGS.TS. NGUYỄN ĐÌNH THÚC**
2. **TS. TÂN HẠNH**

HÀ NỘI - 2022

LỜI CAM ĐOAN

Tôi xin cam đoan luận án tiến sĩ "***Nền tảng đảm bảo an toàn bảo mật dựa trên Blockchain cho liên mạng vạn vật***" là công trình nghiên cứu do tôi thực hiện. Các số liệu và kết quả trình bày trong luận án là trung thực, chưa được công bố trong bất kỳ công trình nào khác. Tất cả những tham khảo từ các nghiên cứu liên quan đều được nêu nguồn gốc một cách rõ ràng trong danh mục các tài liệu tham khảo.

Tác giả luận án

Huỳnh Thanh Tâm

LỜI CẢM ƠN

Trong quá trình hoàn thành luận án này, tôi đã được sự giúp đỡ tận tình từ quý thầy cô nơi cơ sở đào tạo, lãnh đạo Học viện Công nghệ Bưu chính Viễn thông cơ sở tại TP. Hồ Chí Minh và khoa Công nghệ thông tin 2 đã tạo mọi điều kiện thuận lợi, bạn bè cùng gia đình thường xuyên động viên khích lệ.

Luận án này không thể hoàn thành tốt nếu không có sự tận tình hướng dẫn và sự giúp đỡ quý báu của PGS.TS Nguyễn Đình Thúc và TS. Tân Hạnh. Tôi xin được bày tỏ lòng biết ơn sâu sắc nhất đến hai thầy.

Tôi xin chân thành cảm ơn lãnh đạo Học viện Công nghệ Bưu chính Viễn thông, khoa Đào tạo sau đại học đã tạo điều kiện thuận lợi, hỗ trợ hoàn thành các thủ tục để giúp tôi hoàn thành được luận án của mình.

Tôi xin trân trọng cảm ơn các nhà khoa học, các thầy cô, các đồng nghiệp đã có những góp ý hữu ích, phản biện khách quan để tôi không ngừng hoàn thiện luận án này.

Cuối cùng, tôi xin cảm ơn tất cả bạn bè và người thân đã đóng góp nhiều ý kiến thiết thực và có những lời động viên khích lệ quý báu giúp tôi hoàn thành tốt luận án.

Hà Nội, tháng 03 năm 2022

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

Thuật ngữ	Diễn giải tiếng anh	Diễn giải tiếng việt
CMT	Connection Management Table	Bảng quản lý kết nối
DAG	Distributed Acyclic Graph	Đồ thị không chu trình phân tán
DHT	Distributed Hash Table	Bảng băm phân tán
DoS	Denial of Service	Tấn công từ chối dịch vụ
DPoS	Delegated Proof of Stake	Giao thức đồng thuận bằng chứng cổ phần được ủy quyền
GPS	Global Positioning System	Hệ thống định vị toàn cầu
HTTP	Hyper Text Transfer Protocol	Giao thức truyền siêu văn bản
HTTPS	Hyper Text Transfer Protocol Secure	Giao thức truyền siêu văn bản bảo mật
IDC	International Data Corporation	Tập đoàn dữ liệu quốc tế
IoT	Internet of Things	Internet vạn vật
IP	Internet Protocol	Giao thức Internet
IPFS	InterPlanetary File System	Hệ thống tệp phân tán
IPNS	InterPlanetary Naming System	Hệ thống đặt tên trong IPFS
PBFT	Practical Byzantine Fault Tolerance	Giao thức đồng thuận khả năng chịu lỗi Byzantine
PoA	Proof-of-Activity	Giao thức đồng thuận bằng chứng hoạt động
PoAh	Proof-of-Authentication	Giao thức đồng thuận bằng chứng xác thực
PoS	Proof-of-Stake	Giao thức đồng thuận bằng chứng cổ phần
PoW	Proof-of-Work	Giao thức đồng thuận bằng chứng công việc

SFS	Self-Certified File System	Hệ thống tệp tự chứng nhận
TCP	Transmission Control Protocol	Giao thức điều khiển truyền thông
UDP	User Datagram Protocol	Giao thức truyền thông không cần thiết lập kết nối trước khi truyền dữ liệu
WEBRTC	Web Real-Time Communications	Một nền tảng giao tiếp thời gian thực dành cho Web

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC KÝ HIỆU

Ký hiệu	Ý nghĩa
arg	Tham số
$A1$	Thuật toán A1
$A2$	Thuật toán A2
$c_{t\times1}$	Vector bộ đếm
$CERT$	Chứng chỉ
$d(x,y)$	Khoảng cách giữa x và y
$D_K(M)$	Thuật toán giải mã cho thông điệp *M* với khóa bí mật *K*
DO	Chủ sở hữu dữ liệu/thiết bị
DP	Nhà cung cấp dữ liệu
DS	Lưu trữ phi tập trung
DU	Người sử dụng dữ liệu/Người dùng
$E_K(M)$	Thuật toán mã hóa cho thông điệp *M* với khóa bí mật *K*
EMD	Bản mã hóa của dữ liệu có nghĩa
EMD_Link	Địa chỉ truy cập của *EMD*
gmk	Khóa riêng của người quản lý nhóm trong phương thức chữ ký nhóm
gpk	Khóa công khai của nhóm trong phương thức chữ ký nhóm
grk	Khóa riêng của người quản lý thu hồi trong phương thức chữ ký nhóm
GS	Phương thức chữ ký nhóm
gsk	Một vector n phần tử của các khóa thành viên trong phương thức chữ ký nhóm
$gsk[i]$	Khóa riêng của thành viên thứ i trong phương thức chữ ký nhóm
H	Hàm băm mật mã

$Have\_list$	Danh sách chứa các khối đang sở hữu
$IdDP[i]$	Mã định danh của nhà cung cấp dữ liệu thứ i
k	Số mục trong bảng băm phân tán
l	Số lượng giao dịch tối đa trong một khối
m_i	Miner thứ i
m_{ij}	Phần tử của ma trận ở hàng i và cột j của ma trận, $m_{ij} \in \{0,1\}$
$make\_proc(x)$	Hàm tạo ra một dữ liệu số từ một dữ liệu thô x
MD	Dữ liệu có nghĩa/có giá trị
n	Số lượng Miner trong mạng
$[n]$	Tập các phần tử $\{1, 2, \dots, n\}$
$NodeID$	Định danh của Node trong mạng IPFS
$PCS(M, K)$	Một hệ mật mã khóa công khai với thông điệp M và một khóa K
PK_{DO}	Khóa công khai của DO
PK_{DU}	Khóa công khai của DU
PK_{GM}	Khóa công khai của người quản lý nhóm
PK_{RM}	Khóa công khai của người quản lý thu hồi
$PKBC_{GM}$	Khóa công khai của người quản lý nhóm trên Blockchain
$Rand\_key(\cdot)$	Hàm tạo khóa ngẫu nhiên
S_Δ	Danh sách các IP đã bắt được trong khoảng thời gian Δ
SK_{DO}	Khóa riêng của DO
SK_{DU}	Khóa riêng của DU
SK_{GM}	Khóa riêng của người quản lý nhóm
SK_{RM}	Khóa riêng của người quản lý thu hồi
$SKBC_{GM}$	Khóa riêng của người quản lý nhóm trên Blockchain
t	Số hàng của ma trận d-phân-cách, số lượng nhóm thử
t_1	Thời gian xác minh/kiểm tra một giao dịch

t_2	Thời gian tạo một chữ ký số/phiếu/chứng chỉ
t_3	Thời gian xác minh một chữ ký số/phiếu/chứng chỉ
t_4	Thời gian quảng bá một khối/phiếu/chứng chỉ/giao dịch đến đích
t_5	Thời gian lựa chọn một Miner tại mỗi vòng Mining
tx_i	Giao dịch thứ i
T	Thời gian tạo một khối mới của nền tảng được đề xuất với trường hợp 1
T'	Thời gian tạo một khối mới của thuật toán $A1$
$T1$	Thời gian tạo một khối mới của nền tảng được đề xuất với trường hợp 2
$T1'$	Thời gian tạo một khối mới của thuật toán $A2$
TX	Giao dịch Blockchain
TX^*	Giao dịch Blockchain đã được xác minh
VL	Danh sách chứa các giao dịch đã được xác minh là hợp lệ
$Want\_list$	Danh sách chứa các khối muốn nhận
WL	Danh sách chứa các giao dịch chưa được xác minh
α	Số lượng Node được truy vấn song song trong IPFS
δ	Ngưỡng tần suất cao
λ	Tham số bảo mật
σ	Chữ ký số
$\oplus$	Phép XOR
Δ	Khoảng cách/khoảng thời gian
$:\equiv$	Một phương thức được thực hiện bởi sự tương tác của con người
$\|\|$	Phép nối chuỗi
$\xleftarrow{r}$	Hàm lựa chọn Miner ngẫu nhiên

MỞ ĐẦU

1. GIỚI THIỆU

Liên mạng vạn vật còn được gọi là Internet vạn vật (từ này viết là IoT) là một mạng gồm nhiều thiết bị vật lý tham gia vào Internet nhằm mục đích kết nối và trao đổi dữ liệu với các thiết bị và hệ thống khác. Đi kèm với sự phát triển nhanh chóng về số lượng và chủng loại thiết bị IoT kết nối vào hệ thống mạng, nhu cầu về truy cập tài nguyên, lưu trữ và chia sẻ dữ liệu ngày càng gia tăng. Điều này đặt ra các thách thức cho các nền tảng bảo mật của IoT như: (1) tốc độ xử lý dữ liệu phải nhanh chóng và chính xác; (2) cần cung cấp các chức năng bảo mật cần thiết cho người dùng, chẳng hạn như: kiểm soát truy cập, lưu trữ và chia sẻ dữ liệu; và (3) cần đảm bảo tính sẵn sàng và khả năng mở rộng của hệ thống.

Với thực tế như vậy, luận án nghiên cứu và đề xuất một nền tảng bảo mật dựa trên công nghệ xâu chuỗi (từ này viết là Blockchain) cho IoT. Sử dụng Blockchain trong bảo mật IoT có thể là giải pháp thích hợp bởi các ưu điểm mà công nghệ này mang lại như: *tính phi tập trung, tính ẩn danh, tính minh bạch,* và *tính kiểm toán* [1] [70]. So với các nền tảng bảo mật tương tự, nền tảng bảo mật được đề xuất trong luận án đảm bảo tối ưu hiệu năng cho các nút (Node) nắm giữ sổ cái (từ này viết là Miner) trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain, đồng thời cung cấp nhiều tính năng bảo mật hơn.

Trong liên mạng vạn vật, nhu cầu lưu trữ dữ liệu, chia sẻ dữ liệu và truy cập tài nguyên là rất lớn. Nhằm đáp ứng các nhu cầu này, luận án cũng đề xuất ba phương thức: (1) lưu trữ dữ liệu an toàn; (2) chia sẻ dữ liệu đảm bảo tính riêng tư; và (3) kiểm soát truy cập cho các thiết bị IoT theo thời gian được cấp phép bởi chủ sở hữu thiết bị. Các phương thức này là các chức năng trong nền tảng bảo mật được đề xuất của luận án.

Các Miner trong nền tảng bảo mật được đề xuất đóng vai trò quan trọng trong việc xác minh các giao dịch và đồng thuận dữ liệu trên sổ cái. Bảo vệ các Miner này trước các nguy cơ tấn công từ chối dịch vụ từ các Node tiềm tàng độc hại (gọi là Hot-

IP) trong mạng sẽ góp phần nâng cao tính ổn định của nền tảng. Do đó, luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner trong nền tảng.

2. LÝ DO CHỌN ĐỀ TÀI

Ngày nay, số lượng và chủng loại các thiết bị IoT được đưa vào sử dụng ngày càng nhiều và cung cấp nhiều tiện ích cho người dùng. Tuy nhiên, hầu hết các thiết bị IoT đều bị hạn chế về khả năng tính toán và dung lượng lưu trữ, làm cho việc triển khai giải pháp bảo mật trên từng thiết bị trong mạng gặp nhiều khó khăn và đôi khi không khả thi. Xây dựng một nền tảng bảo mật cho IoT là giải pháp khả thi hơn. Dựa trên kiến trúc triển khai, các nền tảng bảo mật cho IoT có thể được chia làm hai nhóm: (1) nhóm các nền tảng bảo mật dựa trên kiến trúc tập trung; và (2) nhóm các nền tảng bảo mật dựa trên kiến trúc phi tập trung.

Các nền tảng bảo mật dựa trên kiến trúc tập trung với các ưu điểm là dễ dàng triển khai, độ trễ thấp và chí phí triển khai thấp. Chúng rất thích hợp với các mạng IoT có kích thước nhỏ với nhu cầu mở rộng thấp. Tuy nhiên, các nền tảng bảo mật thuộc nhóm này có một số hạn chế liên quan đến *bảo mật dữ liệu, tính sẵn sàng* và *khả năng mở rộng của hệ thống* [64][67].

Trong khi đó, các nền tảng bảo mật dựa trên kiến trúc phi tập trung có ưu điểm là đảm bảo được tính sẵn sàng của hệ thống và có khả năng mở rộng cao. Đặc điểm chung của những nền tảng bảo mật thuộc nhóm này là sử dụng công nghệ Blockchain làm thành phần trung tâm. Áp dụng công nghệ Blockchain vào bảo mật IoT đang là xu hướng phát triển mới và thu hút nhiều sự quan tâm của các nhóm nghiên cứu trong thời gian gần đây.

Hiện tại, hầu hết các nền tảng bảo mật dựa trên Blockchain cho IoT chỉ chủ yếu tập trung vào việc cung cấp một trong các chức năng bảo mật, như: *kiểm soát truy cập, xác thực, truyền thông an toàn, lưu trữ dữ liệu an toàn* [17][30][37][46][49][55][57]. Trong khi cơ chế xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain của các Miner phụ thuộc hoàn toàn vào một trong các giao thức đồng thuận như: *PoW, PoS, PoA, PoAh, DPoS, PBFT, Tendermint*. Tuy nhiên, việc sử dụng một trong các giao thức đồng thuận nêu trên trong nền tảng bảo mật dựa trên

Blockchain vẫn chưa đạt được sự tối ưu cho các Miner trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain trong hai trường hợp sau đây:

- ✓ **Trường hợp 1:** Tất cả các Miner trong một mạng Blockchain đều hoàn toàn tin cậy. Khi nhiều Miner tham gia vào mạng Blockchain, tốc độ xác minh các giao dịch và tạo khối mới trên sổ cái vẫn không thay đổi.
- ✓ **Trường hợp 2:** Trong một mạng Blockchain có tồn tại một số Miner không đáng tin cậy, nhưng số lượng ít hơn 1/3 trong tổng số các Miner trong mạng. Nếu tại một vòng đóng khối (từ này viết là Mining), một Miner không tin cậy được chọn để thực hiện công việc đề xuất một khối mới lên mạng Blockchain, Miner này hoàn toàn có thể đặt một hoặc một vài giao dịch không hợp lệ cùng với các giao dịch hợp lệ vào trong một khối mới, sau đó quảng bá khối này đến các Miner khác trong mạng. Khối mới này tất nhiên sẽ bị loại bỏ bởi các Miner tin cậy trong mạng. Tuy nhiên, các giao dịch hợp lệ nằm trong khối này lại phải xác minh thêm một lần nữa tại các vòng Mining tiếp theo. Việc này gây lãng phí tài nguyên cho các Miner khi phải xác minh lại các giao dịch đã được thực hiện trước đây.

Do đó, luận án sẽ đề xuất một nền tảng bảo mật mới với phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của các Miner đảm bảo các yêu cầu cụ thể như sau:

- ✓ **Đối với trường hợp 1:**
  (1) Tăng số lượng giao dịch được xác minh khi tăng số lượng Miner trong nền tảng.
  (2) Giảm thời gian Mining khi tăng số lượng Miner trong nền tảng.
  (3) Tăng số lượng giao dịch được xác minh khi thời gian Mining một khối tăng lên trong khi số lượng Miner không thay đổi.
- ✓ **Đối với trường hợp 2:** Các giao dịch chỉ cần xác minh một lần.

Bên cạnh đó, nền tảng bảo mật được đề xuất sẽ cung cấp các chức năng bảo mật: chức năng kiểm soát truy cập dựa trên thời gian được cấp phép, chức năng lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo tính riêng tư.

3. MỤC TIÊU NGHIÊN CỨU

3.1. Mục tiêu tổng quát

Mục tiêu của luận án là đề xuất một nền tảng đảm bảo an toàn bảo mật dựa trên Blockchain cho IoT; sử dụng một số công nghệ và công cụ toán học kết hợp để đề xuất chức năng lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo tính riêng tư cho nền tảng; đề xuất chức năng kiểm soát truy cập theo thời gian được cấp phép bởi chủ sở hữu thiết bị cho nền tảng. Chức năng kiểm soát truy cập được đề xuất có thể áp dụng triển khai đối với các hệ thống ghi hình (từ này viết là Camera) trong các khu vực công cộng của hệ thống nhà thông minh/thành phố thông minh. Bên cạnh đó, luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner nhằm phát hiện sớm các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng. Nền tảng bảo mật được đề xuất có thể áp dụng cho một mạng IoT với các thiết bị có đặc tính kết nối thông qua công nghệ IP, tầng ứng dụng trong kiến trúc IoT sẽ được dùng để xây dựng các ứng dụng phục vụ tương tác với các chức năng bảo mật được cung cấp trong nền tảng.

3.2. Các mục tiêu cụ thể

- ✓ Nghiên cứu lý thuyết về công nghệ Blockchain, các loại mạng Blockchain và các giao thức đồng thuận. Tìm hiểu các nền tảng bảo mật dựa trên Blockchain cho IoT, phân tích các ưu và nhược điểm của chúng. Từ đó đề xuất một nền tảng bảo mật tốt hơn cho IoT.
- ✓ Nghiên cứu lý thuyết về hệ thống lưu trữ phi tập trung IPFS, phương thức chữ ký nhóm. Từ đó đề xuất phương thức lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo tính riêng tư. Hai phương thức này là hai chức năng trong nền tảng bảo mật được đề xuất.
- ✓ Đề xuất giải pháp kiểm soát truy cập theo thời gian được cấp phép bởi chủ sở hữu thiết bị, giải pháp này là một chức năng của nền tảng bảo mật được đề xuất. Áp dụng giải pháp này để kiểm soát truy cập cho hệ thống Camera công cộng trong hệ thống nhà thông minh/thành phố thông minh để đánh giá tính hiệu quả và an toàn bảo mật của giải pháp.

- ✓ Đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner trong nền tảng bảo mật được đề xuất, nhằm phát hiện sớm các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng.

4. ĐỐI TƯỢNG VÀ PHẠM VI NGHIÊN CỨU

Nghiên cứu về công nghệ Blockchain, các giao thức đồng thuận, các loại mạng Blockchain, phương thức chữ ký nhóm và IPFS. Từ đó đề xuất một nền tảng bảo mật mới cho IoT; đề xuất chức năng lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo tính riêng tư cho nền tảng bảo mật; đề xuất chức năng kiểm soát truy cập dựa trên thời gian được cấp phép cho nền tảng bảo mật.

5. PHƯƠNG PHÁP NGHIÊN CỨU

Luận án sử dụng phương pháp nghiên cứu phân tích, đánh giá và tổng hợp trên các kết quả nghiên cứu đã có. Từ đó đề xuất hướng giải quyết và cách tiếp cận của luận án, sau đó thực hiện so sánh, thử nghiệm và đánh giá kết quả. Cụ thể như sau:

- ✓ Phân tích và đánh giá các nền tảng bảo mật dựa trên Blockchain cho IoT.
- ✓ Phân tích và đánh giá các công trình nghiên cứu liên quan đến phương thức lưu trữ, chia sẻ dữ liệu, và kiểm soát truy cập dựa trên Blockchain cho IoT.
- ✓ Tổng hợp các phân tích và đánh giá từ các nghiên cứu đã khảo sát, từ đó đề xuất một nền tảng bảo mật mới tối ưu hơn so với các nền tảng bảo mật đã khảo sát.
- ✓ Thực hiện so sánh, thử nghiệm và đánh giá nền tảng bảo mật được đề xuất.

6. NHỮNG ĐÓNG GÓP CHÍNH CỦA LUẬN ÁN

Sau đây là những đóng góp chính của luận án:

(i) Đề xuất một nền tảng bảo mật dựa trên Blockchain cho IoT. Trong đó, quy trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain dựa trên hai trường hợp về các Miner trong một mạng Blockchain: trường hợp 1, tất các Miner trong một mạng Blockchain đều hoàn toàn tin cậy; trường hợp 2, trong một mạng Blockchain có tồn tại một số Miner không đáng tin cậy nhưng số lượng ít hơn 1/3 trong tổng số các Miner trong mạng. Quá trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của các Miner trong nền tảng bảo

mật được đề xuất bao gồm hai giai đoạn: giai đoạn xác minh và giai đoạn tạo khối. Trong giai đoạn xác minh, các giao dịch được xác minh bởi một số lượng Miner nhất định tùy thuộc vào từng trường hợp nêu trên. Trong giai đoạn tạo khối, một Miner được lựa chọn sẽ đặt các giao dịch hợp lệ vào một khối mới, sau đó tạo chữ ký số trên khối mới này. Chữ ký số cùng với khối này sẽ được quảng bá đến các Miner khác trong mạng. Nếu khối mới này và chữ ký số hợp lệ, các Miner sẽ lưu khối này vào trong sổ cái của chúng. Nền tảng này mang lại sự tối ưu về mặt hiệu năng cho các Miner trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain, đồng thời có tính mở để có thể dễ dàng tích hợp thêm nhiều chức năng bảo mật vào trong nền tảng. Đóng góp này được công bố ở công trình [CT3] trong danh mục các công trình nghiên cứu của tác giả. Ngoài ra, luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner trong nền tảng bảo mật được đề xuất, giải pháp này nhằm phát hiện sớm các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng. Từ đó sẽ có cơ chế phù hợp để hạn chế ảnh hưởng xấu của chúng. Đóng góp này được công bố ở công trình [CT7] trong danh mục các công trình nghiên cứu của tác giả.

(ii) Đề xuất phương thức lưu trữ và chia sẻ dữ liệu đảm bảo tính riêng tư. Hai phương thức này là hai chức năng trong nền tảng bảo mật được đề xuất. Trong phương thức lưu trữ dữ liệu, sau khi dữ liệu thô được số hóa và cấp chứng chỉ bởi một tổ chức uy tín để trở thành một dữ liệu số có giá trị. Người sở hữu có thể lưu trữ các dữ liệu có giá trị lên một hệ thống lưu trữ an toàn. Trong giải pháp này, luận án sử dụng IPFS để lưu các dữ liệu số có giá trị. Trong khi các thông tin về địa chỉ truy cập của dữ liệu trên IPFS, chứng chỉ của dữ liệu và một số thông tin khác sẽ được lưu trên sổ cái Blockchain của nền tảng bảo mật được đề xuất. Trong phương thức chia sẻ dữ liệu, từ các thông tin được công bố trên Blockchain từ người sở hữu dữ liệu, mọi người trên hệ thống đều có thể kiểm chứng được tính tin cậy và tính chính xác của dữ liệu nhưng không thể hiểu được nội dung của dữ liệu chia sẻ. Quá trình chia sẻ dữ liệu sẽ được

thực hiện một cách chủ động, chính xác, minh bạch và công bằng thông qua một hợp đồng thông minh được triển khai trên Blockchain. Hai phương thức này đạt được các tính chất bảo mật: tính bí mật, tính toàn vẹn, tính riêng tư, tính chống chối bỏ và tính ẩn danh. Đóng góp này được công bố ở công trình [CT1] và [CT4] trong danh mục các công trình nghiên cứu của tác giả.

(iii) Đề xuất giải pháp kiểm soát truy cập dựa trên thời gian được cấp phép cho IoT. Giải pháp này là một chức năng của nền tảng bảo mật được đề xuất. Điểm khác biệt của giải pháp này so với các giải pháp kiểm soát truy cập dựa trên Blockchain khác đó là: khi nhận được một giao dịch yêu cầu truy cập đến một thiết bị IoT, người sở hữu có thể cấp phép một khoảng thời gian truy xuất nhất định cho người yêu cầu truy cập. Khi hết khoảng thời gian được cấp phép, kết nối sẽ tự động bị loại bỏ mà không cần người sở hữu thực hiện thêm bất kỳ giao dịch thu hồi quyền truy cập nào. Đóng góp này được công bố ở công trình [CT2] trong danh mục các công trình nghiên cứu của tác giả.

7. CẤU TRÚC LUẬN ÁN

Luận án được tổ chức thành 4 chương và phần kết luận. Chương 1 trình bày tổng quan về nền tảng bảo mật cho IoT, một số khái niệm, tổng quan về công nghệ Blockchain, khảo sát các nghiên cứu liên quan đến các nền tảng bảo mật dựa trên Blockchain cho IoT. Khảo sát các giải pháp kiểm soát truy cập, giải pháp lưu trữ và chia sẻ dữ liệu dựa trên Blockchain. Trên cơ sở đó, luận án đề xuất một nền tảng đảm bảo an toàn bảo mật mới đảm bảo tối ưu hiệu năng cho các Miner trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain. Nền tảng được đề xuất cung cấp các chức năng như: kiểm soát truy cập, lưu trữ dữ liệu và chia sẻ dữ liệu.

Chương 2 trình bày kiến trúc, quy trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của các Miner trong nền tảng bảo mật được đề xuất. Trong đó, quá trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái dựa trên hai trường hợp về các Miner trong một mạng Blockchain. Luận án so sánh tốc độ xác minh giao dịch và thời gian Mining trung bình một khối mới của nền tảng bảo mật được đề xuất với các nền tảng bảo mật tương tự đã khảo sát dựa trên thuật toán và thực nghiệm. Để

phát hiện sớm các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng, luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner của nền tảng bảo mật được đề xuất.

Chương 3 trình bày hai chức năng lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo tính riêng tư của nền tảng bảo mật được đề xuất. Trong đó, luận án sử dụng phương thức chữ ký nhóm, nền tảng bảo mật được đề xuất ở Chương 2 và IPFS để thiết kế hai chức năng này. Luận án trình bày mô hình hệ thống, các tính năng bảo mật, chi tiết về phương thức lưu trữ và chia sẻ dữ liệu, tiến hành phân tích và đánh giá các ưu điểm và các tính chất bảo mật đạt được của hai chức năng được đề xuất.

Chương 4 trình bày chức năng kiểm soát truy cập dựa trên thời gian được cấp phép của nền tảng bảo mật được đề xuất. Chức năng này được áp dụng trong ngữ cảnh kiểm soát truy cập cho hệ thống Camera công cộng của hệ thống nhà thông minh/thành phố thông minh. Trong đó, quy trình đăng ký thiết bị, đăng ký truy cập và cấp phép truy cập vào thiết bị được thực hiện thông qua các giao dịch Blockchain của nền tảng bảo mật được đề xuất ở Chương 2. Các kết nối sẽ tự động bị loại bỏ khi hết thời gian được cấp phép mà không cần người sở hữu thiết bị thực hiện thêm bất kỳ giao dịch thu hồi quyền truy cập nào.

Trong phần kết luận, luận án trình bày những kết quả đạt được và định hướng phát triển cho nghiên cứu tương lai khi áp dụng kết quả luận án vào thực tiễn.

CHƯƠNG 1. TỔNG QUAN VỀ NỀN TẢNG BẢO MẬT DỰA TRÊN BLOCKCHAIN CHO IoT

Nội dung của chương này trình bày tính cấp thiết của việc xây dựng một nền tảng bảo mật dựa trên Blockchain cho IoT, các khái niệm liên quan, tổng quan về công nghệ Blockchain. Bên cạnh đó, luận án khảo sát các công trình nghiên cứu liên quan đến các nền tảng bảo mật dựa trên Blockchain cho IoT. Khảo sát các nghiên cứu về lưu trữ và chia sẻ dữ liệu, kiểm soát truy cập dựa trên Blockchain. Từ đó, luận án xác định các điểm hạn chế của các công trình nghiên cứu đã khảo sát và đề xuất hướng nghiên cứu của luận án. Chương này được tổng hợp từ các công trình [CT2], [CT3], [CT4], và [CT5] trong danh mục các công trình nghiên cứu của tác giả.

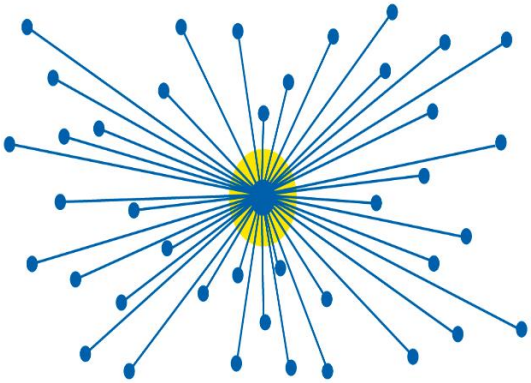
1.1. GIỚI THIỆU

Trong thời đại công nghệ số đang phát triển mạnh mẽ như hiện nay, số lượng và chủng loại các thiết bị IoT được đưa vào sử dụng ngày càng nhiều. Với sự đa dạng các tiện ích mà chúng mang lại, các thiết bị IoT là một thành phần không thể thiếu trong các hệ thống nhà thông minh/thành phố thông minh. Theo dự báo từ tập đoàn dữ liệu quốc tế IDC đến năm 2025 có khoảng 41,6 tỉ thiết bị sẽ được kết nối Internet, tổng số dữ liệu trên toàn thế giới được tạo ra từ các thiết bị IoT là 79,4 Zettabytes [56]. Đi kèm với sự phát triển của IoT, vấn đề nâng cao an toàn bảo mật cho IoT là vô cùng quan trọng, giúp cho sự phát triển đó trở nên vững chắc và tin cậy hơn.

Hầu hết các thiết bị IoT có đặc điểm chung là khả năng tính toán và dung lượng lưu trữ bị hạn chế, làm cho việc triển khai các giải pháp bảo mật cho từng thiết bị trong mạng gặp rất nhiều khó khăn và đôi khi không khả thi. Xây dựng một nền tảng bảo mật cho IoT là giải pháp khả thi hơn và đang thu hút nhiều sự quan tâm của nhiều nhóm nghiên cứu. Sử dụng một nền tảng bảo mật cho một mạng IoT mà không phụ thuộc vào bất kỳ chủng loại thiết bị IoT nào trong mạng và có thể dễ dàng tích hợp các chức năng bảo mật mới mà không cần thay đổi kiến trúc mạng IoT là một bài toán quan trọng đặt ra hiện nay.

Hiện tại, các nền tảng bảo mật cho IoT có thể được chia thành hai nhóm chính: (1) nhóm các nền tảng bảo mật dựa trên kiến trúc tập trung; và (2) nhóm các nền tảng bảo mật dựa trên kiến trúc phi tập trung.

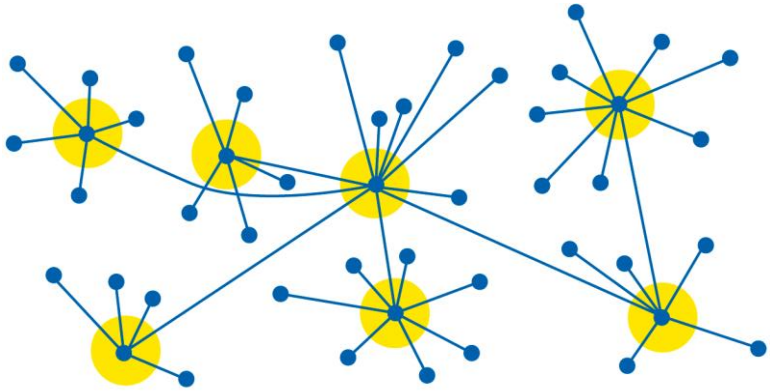
Trong các nền tảng bảo mật dựa trên kiến trúc tập trung, một Node trung tâm sẽ chịu trách nhiệm chính trong việc cung cấp dịch vụ cho toàn mạng và tất cả các Node khác sẽ gửi yêu cầu đến Node trung tâm này để sử dụng dịch vụ. Kiến trúc tập trung được thể hiện ở Hình 1.1. Ưu điểm của các nền tảng này là dễ dàng cài đặt, độ trễ và chi phí triển khai thấp, chúng rất thích hợp với các mạng IoT có kích thước nhỏ và ít có nhu cầu mở rộng. Một số giải pháp điển hình của nhóm giải pháp này được giới thiệu trong các công trình nghiên cứu [3][8][39]. Tuy nhiên, các nền tảng bảo mật tập trung có ba hạn chế [64][67]: (1) *Bảo mật dữ liệu*, tất cả dữ liệu được lưu trữ tại Node trung tâm, chúng có thể bị thay đổi hoặc xóa bởi bất kỳ người nào kiểm soát được Node này; (2) *Tính sẵn sàng*, trong trường hợp Node trung tâm ngừng hoạt động có thể do một trong các nguyên nhân như: hệ thống bị quá tải, bị tấn công từ chối dịch vụ, bị lỗi hệ thống. Khi đó, tất cả các Node khác trong mạng không thể truy cập và sử dụng dịch vụ của hệ thống; và (3) *Quản lý, cấu hình và khả năng mở rộng*, khi số lượng thiết bị và tài nguyên IoT tăng lên đáng kể, các vấn đề liên quan đến quản trị, cấu hình và khả năng mở rộng cho hệ thống trở nên phức tạp hơn.



Hình 1.1: Kiến trúc tập trung [71]

Trong các nền tảng bảo mật dựa trên kiến trúc phi tập trung, không một Node nào đóng vai trò là Node trung tâm trong mạng. Khi một Node ngưng hoạt động, các dịch vụ của hệ thống sẽ được duy trì bởi các Node khác trong mạng. Do đó, chúng có

thể hạn chế được các hình thức tấn công bảo mật nhằm vào tính sẵn sàng của hệ thống. Bên cạnh đó, việc mở rộng hệ thống sẽ rất dễ dàng khi chỉ cần thiết lập thông số cấu hình cho các Node mới để tham gia vào hệ thống. Kiến trúc phi tập trung được thể hiện ở Hình 1.2. Hầu hết các nền tảng bảo mật dựa trên kiến trúc phi tập trung đều sử dụng công nghệ Blockchain làm thành phần chính trong hệ thống bởi các ưu điểm mà công nghệ này mang lại như: *tính ẩn danh, tính minh bạch, tính phi tập trung*, và *tính kiểm toán* [1][70].



Hình 1.2: Kiến trúc phi tập trung [71]

Ở Việt Nam, đã có một số nhóm tác giả nghiên cứu áp dụng Blockchain vào IoT. Một số nghiên cứu điển hình như: nhóm tác giả trong nghiên cứu [51] sử dụng công nghệ Blockchain để nâng cao bảo mật trong việc quản lý chia sẻ dữ liệu IoT. Trong đó, nhóm tác giả sử dụng một thuật toán mật mã để bảo vệ tính bí mật cho dữ liệu IoT; nghiên cứu [14] áp dụng Blockchain để bảo vệ tính riêng tư của dữ liệu trong nhà thông minh thông, nhóm tác giả triển khai các chính sách kiểm soát truy cập dữ liệu IoT thông qua các hợp đồng thông minh trên Ethereum Blockchain; Trong nghiên cứu [18], các tác giả đề xuất B-DAC dựa trên Blockchain, nền tảng này có thể được sử dụng để xác thực thiết bị IoT. Nhóm tác giả trong nghiên cứu [58] sử dụng Blockchain để truy xuất nguồn gốc nông sản, trong đó các cảm biến của các thiết bị IoT sẽ thu thập và gửi thông tin lên Blockchain.

Với xu thế phát triển của IoT như hiện nay, việc sử dụng các một nền tảng bảo mật dựa trên kiến trúc phi tập trung cho các mạng IoT có kích thước lớn với nhu cầu mở rộng cao là một giải pháp phù hợp. Do đó, luận án sẽ đề xuất một nền tảng bảo

mật dựa trên kiến trúc phi tập trung cho IoT với công nghệ Blockchain làm thành phần trung tâm.

Hiện tại, các nền tảng bảo mật dựa trên Blockchain cho IoT có hai hạn chế: (1) các Miner trong nền tảng chưa tối ưu hiệu năng trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain; và (2) hạn chế về số lượng chức năng bảo mật được cung cấp.

Về mô hình quản lý của một mạng IoT, thông thường một mạng IoT được quản lý bởi một hoặc một vài tổ chức. Trong trường hợp một mạng IoT được quản lý bởi một tổ chức, tổ chức này có thể xây dựng một Private Blockchain cho nền tảng bảo mật. Khi đó, người xây dựng mạng Blockchain hoàn toàn có thể chỉ định các Node với vai trò là Miner, các Miner này thường được bảo vệ bởi các giải pháp bảo mật nên chúng rất khó bị thỏa hiệp từ kẻ tấn công, do đó chúng còn được gọi là các Miner tin cậy. Trong trường hợp mạng IoT được quản lý bởi một vài tổ chức, có thể sử dụng một Consortium Blockchain cho nền tảng bảo mật. Trong mạng Blockchain này, bên cạnh các Miner được chỉ định, người xây dựng mạng Blockchain có thể cho phép một số lượng Miner nhất định từ các tổ chức thành viên (còn được gọi là Miner bên ngoài) tham gia vào hệ thống. Mặc dù các Miner bên ngoài được chủ sở hữu thông báo cho người xây dựng mạng Blockchain là đảm bảo an toàn bảo mật nhưng người xây dựng mạng cũng sẽ không thể tin tưởng những Miner này. Có thể xem xét trường hợp xấu nhất xảy ra đối với các Miner bên ngoài này là chúng có thể bị thỏa hiệp bởi kẻ tấn công. Vì vậy, các Miner này được gọi là không tin cậy, vì kẻ tấn công hoàn toàn có thể đặt các giao dịch không hợp lệ vào trong một khối mới, sau đó cho Miner này quảng bá khối mới này đến toàn mạng. Mục tiêu của kẻ tấn công có thể là đưa các giao dịch không hợp lệ lên sổ cái của các Miner nhằm đạt được lợi ích hoặc gây giảm hiệu suất của các Miner trong việc xác minh các khối không hợp lệ.

Xuất phát từ các hạn chế đã trình bày ở trên và mô hình quản lý của một mạng IoT, luận án nghiên cứu đề xuất một nền tảng bảo mật mới cho IoT đảm bảo tối ưu hiệu năng cho các Miner trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain. Đồng thời nền tảng cũng sẽ cung cấp các chức năng bảo mật như:

kiểm soát truy cập dựa trên thời gian được cấp phép bởi chủ sở hữu thiết bị, lưu trữ và chia sẻ dữ liệu đảm bảo tính riêng tư. Nền tảng được đề xuất sử dụng công nghệ Blockchain làm thành phần trung tâm; kết hợp với phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái dựa trên hai trường hợp về các Miner trong một mạng Blockchain. Trường hợp 1, tất cả các Miner trong một mạng Blockchain là hoàn toàn tin cậy, trường hợp này có thể được áp dụng đối với các mạng IoT được quản lý bởi một tổ chức. Trường hợp 2, một mạng Blockchain có tồn tại một số Miner không tin cậy nhưng số lượng ít hơn 1/3 trong tổng số các Miner trong mạng. Trường hợp này có thể được áp dụng đối với các mạng IoT được quản lý bởi một vài tổ chức và số lượng Miner bên ngoài được phép tham gia vào mạng sẽ ít hơn 1/3 trong tổng số các Miner trong mạng.

Con số 1/3 được luận án sử dụng bắt nguồn từ bài toán Byzantine, hay còn được gọi là Byzantine Broadcast, được Lamport và các cộng sự đặt ra [32], bài toán này đã đặt nền tảng cho sự phát triển của giao thức đồng thuận phân tán. Bài toán Byzantine như sau: một số sư đoàn của Byzantine cắm trại bên ngoài một thành phố của đối phương, mỗi sư đoàn được chỉ huy bởi một tướng lĩnh. Các tướng lĩnh chỉ có thể giao tiếp với nhau bằng sứ giả. Sau khi quan sát kẻ thù, họ phải quyết định một kế hoạch hành động chung. Tuy nhiên, một số tướng lĩnh có thể là kẻ phản bội, cố gắng ngăn cản các tướng trung thành đạt được thỏa thuận.

Giả sử rằng có n vị tướng, và một trong số đó được gọi là tướng chỉ huy. Vị tướng chỉ huy muốn đề xuất một mệnh lệnh là “Tấn Công” hoặc “Rút Lui” cho tất cả các tướng còn lại, sao cho: (1) Tất cả các tướng lĩnh trung thành đều đạt được một quyết định như nhau; và (2) Nếu tướng chỉ huy trung thành, thì tất cả các tướng trung thành sẽ tuân theo mệnh lệnh của tướng chỉ huy. Chú ý rằng, nếu tướng chỉ huy là trung thành thì vấn đề này trở nên tầm thường, khi đó tướng chỉ huy này có thể gửi lệnh của mình cho tất cả các tướng khác và tất cả các tướng khác có thể chỉ cần tuân theo. Tuy nhiên, tướng chỉ huy cũng có thể là kẻ phản bội, trong trường hợp này, tướng chỉ huy có thể đề xuất các mệnh lệnh khác nhau cho các tướng lĩnh khác nhau, do đó sẽ dẫn đến các quyết định không nhất quán.

Bài toán Byzantine ở trên tương tự với vấn đề về sự đồng thuận phân tán trong hệ thống máy tính phân tán, khi một số Node trong hệ thống có thể hoạt động theo cách tùy ý (có thể gọi các Node này là Node độc hại), các nút hoạt động chính xác (có thể gọi các Node này là Node tin cậy) vẫn cần phải đồng ý về một giá trị chung giữa chúng. Công trình nghiên cứu [22][50] đã chứng minh rằng trong một mô hình kênh được xác thực theo cặp mà không có bất kỳ giả định thiết lập nào, chẳng hạn như một hạ tầng khóa công khai, Byzantine Broadcast là không thể đạt được nếu vượt quá n/3 Node độc hại. Điều này có nghĩa là Byzantine Broadcast sẽ đạt được khi tổng số Node độc hại ít hơn 1/3 trong tổng số Node trong mạng.

Có thể xem các tướng lĩnh của quân đội Byzantine là các Miner trong một mạng Blockchain, các tướng lĩnh trung thành tương ứng với các Miner tin cậy và các tướng lĩnh là kẻ phản bội tương ứng với các Miner không tin cậy. Các Miner tin cậy sẽ đạt được sự đồng thuận trong việc tạo dữ liệu trên sổ cái Blockchain khi số lượng các Miner không tin cậy ít hơn 1/3 trong tổng số các Miner trong mạng.

Trong nền tảng bảo mật được đề xuất, các Miner đóng vai trò quan trọng trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain. Việc đảm bảo tính an toàn bảo mật cho các Node này sẽ giúp nâng cao tính ổn định của nền tảng. Vì vậy, luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner nhằm phát hiện sớm các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng.

1.2. MỘT SỐ KHÁI NIỆM

Trong luận án có sử dụng một số thuật ngữ có ý nghĩa như sau:

Khái niệm 1: ***Một nền tảng bảo mật*** *là một tập hợp gồm các chính sách, quy trình, công nghệ được xây dựng nhằm đảm bảo an toàn bảo mật cho hệ thống sử dụng nó.*

Khái niệm 2: ***Liên mạng vạn vật*** *(còn được gọi là IoT) là một mạng gồm nhiều thiết bị vật lý tham gia vào nhằm mục đích kết nối và trao đổi dữ liệu với các thiết bị và hệ thống khác thông qua Internet.*

Khái niệm 3: ***Node*** *là một máy tính, một server, hoặc một thiết bị IoT có thể kết nối vào Internet.*

Khái niệm 4: ***Miner*** *là một Node có khả năng tạo ra các khối mới trong sổ cái của một mạng Blockchain.*

Khái niệm 5: ***Sổ cái*** *trong công nghệ Blockchain là một cơ sở dữ liệu của một mạng Blockchain, lưu một chuỗi các khối đã được đồng thuận bởi các Miner trong một mạng Blockchain.*

Khái niệm 6: ***Giao thức đồng thuận*** *là một cơ chế mà tất cả các Miner tin cậy đều có cùng một quyết định (từ chối hoặc chấp nhận) một khối mới.*

Khái niệm 7: ***Mining*** *là quá trình các Miner sử dụng một giao thức đồng thuận để tạo một khối mới và lưu nó lên sổ cái Blockchain của chúng.*

Khái niệm 8: ***Giao dịch trong mạng Blockchain*** *là một cấu trúc dữ liệu bao gồm địa chỉ người gửi, địa chỉ người nhận, và nội dung giao dịch. Mỗi giao dịch được ký bằng phương thức chữ ký số của người thực hiện giao dịch.*

Khái niệm 9: ***Pool*** *là nơi chứa các giao dịch chưa được xác minh.*

Khái niệm 10: ***Hợp đồng thông minh*** *trong Blockchain là các mã lệnh được lưu trữ trên Blockchain và được tự động thực thi khi các điều khoản và điều kiện đã định trước được đáp ứng.*

Trong một mạng Blockchain, các Miner thường có hiệu năng tính toán cao và dung lượng lưu trữ lớn. Mỗi Miner sẽ có một Pool để lưu các giao dịch nhận được từ Node khác trong mạng quảng bá đến, đây chính là những giao dịch đang chờ được Miner xác minh để đưa vào sổ cái.

Một giao thức đồng thuận được sử dụng trong một mạng Blockchain nhằm đảm bảo chỉ có các khối hợp lệ mới có thể được lưu trên sổ cái Blockchain và đồng bộ dữ liệu trên sổ cái giữa các Miner. Về cơ bản, một giao thức đồng thuận hoạt động như sau: tại mỗi vòng Mining, một Miner được chọn sẽ xác minh các giao dịch nằm trong Pool của nó và đặt các giao dịch hợp lệ vào một khối mới, sau đó quảng bá khối mới này đến các Miner khác trong mạng. Sau khi nhận được một khối mới, các Miner

trong mạng xác minh tính hợp lệ của khối mới này, nếu khối hợp lệ sẽ lưu vào sổ cái của chúng, ngược lại loại bỏ khối mới này.

Trong phần tiếp theo sẽ trình bày tổng quan về công nghệ Blockchain và các nghiên cứu liên quan đến các nền tảng bảo mật dựa trên Blockchain cho IoT. Trong đó, luận án tập trung phân tích cơ chế đồng thuận được sử dụng và các chức năng bảo mật được cung cấp trong các nền tảng; các nghiên cứu liên quan đến giải pháp lưu trữ và chia sẻ dữ liệu dựa trên Blockchain; các nghiên cứu liên quan đến giải pháp kiểm soát truy cập dựa trên Blockchain. Từ đó làm cơ sở để thiết kế một nền tảng bảo mật mới với các chức năng bảo mật được tích hợp vào như: kiểm soát truy cập dựa trên thời gian được cấp phép bởi chủ sở hữu thiết bị, lưu trữ và chia sẻ dữ liệu đảm bảo tính riêng tư.

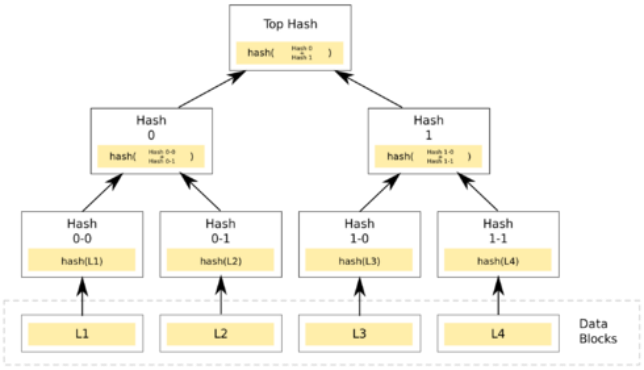
1.3. CÔNG NGHỆ BLOCKCHAIN

Blockchain được đề xuất đầu tiên vào năm 2008 bởi Satoshi Nakamoto [42], là một công nghệ chuỗi khối trong đó các khối được kết nối với nhau tạo thành một chuỗi dưới dạng một danh sách liên kết. Mỗi khối bao gồm phần Header lưu các thông tin quản lý của khối và chuỗi, phần Body chứa danh sách các giao dịch. Các khối liên kết với nhau thông qua một con trỏ băm chứa giá trị băm của khối trước đó được liên kết đến, giá trị băm này cũng được sử dụng để xác định tính toàn vẹn của khối. Khối đầu tiên trong chuỗi được gọi là khối Genesis, giá trị con trỏ băm của khối này sẽ được thiết lập bởi người xây dựng mạng Blockchain [1]. Một số trường thông tin có thể có trong phần Header của một khối bao gồm:

- *Phiên bản*: Thông tin về phiên bản của Blockchain.
- *Con trỏ băm*: Con trỏ băm chứa giá trị băm của khối phía trước được liên kết đến.
- *Nhãn thời gian*: Thời gian mà khối được tạo.
- *Số Nonce*: Giá trị được sử dụng trong giao thức đồng thuận PoW.
- *Giá trị Merkle root*: Trường này chứa một giá trị băm được tạo từ Merkle Tree. Cụ thể, Merkle Tree là một cấu trúc dữ liệu dạng cây, trong đó các giao dịch trong khối được xem như là các nút lá, giá trị băm của các nút lá được nhóm thành từng cặp. Giá trị băm được tạo tại mỗi cặp này sẽ được tiếp tục nhóm thành từng cặp

ở cấp cao hơn, quá trình này sẽ tiếp tục cho đến khi đạt được giá trị băm cuối cùng. Cấu trúc Merkle Tree được thể hiện ở Hình 1.3.

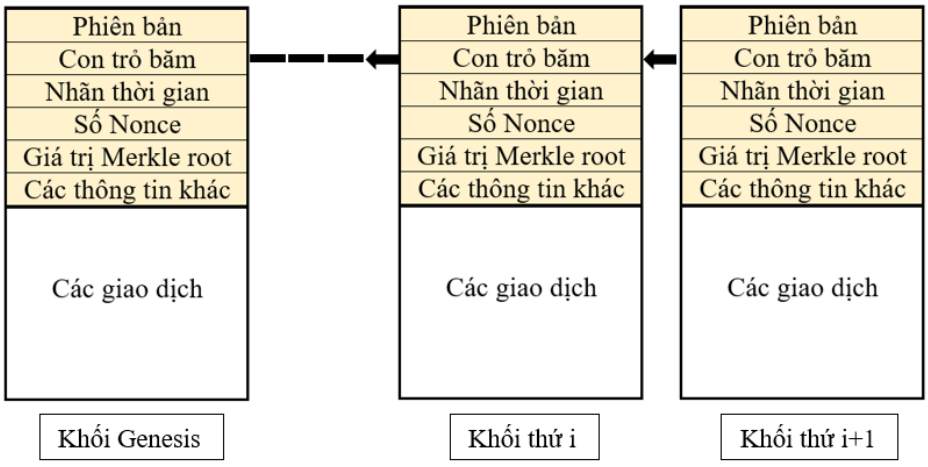
- *Các thông tin khác*: Tùy thuộc vào từng ứng dụng cụ thể mà người xây dựng mạng Blockchain có thể có thêm các trường thông tin khác trong phần Header.



Hình 1.3: Cấu trúc Merkle Tree [72]

Ví dụ về một Blockchain được thể hiện ở Hình 1.4.

Mạng Blockchain là một mạng ngang hàng, trong đó các Node trong mạng giao tiếp trực tiếp với nhau mà không cần phải thông qua bất kỳ hệ thống trung tâm nào. Mô hình mạng ngang hàng được thể hiện ở Hình 1.5.

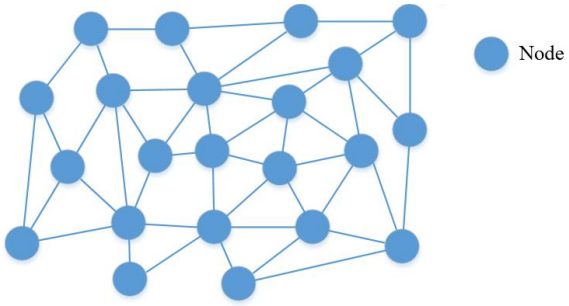


Hình 1.4: Ví dụ về một Blockchain

Có 2 loại Node trong một mạng Blockchain:

- *User Node (hoặc Normal Node)*: là các Node chỉ tham gia vào mạng Blockchain để thực hiện các giao dịch.
- *Miner Node:* là các Node giữ sổ cái, tham gia kiểm tra xác minh các giao dịch và cũng có thể thực hiện các giao dịch.

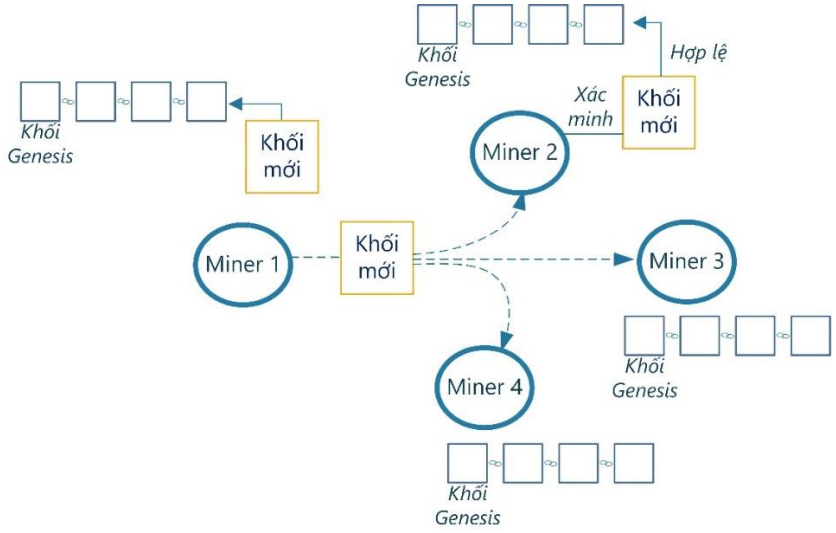
Mỗi Node tự tạo một khóa riêng và một khóa công khai tương ứng, và đăng ký khóa công khai cho hệ thống. Hệ thống cũng có thể cung cấp mã nguồn để người dùng có thể sử dụng hoặc người dùng có thể sử dụng một phần mềm riêng cùng tính chất. Trong đó, khóa công khai được dùng làm địa chỉ giao dịch trên mạng Blockchain của Node và được các Node khác sử dụng để xác minh chữ ký; khóa riêng được sử dụng để ký xác nhận trên các giao dịch do Node đó thực hiện. Các giao dịch sau khi được xác minh là hợp lệ bởi các Miner sẽ được lưu vào sổ cái của chúng. Dữ liệu trên sổ cái được cập nhật đồng bộ để đảm bảo giống nhau trên tất cả các Miner trong mạng thông qua một giao thức đồng thuận.



Hình 1.5: Mô hình mạng ngang hàng

1.3.1. Một số giao thức đồng thuận

Giao thức đồng thuận được sử dụng trong một mạng Blockchain để đồng bộ dữ liệu trên sổ cái giữa các Miner. Khi một Node trong mạng thực hiện một giao dịch Blockchain, giao dịch này sẽ được quảng bá đến các Miner trong mạng. Mỗi Miner sẽ lưu các giao dịch này vào trong Pool của nó. Tại mỗi vòng Mining, một Miner sẽ xác minh và đặt các giao dịch hợp lệ vào phần Body của một khối mới. Khối mới này sẽ được quảng bá đến các Miner khác trong mạng, đồng thời Miner này cũng sẽ lưu khối mới này vào trong sổ cái của nó. Sau khi nhận được khối mới này, các Miner xác minh tính hợp lệ của khối, nếu khối này hợp lệ các Miner sẽ thêm vào sổ cái của chúng. Quá trình đồng thuận dữ liệu trên sổ cái của các Miner trong một mạng Blockchain được thể hiện ở Hình 1.6. Trong đó, Miner 1 sẽ quảng bá một khối mới, Miner 2, Miner 3, và Miner 4 thực hiện xác minh khối mới này, nếu khối này hợp lệ sẽ thêm vào ví trí cuối cùng trong danh sách chuỗi khối của chúng.



Hình 1.6: Quá trình đồng thuận dữ liệu trên sổ cái

Một số giao thức đồng thuận thường được sử dụng trong một mạng Blockchain:

- *Proof-of-Work (PoW)[42]:* Các Miner được lựa chọn phải có nguồn lực tính toán lớn. Tại mỗi vòng Mining, các Miner sẽ phải cạnh tranh để giải và tìm ra một số Nonce sao cho khi băm mật mã toàn bộ khối mới kết hợp với số Nonce này sẽ cho ra một giá trị băm nhỏ hơn một giá trị mục tiêu đã được định trước:

$$H(Nonce||Khối\_mới) \leq Giá\_trị\_mục\_tiêu$$

  Trong đó, H là một hàm băm mật mã, ký hiệu $||$ là một phép nối chuỗi, *Giá_trị_mục_tiêu* là một giá trị băm mục tiêu.

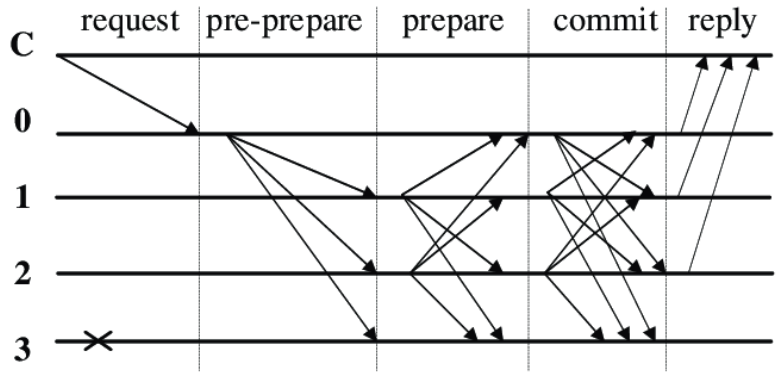
- *Proof-of-Stake (PoS)[70]:* Một Miner nắm giữ phần trăm của tổng giá trị mạng (hay còn gọi là cổ phần) đủ lớn sẽ có xác suất lớn được lựa chọn cho việc quảng bá một khối mới cho toàn mạng. Tùy thuộc vào từng ứng dụng mà giá trị "*Stake*" sẽ được xác định cụ thể.

- *Proof-of-Activity (PoA)[33]:* PoA là một giao thức lai giữa PoS và PoW, trong đó mỗi Miner cố gắng tạo ra một khối chỉ bao gồm các thông tin trong phần Header trong khi phần Body không chứa bất kỳ giao dịch nào, sao cho thỏa mãn yêu cầu cho trước theo giao thức PoW. Sau đó chuyển sang giao thức PoS, khối vừa tạo ra cần phải được ký bởi một số lượng nhất định các Miner nắm giữ cổ phần lớn trong mạng. Nếu khối vẫn chưa được ký đủ với số lượng chữ ký được

yêu cầu, sau một khoảng thời gian nhất định nó sẽ bị loại bỏ vì chưa hoàn thành. Khi đó, khối chiến thắng tiếp theo sẽ được lựa chọn để thực hiện công việc này.

- *Proof-of-Authentication (PoAh)[53]:* Ý tưởng cơ bản của giao thức PoAh là một User Node sẽ thu thập các giao dịch chưa được xác minh và đưa chúng vào một khối mới tại mỗi vòng Mining. Node này sẽ tạo chữ ký số trên khối mới này và quảng bá chúng lên mạng Blockchain. Sau khi nhận được một khối mới, một Miner tin cậy trong mạng sẽ xác minh tính hợp lệ của khối này, nếu khối hợp lệ thì Miner này sẽ thêm khối mới này vào sổ cái của nó. Đồng thời Miner này cũng sẽ đính kèm định danh của nó vào khối này, sau đó quảng bá chúng lên mạng Blockchain. Các Miner khác trên mạng kiểm tra định danh của Miner trong khối mới này, nếu thông tin định danh là hợp lệ sẽ thêm khối này vào sổ cái của chúng, ngược lại sẽ loại bỏ khối mới này.
- *Delegated Proof of Stake (DPoS)[34]:* Tại mỗi vòng Mining, mỗi Node trên mạng có trách nhiệm bỏ phiếu cho một Miner đáng tin cậy của mình. Một Miner sở hữu nhiều cổ phần trong mạng Blockchain sẽ có tỉ lệ cao được bỏ phiếu từ các Node khác để thực hiện công việc tạo và quảng bá một khối mới cho toàn mạng. Nếu một Miner không thể thực hiện công việc được giao trong một khoảng thời gian quy định, nhiệm vụ Mining sẽ được thực hiện bởi Miner có số lượng phiếu bầu cao kế tiếp.
- *Practical Byzantine Fault Tolerance (PBFT)[58]:* Giao thức PBFT được sử dụng cho các mạng Blockchain có tồn tại một số Miner không tin cậy với số lượng ít hơn 1/3 trong tổng số các Miner trong mạng. Giao thức PBFT được thể hiện ở Hình 1.7, bao gồm 3 giai đoạn xử lý như sau: giai đoạn 1 có tên gọi là Pre-prepared, một Miner được lựa chọn sẽ xác minh và chuyển các giao dịch hợp lệ trong Pool của mình vào một khối mới, sau đó quảng bá khối mới này đến các Miner khác trong mạng; giai đoạn 2 có tên gọi là Prepared, mỗi Miner sẽ quảng bá một phiếu cho khối mới này nếu khối đó hợp lệ; giai đoạn 3 có tên gọi là Commit, khi một Miner nhận được ít nhất 2/3 số phiếu trong tổng số các Miner trong mạng, Miner đó sẽ quảng bá một cam kết cho khối mới này. Các Miner sẽ

chấp nhận khối mới này nếu đã nhận được ít nhất 2/3 số cam kết trong tổng số các Miner trong mạng.



Hình 1.7: Quá trình xử lý của giao thức PBFT [11]

- *Tendermint [31]:* Quá trình xử lý của giao thức này bao gồm ba giai đoạn: Prevote, Precommit và Commit. Nhìn chung, các hoạt động trong 3 giai đoạn này tương tự như 3 giai đoạn trong giao thức PBFT. Tuy nhiên, mỗi giao thức sử dụng các kỹ thuật khác nhau cho mỗi giai đoạn. Một điểm khác biệt nữa của giao thức Tendermint so với giao thức PBFT là Miner sẽ phải ký quỹ một số tiền nhất định khi tham gia vào quá trình Prevote để khuyến khích tính trung thực.

1.3.2. Các loại mạng Blockchain

Có 3 loại mạng Blockchain [9]: *Public Blockchain*, *Private Blockchain*, và *Consortium Blockchain*.

- *Public Blockchain:* Loại mạng Blockchain này cho phép các Node trên thế giới đều có thể tham gia để thực hiện các giao dịch, xem nội dung các giao dịch trên sổ cái và cũng có thể tham gia vào quá trình Mining.
- *Private Blockchain:* Một Private Blockchain được xây dựng và quản lý bởi một tổ chức, do đó quá trình Mining sẽ được thực hiện bởi các Miner của tổ chức đó. Quyền đọc các giao dịch trên sổ cái có thể được công khai hoặc bị giới hạn tùy theo chính sách của tổ chức.
- *Consortium Blockchain:* Loại mạng Blockchain này được xây dựng và quản lý bởi một nhóm các tổ chức. Quá trình Mining được kiểm soát bởi một tập hợp các Miner được chỉ định trước, mỗi tổ chức có thể vận hành một hoặc một vài Node

với vai trò là Miner. Số lượng các Miner phụ thuộc vào kích thước của mạng Blockchain. Quyền đọc các giao dịch trên sổ cái có thể được công khai hoặc bị hạn chế đối với các bên tham gia.

1.3.3. Các hình thức tấn công bảo mật trên Blockchain

Các hình thức tấn công có thể xảy ra trên một mạng Blockchain bao gồm:

- *Tấn công 51 phần trăm:* Dựa trên đặc trưng của giao thức đồng thuận PoW, các Miner có hiệu năng tính toán lớn trong mạng sẽ có xác suất rất cao để tìm ra số Nonce hợp lệ so với các Miner khác trong mạng. Do đó, khi một Miner nắm giữ 51 phần trăm năng lực tính toán so với toàn mạng sẽ chi phối quá trình tạo khối trên sổ cái Blockchain [18]. Khi đó, Miner này có thể thực hiện các hình thức tấn công như: Double Spending, Selfish Mining. Để giảm thiểu hình thức tấn công này, các tác giả trong công trình nghiên cứu [4] đề xuất sử dụng phương thức Two-phase Proof of Work, Bae và cộng sự đề xuất sử dụng kỹ thuật lựa chọn một Miner ngẫu nhiên trong danh sách các Miner cho việc đề xuất một khối mới tại mỗi vòng Mining [2].
- *Tấn công Double Spending:* Hình thức tấn công này có thể xảy ra đối với các ứng dụng tiền điện tử sử dụng công nghệ Blockchain. Trong đó, một Node dùng cùng một đơn vị tiền điện tử để chi trả trong hai giao dịch khác nhau. Để ngăn chặn hình thức tấn công này, các tác giả trong công trình nghiên cứu [42] đề xuất sử dụng giao thức đồng thuận PoW và dịch vụ nhãn thời gian phân tán. Karame và cộng sự đề xuất 3 kỹ thuật có tên là Listening Period, Inserting Observers và Forwarding Double-Spending để nhanh chóng phát hiện và ngăn chặn các cuộc tấn công Double Spending trong các hệ thống yêu cầu thực hiện thanh toán trong khoảng thời gian rất ngắn [29]. Nhóm nghiên cứu của Yu đề xuất mỗi người dùng phải gửi tiền ký quỹ để khuyến khích tính trung thực khi thực hiện các giao dịch Blockchain [66].
- *Tấn công Eclipse:* Trong hình thức tấn công Eclipse, kẻ tấn công kiểm soát tất cả các kết nối đến và đi của một Node nạn nhân. Do đó, kẻ tấn công có thể lọc các giao dịch của nạn nhân hoặc có thể thực hiện các cuộc tấn công Double Spending,

Selfish Mining [25]. Các tác giả trong công trình nghiên cứu [25] đề xuất 10 kỹ thuật đối phó với hình thức tấn công này đó là: Deterministic Random Eviction, Random Selection, Test Before Evict, Feeler Connections, Anchor Connections, More Buckets, More Outgoing Connections, Ban Unsolicited ADDR Messages, Diversify Incoming Connections, và Anomaly Detection.

- *Tấn công Selfish Mining:* Khi một Miner Mining ra một khối mới, nó lưu khối này vào trong sổ cái của nó mà không quảng bá khối này cho toàn mạng, trong khi đó các Miner khác vẫn đang tiến hành Mining để tìm khối mới. Sau đó, Miner này tiếp tục Mining để có được thêm khối mới thứ 2. Khi Miner này đã có hai khối mới, nó sẽ quảng bá hai khối mới này cho toàn mạng. Kết quả là làm lãng phí sức mạnh tính toán của các Miner khác trong mạng [18]. Để phòng chống hình thức tấn công này, các tác giả trong công trình nghiên cứu [24] đề xuất phương thức Freshness Preferred, Zhang và cộng sự đề xuất cơ chế tương thích ngược [68].
- *Tấn công từ chối dịch vụ:* Kẻ tấn công sử dụng các User Node để gửi rất nhiều giao dịch không hợp lệ đến các Miner. Mục tiêu của cuộc tấn công này là làm giảm hiệu năng hoặc có thể gây gián đoạn hoạt động của toàn mạng [60]. Bentov và cộng sự đề xuất sử dụng giao thức đồng thuận Proof-of-Activity để giảm thiểu hình thức tấn công này [7].

Nội dung được trình bày trong Mục 1.3 được công bố trong công trình [CT3] và [CT5] trong danh mục các công trình nghiên cứu của tác giả.

1.4. KHẢO SÁT CÁC NỀN TẢNG BẢO MẬT CHO IoT

Các nền tảng bảo mật bên cạnh việc cung cấp các tiện ích cho người sử dụng, còn giúp giảm thiểu tối đa các hình thức tấn công bảo mật vào IoT. Luận án tập trung phân tích một số nền tảng bảo mật dựa trên Blockchain cho IoT dựa trên hai đặc trưng: (1) các chức năng mà nền tảng cung cấp; và (2) giao thức đồng thuận được sử dụng. Từ đó làm cơ sở để đề xuất một nền tảng bảo mật mới cũng như để so sánh giữa nền tảng bảo mật được đề xuất của luận án với các nghiên cứu liên quan đã khảo sát.

Nền tảng bảo mật FairAccess cung cấp chức năng kiểm soát truy cập đảm bảo tính riêng tư cho IoT [46]. Trong đó, để truy cập đến một tài nguyên trong mạng, người yêu cầu truy cập phải gửi yêu cầu đến chủ sở hữu tài nguyên. Sau đó, chủ sở hữu sẽ định nghĩa các chính sách kiểm soát truy cập thông qua một giao dịch Blockchain và quảng bá giao dịch này lên mạng Blockchain. Giao dịch này được xem là hợp lệ khi thỏa mãn 3 điều kiện sau: (1) chữ ký của người thực hiện giao dịch là hợp lệ; (2) dữ liệu trong giao dịch phải đảm bảo tính toàn vẹn; (3) các chính sách cấu hình trong giao dịch phải đúng cú pháp. Các giao dịch hợp lệ sẽ được các Miner lưu vào sổ cái của chúng. Tuy nhiên, các tác giả chỉ đưa ra quy trình xác minh tính hợp lệ của các giao dịch nhưng chưa chỉ ra chi tiết cách đồng thuận dữ liệu trên sổ cái Blockchain giữa các Miner.

Nền tảng bảo mật được trình bày trong nghiên cứu [17] của Dorri và cộng sự đề xuất phương thức kiểm soát truy cập cho các thiết bị IoT trong hệ thống nhà thông minh. Quá trình xác minh các giao dịch và tạo khối trên sổ cái do một Miner thực hiện, do đó giao thức đồng thuận trong giải pháp này là PoS. Liu cùng các cộng sự [37] đề xuất một nền tảng đảm bảo tính toàn vẹn cho dữ liệu lưu trữ trên dịch vụ lưu trữ đám mây, nền tảng bảo mật này sử dụng Ethereum Blockchain.

Panda và các cộng sự [49] đề xuất nền tảng chứng thực cho các thiết bị IoT, nền tảng này sử dụng Ethereum Blockchain. Sheron và các cộng sự [55] đề xuất một nền tảng bảo mật cung cấp phương thức giao tiếp đảm bảo tính riêng tư và toàn vẹn trong môi trường IoT, nền tảng bảo mật này sử dụng giao thức đồng thuận PoW.

Nghiên cứu [30] giới thiệu một nền tảng giao tiếp đảm bảo an toàn bảo mật cho mạng IoT. Nền tảng này được triển khai trong mạng Consortium Blockchain và sử dụng thuật toán đồng thuận kết hợp. Nhìn chung, thuật toán đồng thuận này tương tự như giao thức đồng thuận PoS. Cụ thể, mỗi vùng mạng trong hệ thống Blockchain sẽ bầu chọn một Miner, khi một Node muốn gửi dữ liệu đến một Node khác, Node gửi sẽ phải thiết lập một giao tiếp bằng cách tạo một hợp đồng. Hợp đồng này sẽ phải trải một quá trình xác minh gồm 2 giai đoạn. Giai đoạn 1, Miner trong vùng mạng chịu trách nhiệm tạo chữ ký cho hợp đồng và chuyển tiếp hợp đồng đã ký cho các

Miner khác trong mạng Blockchain. Giai đoạn 2, các Miner trong mạng kiểm tra tính xác thực của hợp đồng nhận được, nếu chữ ký trên hợp đồng là hợp lệ thì một khối mới sẽ được tạo cho hợp đồng đã ký này.

Trong nền tảng phục vụ cho việc trao đổi dữ liệu IoT đảm bảo an toàn bảo mật được đề xuất bởi Singh và các cộng sự [57], các hợp đồng thông minh được sử dụng để quản lý thiết bị, quản lý dữ liệu trao đổi giữa nhà sản xuất dữ liệu và khách hàng, và để đánh giá chất lượng của dịch vụ. Tuy nhiên, các tác giả không đề cập cụ thể giao thức đồng thuận nào được sử dụng trong nền tảng được đề xuất của họ.

Hiện tại Ethereum Blockchain đang chuyển từ giao thức đồng thuận PoW sang PoS bởi vì giao thức đồng thuận PoW làm các Miner tốn nhiều năng lượng điện và tài nguyên tính toán [35]. Các mạng IoT thường được quản lý bởi một hoặc một vài tổ chức, do đó sử dụng mạng Private hoặc Consortium Blockchain có thể là lựa chọn phù hợp. Nghiên cứu [70] chỉ ra rằng việc sử dụng một trong các giao thức đồng thuận PBFT, Tendermint, và DPoS là phù hợp cho mạng Private và Consortium Blockchain. He Yi và cộng sự [65] cũng đề xuất sử dụng giao thức đồng thuận Tendermint cho mạng Private Blockchain. Các giao thức đồng thuận PBFT và Tendermint có thể được áp dụng cho một mạng Blockchain có tồn tại một số Miner không đáng tin cậy nhưng số lượng ít hơn 1/3 trong tổng số các Miner trong mạng. Trong khi đó, Deepak Puthal và các cộng sự [53] đề xuất sử dụng giao thức PoAh cho các mạng Blockchain cho IoT. Tuy nhiên, trong trường hợp một nền tảng bảo mật sử dụng một trong các giao thức đồng thuận PoW, PoS, PoAh, DPoS, PBFT, và Tendermint thì hiệu năng của các Miner vẫn chưa đạt được sự tối ưu trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain.

Nhận xét: Qua khảo sát một số nghiên cứu điển hình về nền tảng bảo mật dựa trên Blockchain cho IoT, các giải pháp này có hai hạn chế như sau:

(1) Hạn chế về các tính năng bảo mật được cung cấp.

(2) Các Miner chưa đạt được sự tối ưu trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain.

Do đó, luận án sẽ đề xuất một nền tảng bảo mật mới cho IoT với phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain đảm bảo tối ưu hiệu năng cho các Miner. Đồng thời nền tảng được đề xuất cung cấp các tính năng bảo mật như: kiểm soát truy cập cho IoT dựa trên thời gian được cấp phép bởi chủ sở hữu thiết bị, lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo tính riêng tư. Các khảo sát về các nền tảng bảo mật dựa trên Blockchain cho IoT trong mục này được công bố trong công trình [CT3] trong danh mục các công trình nghiên cứu của tác giả.

1.5. CÁC NGHIÊN CỨU VỀ LƯU TRỮ VÀ CHIA SẺ DỮ LIỆU

Nhu cầu lưu trữ và chia sẻ dữ liệu là vô cùng cần thiết trong các mạng IoT. Các giải pháp lưu trữ và chia sẻ dữ liệu ngang hàng hiện tại đều sử dụng Blockchain để quản lý thông tin của dữ liệu và để thực hiện các giao dịch. Vì các khối trong một Blockchain không thể chứa dữ liệu lớn (hàng chục/trăm Megabyte trở lên). Nếu kích thước khối lớn sẽ làm cho mạng Blockchain hoạt động không hiệu quả, bởi vì thời gian đồng bộ dữ liệu trên sổ cái sẽ rất chậm do độ trễ từ mạng và tốn nhiều nguồn lực tính toán của các Miner [14]. Do đó, các dữ liệu lớn phải được lưu trữ ở một hệ thống khác và các giao dịch Blockchain chỉ chứa các thông tin quản lý của dữ liệu như: địa chỉ truy cập của dữ liệu trên hệ thống lưu trữ, khóa giải mã, … Hệ thống lưu trữ dữ liệu để hỗ trợ cho Blockchain trong các giải pháp lưu trữ và chia sẻ dữ liệu hiện tại có thể được chia làm hai nhóm chính, đó là: (1) nhóm giải pháp sử dụng hệ thống lưu trữ tập trung; và (2) nhóm giải pháp sử dụng hệ thống lưu trữ phi tập trung.

❖ **Nhóm giải pháp sử dụng hệ thống lưu trữ tập trung**

Hầu hết các giải pháp lưu trữ tập trung đều sử dụng dịch vụ lưu trữ đám mây làm hệ thống lưu trữ, một số nghiên cứu tiêu biểu có thể kể đến là:

Qi Xia và các cộng sự đề xuất nền tảng chia sẻ dữ liệu dựa trên Blockchain cho hồ sơ bệnh án điện tử [63]. Mô hình hệ thống đề xuất bao gồm ba tầng: (1) tầng người dùng: là những cá nhân hoặc tổ chức muốn truy cập hoặc đóng góp dữ liệu để phục vụ cho mục đích nghiên cứu; (2) tầng quản lý hệ thống: chịu trách nhiệm thiết lập an toàn, vận hành hiệu quả, và tối ưu hóa chương trình. Tầng này bao gồm: người phát hành có trách nhiệm tiếp nhận các yêu cầu tham gia vào nhóm, xác thực người

dùng và chấp nhận người dùng vào nhóm hoặc từ chối quyền gia nhập của người dùng vào nhóm; người xác minh có trách nhiệm xác minh tư cách thành viên của người dùng trong nhóm, gửi khóa cá nhân thành viên đến các thành viên của nhóm, xác thực các khối đã được ký bởi người dùng; và các Consensus Node, có nhiệm vụ xử lý, xác minh tính xác thực và các chi tiết liên quan đến một khối; (3) tầng lưu trữ: sử dụng dịch vụ lưu trữ đám mây để lưu dữ liệu. Để truy xuất dữ liệu trên hệ thống, người dùng gửi một yêu cầu truy xuất thông qua một giao dịch Blockchain đến tầng quản lý hệ thống. Tầng quản lý hệ thống sẽ xác minh tính hợp lệ của yêu cầu, nếu yêu cầu là hợp lệ, nó sẽ thực hiện truy vấn dữ liệu đến tầng lưu trữ và chuyển kết quả truy vấn đến người dùng. Tuy nhiên, nền tảng này bị hạn chế về số lượng các đối tượng tham gia vào, vì chỉ những người dùng được cấp quyền mới có thể tham gia lưu trữ và truy cập các dữ liệu chia sẻ trên hệ thống. Bên cạnh đó, quá trình lưu trữ và chia sẻ dữ liệu vẫn chưa thực sự chủ động giữa các bên tham gia vì phải phụ thuộc vào người xác minh.

Trong công trình nghiên cứu của Xueping Liang và cộng sự [36], thông tin sức khỏe của người dùng sẽ được các thiết bị như: đồng hồ thông minh, thiết bị theo dõi hoạt động, máy đo nhịp tim, … gửi đến nhà cung cấp dịch vụ lưu trữ đám mây để lưu trữ. Dữ liệu của người dùng được đảm bảo tính toàn vẹn bằng cách sử dụng cấu trúc Merkle Tree. Người dùng có thể chia sẻ dữ liệu của mình với các nhà cung cấp dịch vụ chăm sóc sức khỏe và với các công ty bảo hiểm. Các yêu cầu truy cập và cập nhật dữ liệu sẽ được lưu lại trong các giao dịch Blockchain.

Liu và các cộng sự đề xuất giải pháp chia sẻ dữ liệu đảm bảo tính riêng tư dựa trên Blockchain cho bệnh án điện tử, giải pháp có tên là BPDS [38]. Kiến trúc của hệ thống này bao gồm 3 tầng: tầng thu thập dữ liệu; tầng lưu trữ dữ liệu; và tầng chia sẻ dữ liệu. Trong tầng thu thập dữ liệu, các bệnh án điện tử sẽ được tạo và được ký bởi các bác sĩ trước khi gửi chúng đến bệnh nhân. Bệnh nhân là người sở hữu dữ liệu nên có quyền chia sẻ bệnh án của mình đến những người hoặc tổ chức có nhu cầu sử dụng. Để bảo vệ thông tin riêng tư trong quá trình chia sẻ dữ liệu, bệnh nhân có thể xóa các thông tin nhạy cảm trên bệnh án điện tử của mình và tạo chữ ký trích xuất hợp lệ.

Tầng lưu trữ dữ liệu sử dụng dịch vụ lưu trữ đám mây để lưu bản mã hóa của bệnh án điện tử và chữ ký trích xuất, sử dụng một mạng Consortium Blockchain để lưu các chỉ mục của bệnh án điện tử và lưu các giao dịch chia sẻ dữ liệu. Bệnh nhân có thể định nghĩa các quyền truy cập dữ liệu trong các hợp đồng thông minh để đảm bảo chia sẻ dữ liệu được an toàn. Trong tầng chia sẻ dữ liệu, nhân viên y tế và cơ sở chăm sóc sức khỏe có thẩm quyền có thể yêu cầu truy cập bệnh án điện tử của bệnh nhân và sử dụng chúng để lập kế hoạch kiểm tra sức khỏe cá nhân, điều trị tại phòng khám tốt hơn hoặc thực hiện các nghiên cứu y tế. Tuy nhiên, giải pháp trong công trình nghiên cứu [36] và [38] không cung cấp phương thức để mọi người trên hệ thống có thể kiểm chứng tính chính xác và tính tin cậy của dữ liệu y tế trước khi gửi yêu cầu chia sẻ dữ liệu đến chủ sở hữu dữ liệu.

Nhóm nghiên cứu của Zheng đề xuất một hệ thống chia sẻ dữ liệu sức khỏe cá nhân sử dụng công nghệ Blockchain, lưu trữ đám mây và các kỹ thuật máy học [69]. Trong nghiên cứu này, thông tin sức khỏe cá nhân được nén và mã hóa trước khi lưu trữ trên hệ thống lưu trữ đám mây, khóa bí mật sau đó sẽ được chuyển từ người sở hữu dữ liệu đến người giữ khóa thông qua một kênh an toàn. Người sở hữu sẽ công khai thông tin chia sẻ thông qua một giao dịch Blockchain, khách hàng có thể tìm kiếm dữ liệu và có thể gửi yêu cầu mua dữ liệu thông qua một giao dịch Blockchain. Khóa giải mã cũng sẽ được người giữ khóa chuyển đến cho người mua thông qua một kênh an toàn. Tuy nhiên, giải pháp chia sẻ dữ liệu này vẫn chưa đạt được sự chủ động giữa các bên tham gia vì vẫn còn phụ thuộc vào một bên trung gian là người giữ khóa.

Nhóm nghiên cứu của Fan [20] đề xuất giải pháp MedBlock cho phép bệnh nhân có thể quản lý và chia sẻ dữ liệu từ các bệnh viện mà họ đã từng khám chữa bệnh. Trong giải pháp này một nhóm các bệnh viện sẽ tham gia vào hệ thống, bệnh án điện tử của bệnh nhân sẽ được lưu trong hệ thống lưu trữ của bệnh viện hoặc trên dịch vụ lưu trữ đám mây. Các thông tin bệnh án điện tử của bệnh nhân sẽ được công bố lên mạng Blockchain. Bệnh nhân có thể tải xuống bệnh án điện tử của mình từ các bệnh viện khác nhau, sau đó sử dụng khóa riêng để giải mã thông tin bệnh án. Tuy

nhiên, giải pháp này chỉ đưa ra phương thức lưu trữ dữ liệu đồng bộ và kiểm soát quyền truy cập từ người dùng ở các bệnh viện khác nhau.

❖ **Nhóm giải pháp sử dụng hệ thống lưu trữ phi tập trung**

Nhóm giải pháp lưu trữ phi tập trung có ưu điểm là không phụ thuộc bất kỳ vào một nhà cung cấp dịch vụ lưu trữ nào. Một số nền tảng lưu trữ phi tập trung như: IPFS, Storj, Swarm, Filecoin, … Trong đó, nền tảng IPFS được sử dụng trong nhiều nghiên cứu bởi đây là một giải pháp mã nguồn mở và chưa tích hợp thêm bất kỳ giao thức phụ nào khác để phục vụ cho mục đích thương mại. Cụ thể, các tác giả trong công trình nghiên cứu [61] đề xuất nền tảng chia sẻ dữ liệu phi tập trung sử dụng IPFS, Ethereum Blockchain, và mã hóa dựa trên thuộc tính.

Muqaddas Naz và cộng sự đề xuất nền tảng chia sẻ dữ liệu an toàn dựa trên Blockchain và IPFS [43]. Trong đó, dữ liệu sẽ được lưu trữ trên IPFS và địa chỉ truy cập của dữ liệu trên IPFS sẽ được mã hóa bằng khóa công khai của Worker Node. Quá trình chia sẻ dữ liệu từ người sở hữu đến khách hàng được thực hiện thông qua một hợp đồng thông minh, Worker Node là một bên trung gian cung cấp dịch vụ giải mã địa chỉ truy cập của dữ liệu trên IPFS và chuyển chúng đến khách hàng.

Nhóm tác giả trong công trình nghiên cứu [62] đề xuất giải pháp chia sẻ hồ sơ sức khỏe cá nhân an toàn dựa trên Blockchain và IPFS. Trong đó, hồ sơ sức khỏe cá nhân sẽ được mã hóa bởi một thuật toán mật mã đối xứng trước khi lưu trữ trên IPFS, các khóa bí mật được mã hóa bởi phương thức mã hóa dựa trên thuộc tính chính sách mã hóa (ciphertext-policy attribute-based encryption), và các hợp đồng thông minh được sử dụng để quản lý thông tin của dữ liệu và quản lý quá trình chia sẻ dữ liệu.

Makhdoom và cộng sự đề xuất giải pháp chia sẻ dữ liệu đảm bảo tính riêng tư có tên PrivySharing cho hệ thống thành phố thông minh [40]. Giải pháp tập trung vào việc đảm bảo tính bảo mật cho dữ liệu chia sẻ của người dùng và kiểm soát truy cập trên dữ liệu chia sẻ giữa các bên liên quan thông qua các chính sách kiểm soát truy cập được triển khai trong hợp đồng thông minh.

Trong nghiên cứu [26], các tác giả đề xuất giải pháp chia sẻ dữ liệu đảm bảo tính riêng tư dựa trên Blockchain cho các hệ thống lưu trữ phi tập trung. Nhóm tác

giả đề xuất sử dụng phương thức chữ ký vòng để đảm bảo tính ẩn danh của người dùng. Để truy cập dữ liệu trên IPFS, người dùng cần đáp ứng hai điều kiện: (1) người dùng phải sở hữu một khóa ẩn riêng tương ứng với một khóa công khai ẩn có trong danh sách kiểm soát truy cập ẩn liên quan của dữ liệu; (2) người dùng phải có một khóa riêng hợp lệ để giải mã dữ liệu.

Tuy nhiên, hạn chế của các giải pháp [26][40][43][61][62] là chưa cung cấp phương thức để người yêu cầu chia sẻ có thể kiểm chứng tính chính xác và tính tin cậy của dữ liệu trước khi gửi yêu cầu chia sẻ dữ liệu đến chủ sở hữu dữ liệu.

Nhận xét: Qua khảo sát các nghiên cứu điển hình về lưu trữ và chia sẻ dữ liệu dựa trên Blockchain, các giải pháp này chưa đáp ứng được tất cả các yêu cầu sau đây:

(1) Dữ liệu lưu trữ cần phải đảm bảo tính bí mật, tính toàn vẹn.

(2) Quá trình chia sẻ dữ liệu cần phải chủ động giữa người sở hữu và người yêu cầu chia sẻ.

(3) Cần cung cấp phương thức để mọi người trên hệ thống có thể kiểm chứng được tính chính xác và tính tin cậy của dữ liệu chia sẻ trước khi gửi yêu cầu chia sẻ đến chủ sở hữu dữ liệu.

Trong luận án sẽ đề xuất phương thức lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo các yêu cầu nêu trên. Đồng thời các phương thức đề xuất cũng sẽ đạt được tính riêng tư, tính chống chối bỏ, và tính ẩn danh. Hai phương thức này là hai chức năng trong nền tảng bảo mật được đề xuất. Các khảo sát một số nghiên cứu liên quan đến lưu trữ và chia sẻ dữ liệu dựa trên Blockchain cho IoT trong mục này được công bố trong công trình [CT4] trong danh mục các công trình nghiên cứu của tác giả.

1.6. CÁC NGHIÊN CỨU VỀ KIỂM SOÁT TRUY CẬP CHO IoT

Kiểm soát truy cập là một phương thức bảo mật để giám sát, cấp quyền hoặc từ chối quyền truy cập vào các tài nguyên IoT. Các giải pháp kiểm soát truy cập dựa trên Blockchain cho IoT có các ưu điểm như đảm bảo tính sẵn sàng và khả năng mở rộng của hệ thống.

Giải pháp bảo mật FairAccess cung cấp chức năng kiểm soát truy cập đảm bảo tính riêng tư cho IoT [46]. Trong đó, chủ sở hữu tài nguyên IoT sử dụng các hợp đồng

thông minh để thiết lập các chính sách bảo mật và phân phối các Token đến người yêu cầu truy cập tài nguyên IoT. Người yêu cầu truy cập sẽ sử dụng Token được cấp phát bởi chủ sở hữu tài nguyên để truy cập đến các tài nguyên được cấp phép. Bên cạnh đó, chủ sở hữu tài nguyên cũng có thể thực hiện các giao dịch GrantAccess để thu hồi hoặc cập nhật các quyền đã được cấp đến người yêu cầu truy cập.

Pinno và cộng sự đã chỉ ra các hạn chế của FairAccess liên quan đến tốn chi phí phân phối quyền truy xuất đến người yêu cầu truy cập và thiếu các chính sách liên quan đến các mối quan hệ giữa các đối tượng trong mạng [52]. Nhóm tác giả cũng đề xuất giải pháp ControlChain với 4 Blockchain được sử dụng có tên là Context, Relatoinships, Rules và Accountability. Trong đó, Context Blockchain được sử dụng để lưu trữ các thông tin ngữ cảnh thu được từ các cảm biến hoặc dữ liệu đã xử lý; Relatoinships Blockchain chịu trách nhiệm lưu trữ thông tin đăng nhập công khai và mối quan hệ của tất cả các thực thể trong hệ thống; Rules Blockchain lưu các quy tắc ủy quyền được xác định bởi chủ sở hữu; và Accountability Blockchain dùng để đăng ký thông tin về quyền hoặc từ chối quyền truy cập vào đối tượng.

Các tác giả trong nghiên cứu [17] sử dụng Blockchain để kiểm soát truy cập cho các thiết bị IoT trong hệ thống nhà thông minh. Trong kiến trúc đề xuất gồm có 3 tầng: (1) Smart Home: gồm các thiết bị IoT, một Blockchain nội bộ và một hệ thống lưu trữ nội bộ. Mỗi nhà thông minh sử dụng một hay nhiều thiết bị có hiệu năng tính toán cao (như máy chủ/máy trạm) đóng vai trò là Miner trong mạng Blockchain nội bộ. Miner có chức năng tạo giao dịch, xác thực, phân quyền, kiểm toán các giao dịch, phân phối và cập nhật khóa cho các thiết bị IoT trong hệ thống nhà thông minh. Người sở hữu có quyền thêm thiết bị IoT hoặc loại bỏ thiết bị IoT ra khỏi mạng Blockchain thông qua các giao dịch. Phần Header của mỗi khối chứa các chính sách điều khiển truy cập, cho phép chủ sở hữu kiểm soát các giao dịch xảy ra trong hệ thống nhà thông minh của họ. Giao tiếp giữa các thiết bị sẽ được bảo mật bằng khóa chia sẻ sử dụng thuật toán Diffie-Hellman. Ngoài ra, Miner kiểm soát các truy cập từ bên ngoài vào dữ liệu bên trong của nhà thông minh thông qua danh sách các khóa công khai đã được đăng ký; (2) Overlay Network: gồm các Miner của các nhà thông minh, các

thiết bị di động hoặc máy tính của người dùng; và (3) Cloud Storage: nhà cung cấp dịch vụ lưu trữ đám mây, cung cấp tài nguyên lưu trữ để lưu dữ liệu của hệ thống nhà thông minh. Các yêu cầu về lưu trữ dữ liệu trên dịch vụ lưu trữ đám mây, truy cập dữ liệu, giám sát định kỳ thông tin thiết bị, và thu hồi quyền truy cập được thực hiện thông qua các giao dịch Blockchain.

Trong công trình nghiên cứu của Han và các cộng sự đã đề xuất hệ thống khóa cửa thông minh đảm bảo tính toàn vẹn dữ liệu, tính xác thực và tính chống chối bỏ dựa trên công nghệ Blockchain [23]. Các chỉ thị điều khiển (đóng/mở) cửa thông minh được thực hiện dưới dạng các giao dịch Blockchain. Để yêu cầu mở cửa, người sử dụng thực hiện một giao dịch chứa hai thông tin: (1) thông điệp kiểm soát mở (OPEN control message); và (2) thông tin định vị (GPS) từ thiết bị của người sử dụng, để xác định khoảng cách từ người sử dụng đến cửa thông minh cần mở. Khi giao dịch được xác nhận thành công, cửa thông minh sẽ tự động mở nếu thông số khoảng cách từ GPS của thiết bị đến cửa thông minh nhỏ hơn hoặc bằng một khoảng cách điều kiện cho trước.

Oscar Novo đề xuất kiến trúc kiểm soát truy cập cho IoT dựa trên Blockchain [44]. Trong đó, chủ sở hữu thiết bị có thể đăng ký các thiết bị của họ trên Blockchain và thiết lập các chính sách kiểm soát truy cập cho các thiết bị thông qua một hợp đồng thông minh. Bên cạnh đó, các Management Hub được sử dụng để quản lý các thiết bị IoT và là thành phần trung gian để kết nối giữa các thiết bị IoT với mạng Blockchain. Mỗi Management Hub truy vấn các dữ liệu về kiểm soát truy cập trên sổ cái của một trong các Miner để quyết định cho phép hoặc từ chối các kết nối đến các thiết bị IoT mà nó đang quản lý.

Các tác giả trong công trình nghiên cứu [16] đề xuất phương thức kiểm soát truy cập dựa trên thuộc tính cho IoT. Trong đó, người sở hữu sẽ lưu các thuộc tính của mỗi thiết bị lên Blockchain. Để đảm bảo quyền truy cập hợp lệ và bảo mật dữ liệu, người yêu cầu dữ liệu cần phải được sự cấp quyền truy cập từ chủ sở hữu dữ liệu. Việc thu hồi thuộc tính từ một người dùng được thực hiện thông qua một giao dịch Blockchain.

Outchakoucht và các cộng sự đề xuất một chính sách kiểm soát truy cập động dựa trên Blockchain và học máy cho IoT [48]. Trong giải pháp này, các chính sách bảo mật được tối ưu hóa và được điều chỉnh một cách tự động dựa trên các thông tin phản hồi từ người yêu cầu truy cập.

Nhóm tác giả trong công trình nghiên cứu [47] sử dụng Ethereum Blockchain để kiểm soát truy cập và quản lý xác thực cho IoT. Để được truy cập vào một thiết bị IoT, người yêu cầu truy cập phải xác thực danh tính của mình thông qua một hợp đồng thông minh. Nếu xác thực thành công hợp đồng thông minh sẽ quảng bá một Access Token và địa chỉ Ethereum của người yêu cầu, sau đó người yêu cầu gửi một thông điệp chứa Access Token cùng một số thông tin xác thực đến thiết bị IoT. Thiết bị IoT xác thực thông tin trong thông điệp nhận được và cấp quyền truy cập cho người yêu cầu truy cập nếu thông tin nhận được là chính xác.

Công trình nghiên cứu [45] trình bày một hệ thống quản lý định danh và quản lý truy cập cho các thiết bị IoT trong mạng doanh nghiệp. Trong đó, một mạng Private Blockchain sẽ được dùng cho 3 chức năng: (1) quản lý định danh cho thiết bị IoT, thông tin định danh của người dùng và các thiết bị IoT sẽ được mã hóa và lưu trữ trên Identity Store, giá trị băm của các định danh sẽ được lưu trên Blockchain; (2) kiểm soát truy cập, các chính sách kiểm soát truy cập được thiết lập dưới dạng các giao dịch Blockchain; và (3) giám sát, dùng để lưu lại các hoạt động truy cập.

Nhận xét: Trong các giải pháp kiểm soát truy cập đã khảo sát, chưa có giải pháp nào cấp quyền truy cập vào tài nguyên IoT theo thời gian được cấp phép bởi chủ sở hữu tài nguyên; và việc thu hồi quyền truy cập chưa được tự động hóa, nghĩa là sau khi hết khoảng thời gian được cấp phép, kết nối sẽ tự động bị loại bỏ.

Do đó, luận án sẽ đề xuất giải pháp kiểm soát truy cập dựa trên thời gian được cấp phép bởi chủ sở hữu. Trong đó, người sở hữu thiết bị IoT có thể cấp phép một khoảng thời gian truy xuất nhất định cho người yêu cầu truy cập. Sau khi hết thời gian được cấp phép, kết nối sẽ tự động bị loại bỏ mà không cần người sở hữu thực hiện thêm bất kỳ giao dịch thu hồi quyền truy cập nào. Giải pháp này là một chức năng trong nền tảng bảo mật được đề xuất. Nội dung chi tiết của giải pháp này sẽ

được trình bày ở Chương 4. Các khảo sát một số nghiên cứu liên quan đến kiểm soát truy cập dựa trên Blockchain cho IoT trong mục này được công bố trong công trình [CT2] trong danh mục các công trình nghiên cứu của tác giả.

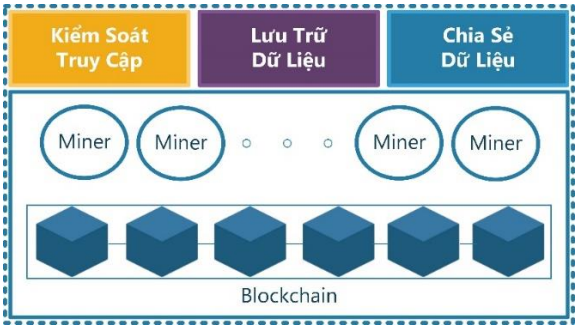
1.7. HƯỚNG NGHIÊN CỨU CỦA LUẬN ÁN

Trên cơ sở các phân tích được trình bày ở trên cho thấy rằng: (1) sử dụng công nghệ Blockchain để xây dựng một nền tảng bảo mật cho IoT là một giải pháp phù hợp với sự phát triển của IoT; (2) các nền tảng bảo mật dựa trên Blockchain hiện tại chưa đạt được sự tối ưu hiệu năng cho các Miner trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain, và tính mở rộng/tích hợp còn hạn chế khi chỉ cung cấp một số chức năng bảo mật nhất định. Bên cạnh đó, các Miner cần được bảo vệ trước các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng; (3) vấn đề lưu trữ và chia sẻ dữ liệu đảm bảo tính riêng tư là vô cùng cần thiết cho IoT khi tốc độ tăng trưởng dữ liệu và nhu cầu trao đổi dữ liệu ngày càng lớn; (4) việc kiểm soát truy cập cho IoT cần có phương thức linh hoạt trong việc cấp quyền và thu hồi quyền truy cập đến các thiết bị IoT. Do đó, luận án đưa ra các hướng nghiên cứu như sau:

(1) Đề xuất một nền tảng bảo mật mới dựa trên Blockchain cho IoT với phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain được xây dựng dựa trên hai trường hợp về các Miner trong một mạng Blockchain. Trường hợp 1, tất cả Miner trong mạng là hoàn toàn tin cậy. Trường hợp 2, trong một mạng Blockchain có tồn tại một số Miner không tin cậy với số lượng ít hơn 1/3 trong tổng số các Miner trong mạng. Bên cạnh đó, luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner để phát hiện sớm các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng, từ đó sẽ có phương thức bảo mật phù hợp để ngăn chặn chúng. Hướng nghiên cứu này sẽ được luận án trình bày ở Chương 2.

(2) Đề xuất chức năng lưu trữ và chia sẻ dữ liệu đảm bảo tính riêng tư cho nền tảng bảo mật được đề xuất. Hướng nghiên cứu này sẽ được trình bày ở Chương 3.

(3) Đề xuất chức năng kiểm soát truy cập theo thời gian được cấp phép bởi chủ sở hữu cho nền tảng bảo mật được đề xuất. Hướng nghiên cứu này sẽ được trình bày ở Chương 4.



Hình 1.8: Kiến trúc tổng quan của nền tảng bảo mật được đề xuất

Kiến trúc tổng quan của nền tảng bảo mật được đề xuất của luận án được thể hiện ở Hình 1.8.

1.8. KẾT LUẬN CHƯƠNG 1

Trong chương này, luận án giới thiệu về công nghệ Blockchain, một số giao thức đồng thuận thường được sử dụng trong các nền tảng bảo mật dựa trên Blockchain cho IoT, các loại mạng Blockchain và các hình thức tấn công bảo mật giả định trên Blockchain. Luận án cũng đã khảo sát các nền tảng bảo mật dựa trên Blockchain cho IoT, khảo sát các giải pháp lưu trữ và chia sẻ dữ liệu dựa trên Blockchain, khảo sát các nghiên cứu liên quan đến kiểm soát truy cập dựa trên Blockchain. Trong đó, luận án đã chỉ ra hai hạn chế của các nền tảng bảo mật dựa trên Blockchain cho IoT, đó là: (1) hạn chế về các tính năng bảo mật được cung cấp; và (2) chưa tối ưu hiệu năng của các Miner trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain.

Đối với các giải pháp lưu trữ và chia sẻ dữ liệu dựa trên Blockchain, các giải pháp đã khảo sát chưa đạt được tất cả các yêu cầu sau đây: (1) dữ liệu lưu trữ cần phải đảm bảo tính bí mật, tính toàn vẹn; (2) cần sự chủ động trong quá trình chia sẻ dữ liệu giữa chủ sở hữu dữ liệu và người được chia sẻ; (3) cần cung cấp một phương thức để người yêu cầu chia sẻ dữ liệu có thể kiểm tra tính chính xác và tin cậy của dữ liệu được chia sẻ trước khi gửi yêu cầu chia sẻ đến người sở hữu.

Đối với các giải pháp kiểm soát truy cập dựa trên Blockchain đã khảo sát, chưa có giải pháp nào cho phép chủ sở hữu tài nguyên IoT có thể cấp quyền truy cập dựa trên thời gian được cấp phép cho người yêu cầu truy cập, và việc thu hồi quyền truy cập chưa được tự động hóa.

Trên cơ sở các phân tích và xác định các hạn chế từ các nghiên cứu đã khảo sát, luận án đã đề xuất xây dựng một nền tảng bảo mật mới đảm bảo tối ưu hiệu năng cho các Miner trong việc xác minh các giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain. Nền tảng bảo mật được đề xuất sẽ cung cấp các chức năng: kiểm truy cập dựa trên thời gian được cấp phép bởi chủ sở hữu thiết bị, lưu trữ dữ liệu và chia sẻ dữ liệu đảm bảo tính riêng tư. Nền tảng bảo mật cho IoT được đề xuất có thể được áp dụng cho mạng Private Blockchain hoặc Consortium Blockchain.

Trong một mạng Blockchain có thể tồn tại một số Node độc hại, chúng có thể thực hiện các cuộc tấn công từ chối dịch vụ đến các Miner. Để phát hiện sớm nguy cơ tấn công này, luận án cũng đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner trong nền tảng bảo mật được đề xuất.

CHƯƠNG 2: NỀN TẢNG BẢO MẬT DỰA TRÊN BLOCKCHAIN CHO IoT

Chương này phân tích các hạn chế về hiệu năng của các Miner trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái trong một số các nền tảng bảo mật dựa trên Blockchain cho IoT. Từ đó, luận án đề xuất một nền tảng bảo mật mới dựa trên Blockchain cho IoT. Trong đó, luận án trình bày kiến trúc, quy trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của nền tảng bảo mật được đề xuất. Luận án tiến hành đánh giá hiệu năng của các Miner trong nền tảng bảo mật được đề xuất. Bên cạnh đó, luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner trong nền tảng nhằm phát hiện sớm các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng. Chương này được tổng hợp từ các công trình [CT3] và [CT7] trong danh mục các công trình nghiên cứu của tác giả.

2.1. GIỚI THIỆU

Triển khai một nền tảng bảo mật cho một mạng IoT là rất cần thiết, giúp hệ thống hoạt động ổn định và tin cậy hơn. Với các mạng IoT có kích thước lớn và có nhu cầu mở rộng cao như mạng IoT của thành phố thông minh, sử dụng công nghệ Blockchain trong nền tảng bảo mật là lựa chọn phù hợp. Hai thành phần quan trọng trong một mạng Blockchain chính là các Miner và phương thức đồng thuận được sử dụng.

Các Miner cần có hiệu năng tính toán cao và dung lượng lưu trữ đủ lớn để xác minh giao dịch và lưu trữ dữ liệu cho toàn mạng. Tùy thuộc vào từng loại mạng Blockchain mà các Miner có thể được thiết lập theo các cách khác nhau. Người xây dựng hệ thống Blockchain có thể thiết lập một số lượng các Miner cố định hoặc có thể thiết lập một số lượng cố định các Miner của họ và cho phép một số lượng nhất định các Miner từ bên ngoài tham gia vào mạng.

Phương thức đồng thuận dữ liệu trên sổ cái của một mạng Blockchain có thể ảnh hưởng đến hiệu năng của các Miner, tốc độ xác minh giao dịch và tạo khối trên sổ cái. Tùy thuộc vào từng ứng dụng cụ thể và loại mạng Blockchain khác nhau mà

có thể thiết kế và áp dụng cơ chế đồng thuận phù hợp. Trong chương này, luận án đề xuất một nền tảng bảo mật dựa trên Blockchain cho IoT. Trong đó chỉ tập trung vào việc thiết kế kiến trúc của nền tảng, xây dựng quy trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain. Các chức năng bảo mật trong nền tảng như lưu trữ dữ liệu, chia sẻ dữ liệu và kiểm soát truy cập sẽ được trình bày ở các chương tiếp theo.

Quy trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain của các Miner trong nền tảng được đề xuất phụ thuộc vào hai trường hợp về các Miner trong một mạng Blockchain. Trường hợp 1: một mạng Blockchain với tất cả các Miner đều hoàn toàn tin cậy. Tính tin cậy của các Miner ở đây có nghĩa là chúng hoàn toàn không thể bị thỏa hiệp từ kẻ tấn công và cũng không thực hiện bất kỳ hành vi gian lận nào trên mạng Blockchain. Trường hợp 2: trong một mạng Blockchain có tồn tại một số Miner không tin cậy với số lượng ít hơn 1/3 trong tổng số các Miner trong mạng. Với mỗi trường hợp, luận án sẽ thiết kế phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain tương ứng. Các đề xuất này được công bố trong công trình [CT3] trong danh mục các công trình nghiên cứu của tác giả.

Trong một mạng Blockchain có thể tồn tại một số Node độc hại, chúng có thể thực hiện các cuộc tấn công từ chối dịch vụ đến các Miner trong nền tảng bảo mật. Để phát hiện sớm các nguy cơ này, luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner trong nền tảng. Đề xuất này được công bố trong công trình [CT7] trong danh mục các công trình nghiên cứu của tác giả.

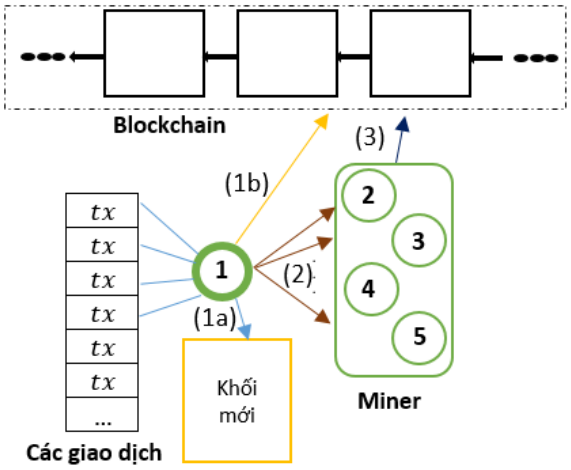
2.2. VẤN ĐỀ VỀ HIỆU NĂNG CỦA MINER

Các nền tảng bảo mật được khảo sát ở Chương 1 chưa đảm bảo tối ưu hiệu năng của các Miner trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái trong hai trường hợp sau đây:

a. Trường hợp 1

Tất cả các Miner trong một mạng Blockchain đều hoàn toàn tin cậy, nghĩa là các Miner này không thể bị thỏa hiệp bởi kẻ tấn công và cũng không thực hiện bất kỳ hoạt động gian lận nào trên mạng Blockchain. Giả sử một nền tảng bảo mật sử dụng

một trong các giao thức đồng thuận *PoW*, *PoS*, *PoA*, *PoAh*, *DPoS*, *PBFT*, và *Tendermint*. Đặc điểm chung của các giao thức đồng thuận này là: tại mỗi vòng Mining, một Miner được chọn có trách nhiệm xác minh giao dịch sau đó tạo và đề xuất một khối mới đến Miner khác trong mạng, các Miner khác có trách nhiệm xác minh khối được đề xuất này. Nếu khối mới này hợp lệ, các Miner sẽ thêm khối này vào sổ cái của chúng.



Hình 2.1: Phương thức đồng thuận tổng quát trong trường hợp 1

Hình 2.1 mô tả quá trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của các Miner đối với các giao thức đồng thuận nêu trên. Trong mô hình này có 5 Miner, giả sử tại vòng Mining này Miner ① được lựa chọn để xác minh các giao dịch, tạo và đề xuất khối mới cho mạng Blockchain. Chi tiết các bước thực hiện như sau:

- Bước 1: Miner ① thực hiện 2 công việc:
  + Xác minh và đặt các giao dịch hợp lệ vào một khối mới.
  + Lưu khối mới này vào sổ cái của nó.
- Bước 2: Miner ① quảng bá khối mới này đến các Miner khác trong mạng.
- Bước 3: Các Miner ②, ③, ④ và ⑤ xác minh tính hợp lệ của khối nhận được từ Miner ①. Nếu khối này hợp lệ, các Miner sẽ lưu khối này vào sổ cái Blockchain của chúng.

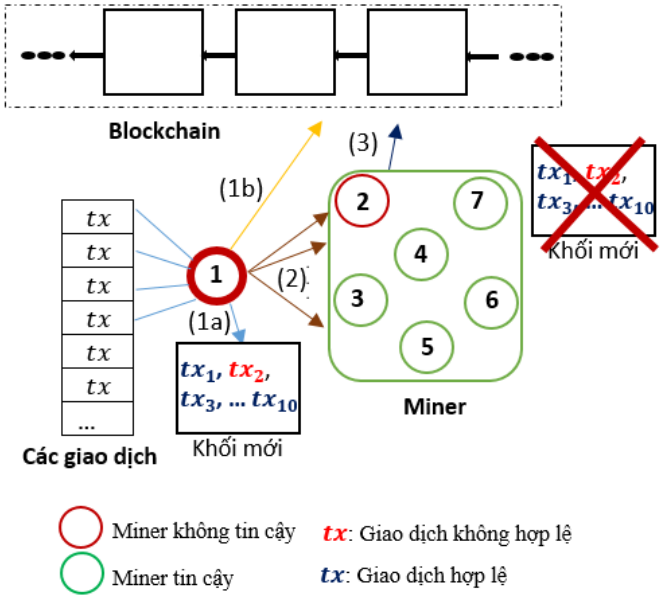
Nhược điểm của những nền tảng bảo mật sử dụng một trong các giao thức đồng thuận này là tốc độ xác minh các giao dịch và tốc độ tạo khối trên sổ cái của các Miner không thay đổi khi bổ sung thêm các Miner vào trong mạng Blockchain. Cụ

thể, giả sử khi bổ sung thêm các Miner ⑥ và ⑦ vào trong danh sách các Miner trong mạng ở Hình 2.1, Miner ⑥ và ⑦ cũng chỉ thực hiện công việc tại bước 3 giống như các Miner ②, ③, ④ và ⑤.

b. Trường hợp 2

Trong mạng Blockchain có tồn tại một số Miner không tin cậy nhưng số lượng ít hơn 1/3 trong tổng số Miner trong mạng. Trong trường hợp một nền tảng bảo mật sử dụng một trong các giao thức đồng thuận *PoW*, *PoS*, *PoA*, *PoAh*, *DPoS*, *PBFT*, và *Tendermint*.

Xét trường hợp tại một vòng Mining, một Miner không tin cậy (Miner bị thỏa hiệp bởi kẻ tấn công) được lựa chọn để làm nhiệm vụ xác minh giao dịch, tạo và đề xuất một khối mới đến các Miner khác trong mạng. Khi đó, Miner này có thể đặt một hoặc một vài giao dịch không hợp lệ cùng với các giao dịch hợp lệ vào trong một khối mới và quảng bá khối này đến các Miner khác trong mạng. Khi nhận được khối mới này, các Miner tin cậy tất nhiên sẽ loại bỏ khối mới này vì nó có chứa các dịch không hợp lệ, Hình 2.2 thể hiện trường hợp này. Tuy nhiên, các giao dịch hợp lệ trong khối này sẽ phải xác minh lại trong lần Mining kế tiếp. Điều này là không cần thiết và dẫn đến các Miner phải tốn chí phí tài nguyên để xác minh lại các giao dịch hợp lệ đã xác minh từ trước đó.



Hình 2.2: Phương thức đồng thuận tổng quát trong trường hợp 2

Trên Hình 2.2, Miner ① và ② là các Miner không tin cậy, các Miner ③, ④, ⑤, ⑥, và ⑦ là các Miner tin cậy. Giả sử tại một vòng Mining Miner ① được chọn để xác minh các giao dịch, tạo và đề xuất một khối mới, Miner này đặt một giao dịch không hợp lệ tx_2 cùng với các giao dịch hợp lệ $tx_1, tx_3, \dots, tx_{10}$ vào một khối mới. Khi khối này quảng bá đến các Miner còn lại để xác minh thì chắc chắn các Miner ③, ④, ⑤, ⑥, và ⑦ sẽ loại bỏ khối mới này vì nó có chứa một giao dịch không hợp lệ. Như vậy, các giao dịch $tx_1, tx_3, \dots, tx_{10}$ sẽ phải xác minh lại tại lần Mining tiếp theo.

Từ các phân tích ở trên cho thấy rằng cần phải xây dựng một nền tảng bảo mật mới, với phương thức xác minh và đồng thuận dữ liệu trên sổ cái đảm bảo tối ưu hiệu năng cho các Miner trong mạng. Khi các hạn chế nêu trên được khắc phục, hiệu năng xử lý của các Miner trong mạng được tối ưu, tốc độ xác minh các giao dịch sẽ nhanh hơn rất nhiều.

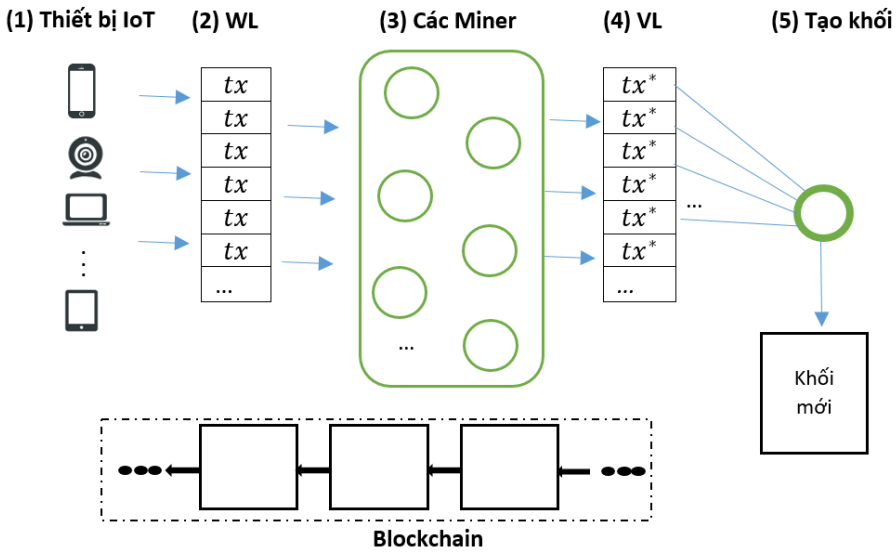
Trong phần tiếp theo, luận án trình bày đề xuất nền tảng bảo mật dựa trên Blockchain dựa trên 2 trường hợp về các Miner trong một mạng Blockchain. Trong đó, luận án tập trung trình bày kiến trúc, quy trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của các Miner trong nền tảng được đề xuất. Sau đó tiến hành so sánh về số lượng giao dịch được xác minh và thời gian Mining trung bình một khối mới của nền tảng được đề xuất với các nền tảng bảo mật tương tự đã khảo sát

2.3. NỀN TẢNG ĐỀ XUẤT

Gọi $M = \{m_1, m_2, \dots, m_n\}$ là một tập hợp gồm n Miner trong một mạng Blockchain. Mỗi Miner được khởi tạo một khóa riêng và một khóa công khai tương ứng bởi một hệ mật mã khóa công khai được cung cấp bởi hệ thống. Trong đó, khóa công khai được sử dụng làm định danh cho Miner và cũng là một địa chỉ giao dịch trên mạng Blockchain, khóa riêng được sử dụng để ký trên các giao dịch/khối do Miner đó thực hiện/quảng bá. Tất cả các Miner đều tham gia vào quá trình xác minh các giao dịch.

Gọi $WL = \{tx_1, tx_2, \dots, tx_m\}$ là một danh sách chứa các giao dịch chưa được xác minh nhận được từ các thiết bị IoT trong mạng. Đây được xem như một Pool công khai và được dùng chung cho tất cả các Miner. Gọi $VL = \{tx_1^*, tx_2^*, \dots, tx_k^*\}$ là một danh sách chứa các giao dịch đã được xác minh là hợp lệ bởi các Miner. Một giao dịch được xem là hợp lệ khi chữ ký số trên giao dịch đó là hợp lệ. VL cũng được dùng chung cho các Miner trong mạng. Gọi l là số lượng giao dịch tối đa trong một khối. Tại mỗi vòng Mining, một trong số các Miner này được lựa chọn ngẫu nhiên bởi một ứng dụng của hệ thống để đặt l giao dịch trong VL vào một khối mới và quảng bá khối mới này đến các Miner khác trong mạng.

Mỗi thiết bị IoT là một Node trong mạng Blockchain, chúng có thể thực hiện các giao dịch trong mạng. Mỗi Node sở hữu một cặp khóa được khởi tạo bởi một hệ mật mã khóa công khai được cung cấp bởi hệ thống. Trong đó, khóa công khai là địa chỉ giao dịch trên mạng Blockchain, khóa riêng được sử dụng để ký trên các giao dịch do Node đó thực hiện. Tổng quan về kiến trúc, quy trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của nền tảng được đề xuất được thể hiện ở Hình 2.3. Trong đó, ký hiệu tx thể hiện một giao dịch chưa được xác minh, tx^* là một giao dịch hợp lệ hay còn được gọi là giao dịch đã được xác minh.



Hình 2.3: Kiến trúc, quy trình xác minh và đồng thuận dữ liệu

Các luật được thiết lập cho WL và VL như sau:

(i) Các giao dịch chưa được xác minh được lưu vào WL.

(ii) Chỉ các Miner mới có thể xác minh các giao dịch trong WL.

(iii) Các giao dịch được xác minh là hợp lệ sẽ được di chuyển từ WL sang VL. Ngược lại, chúng sẽ bị xóa khỏi WL bởi một ứng dụng của hệ thống.

(iv) Các giao dịch trong VL sau khi được lưu vào sổ cái thành công sẽ được xóa khỏi VL bởi một ứng dụng của hệ thống.

Quá trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của các Miner trong nền tảng bảo mật được đề xuất dựa trên hai trường hợp về các Miner trong một mạng Blockchain như sau:

- *Trường hợp 1:* Tất cả các Miner trong một mạng Blockchain đều hoàn toàn tin cậy. Điều này nghĩa là các Miner này rất khó bị thỏa hiệp bởi kẻ tấn công và cũng không thực hiện bất kỳ hành vi gian lận nào trên mạng Blockchain.
- *Trường hợp 2:* Trong mạng có tồn tại một số Miner không tin cậy, chúng có thể bị thỏa hiệp bởi kẻ tấn công thông qua các lỗ hổng bảo mật của hệ điều hành hoặc các ứng dụng đã cài đặt trên chúng. Tuy nhiên, số lượng Miner không tin cậy ít hơn 1/3 trong tổng số Miner trong mạng.

Nền tảng bảo mật của luận án ở Chương này chỉ tập trung vào việc xây dựng phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của các Miner, sao cho dữ liệu lưu trữ trên sổ cái đảm bảo tính chính xác và tối ưu hiệu năng cho các Miner. Các chức năng bảo mật được tích hợp trong nền tảng sẽ được trình bày trong các Chương tiếp theo của luận án. Quá trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của các Miner trong nền tảng bao gồm hai giai đoạn như sau:

- *Giai đoạn 1*: Giai đoạn xác minh

Khi một thiết bị IoT thực hiện một giao dịch Blockchain tx, giao dịch tx sẽ được quảng bá trên mạng Blockchain và sẽ được lưu trữ trên WL. Quá trình xác minh các giao dịch trong WL phụ thuộc vào 2 trường hợp về các Miner:

+ *Đối với trường hợp 1*: Vì tất cả các Miner đều hoàn toàn tin cậy nên mỗi giao dịch chỉ cần được xác minh bởi một Miner trong mạng. Nếu giao dịch tx là hợp lệ, tx sẽ được lưu vào vị trí cuối cùng của danh sách VL.

+ *Đối với trường hợp 2*: Mỗi giao dịch cần phải được xác minh bởi ít nhất 2/3 trong tổng số các Miner trong mạng. Một giao dịch được xem là hợp lệ nếu đạt được sự công nhận là hợp lệ của ít nhất 2/3 trong tổng số các Miner. Nếu giao dịch tx là hợp lệ, tx sẽ được lưu vào vị trí cuối cùng của danh sách VL.

❖ *Giai đoạn 2*: Giai đoạn tạo khối

Tại mỗi vòng Mining, một Miner được lựa chọn sẽ đặt l giao dịch trong VL vào một khối mới, sau đó tạo chữ ký số trên khối mới này và quảng bá chúng đến các Miner khác. Tùy vào kích thước của mỗi giao dịch và kích thước tối đa cho phép của một khối mà giá trị l sẽ được ấn định. Trong trường hợp số lượng giao dịch trong VL nhỏ hơn l thì Miner sẽ đặt các giao dịch hiện có trong VL vào khối mới. Khối mới này sẽ được các Miner đưa vào sổ cái của chúng nếu thỏa mãn các yêu cầu tùy theo từng trường hợp của các Miner.

Chi tiết các bước trong giai đoạn này như sau:

+ *Bước 1*: Mục tiêu của bước này là lựa chọn một Miner để tạo và quảng bá khối mới đến các Miner khác trong mạng.
  - ✓ *Đối với trường hợp 1:* Vì tất cả các Miner đều tin cậy nên có thể chỉ định một Miner m_i (cố định) để thực hiện công việc này, và m_i cũng có thể bị thay bằng một Miner khác khi cần thiết.
  - ✓ *Đối với trường hợp 2*: Một Miner sẽ được lựa chọn ngẫu nhiên tại mỗi vòng Mining: $m_i \xleftarrow{r} M$, với $1 \leq i \leq n$.
+ *Bước 2*: m_i lấy l giao dịch trong VL đưa vào một khối mới. Sau đó, m_i tạo chữ ký số trên khối mới này.
+ *Bước 3*: m_i quảng bá khối mới này cùng với chữ ký số đến các Miner khác trong mạng. Bên cạnh đó, m_i cũng sẽ thêm khối mới này vào sổ cái của nó.
+ *Bước 4*: Sau khi nhận được khối mới cùng chữ ký số, các Miner xác minh tính hợp lệ của khối mới tùy theo hai trường hợp về Miner trong mạng.
  - ✓ *Đối với trường hợp 1:* Các Miner xác minh chữ ký của m_i, nếu chữ ký hợp lệ, các Miner sẽ thêm khối mới này vào sổ cái của chúng. Ngược lại, bỏ qua khối mới này.

- ✓ *Đối với trường hợp 2:* Thực hiện hai bước như sau:
  - (i) Các Miner xác minh chữ ký của m_i, nếu chữ ký hợp lệ sẽ chuyển sang bước (ii). Ngược lại, bỏ qua khối mới này.
  - (ii) Các Miner kiểm tra xem các giao dịch trong khối mới này có nằm trong VL hay không. Nếu đúng, khối mới này sẽ được thêm vào sổ cái của Miner. Ngược lại, bỏ qua khối mới này.

2.4. ĐÁNH GIÁ HIỆU NĂNG

Luận án đánh giá nền tảng được đề xuất dựa trên thời gian tạo khối chứa l giao dịch và số lượng các giao dịch được xác minh trong một thời gian nhất định. Nhìn chung, các nền tảng bảo mật dựa trên Blockchain cho IoT đã khảo sát chủ yếu tập trung vào việc cung cấp các tính năng cụ thể. Trong khi các cơ chế xác minh giao dịch, tạo khối, và đồng bộ dữ liệu trên sổ cái phụ thuộc hoàn toàn vào giao thức đồng thuận được sử dụng trong mạng Blockchain. Do đó, luận án sẽ so sánh quá trình xác minh và đồng thuận dữ liệu trên sổ cái của các Miner trong nền tảng được đề xuất với các giao thức đồng thuận được trình bày ở Mục 1.3.1.

Luận án giả định tất cả các Miner có hiệu năng tính toán là như nhau. Gọi t_1 là thời gian xác minh/kiểm tra một giao dịch của một Miner, t_2 là thời gian tạo một chữ ký số/phiếu/chứng chỉ của một Miner cho mỗi khối, t_3 là thời gian xác minh một chữ ký số/phiếu/chứng chỉ của một Miner. Gọi t_4 là thời gian chuyển/quảng bá một khối/phiếu/chứng chỉ/giao dịch đến đích (như VL hoặc Miner), và t_5 là thời gian lựa chọn ngẫu nhiên một Miner tại mỗi vòng Mining.

2.4.1. Đánh giá nền tảng đề xuất với trường hợp 1

Trong giai đoạn 1, mỗi giao dịch được xác minh bởi một Miner trong tổng số n Miner, do đó thời gian xác minh của l giao dịch là $\frac{l}{n}t_1$, thời gian quảng bá l giao dịch đã xác minh đến VL là $\frac{l}{n}t_4$. Trong giai đoạn 2, thời gian lựa chọn Miner để tạo khối $t_4 = 0$, vì một Miner đã được chỉ định để thực hiện công việc này, thời gian thực hiện tại *Bước 2, 3, 4* trong giai đoạn này lần lượt là t_2, t_4, t_3. Tổng thời gian tạo một khối mới của nền tảng trong trường hợp này được ký hiệu là T, thời gian này có thể

xem như là thời gian Mining trung bình một khối mới. *T* được tính bằng công thức như sau:

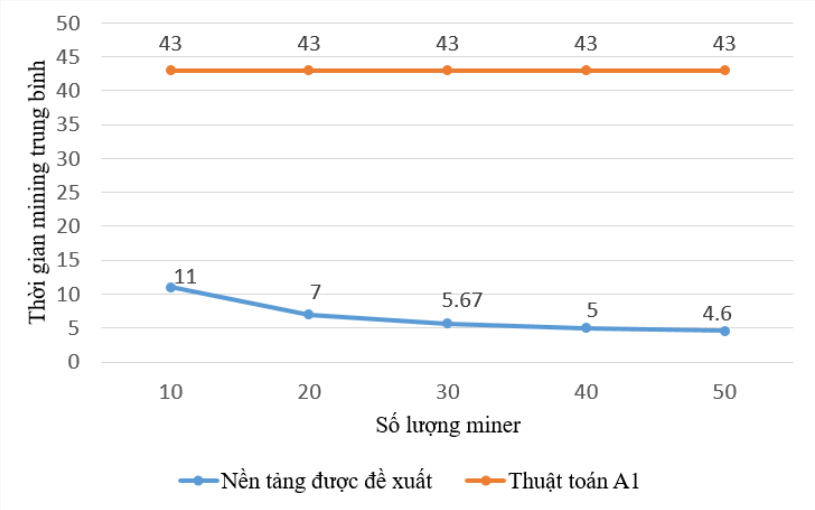
$$T = \frac{l}{n}t_1 + t_2 + t_3 + \left(\frac{l}{n} + 1\right)t_4 \quad (2.1)$$

Xét thời gian tạo khối của các nền tảng bảo mật dựa trên Blockchain cho IoT sử dụng một trong các giao thức đồng thuận *PoW, PoS, PoA, PoAh, DPoS, PBFT*, và *Tendermint*. Đặc điểm chung của các giao thức đồng thuận này là một Miner được chọn sẽ có trách nhiệm xác minh giao dịch, sau đó đặt các giao dịch vào một khối mới và quảng bá khối mới này đến các Miner khác tại mỗi vòng Mining. Trong khi đó, các Miner khác có trách nhiệm xác minh khối mới này. Với trường hợp 1, các Miner trong mạng là hoàn toàn tin cậy, có thể khái quát thuật toán đồng thuận cho các giao thức đồng thuận nêu trên, được ký hiệu là $A1$, như sau:

Thuật toán: A1	
	Input: l giao dịch trong Pool, một Miner m_i được lựa chọn cố định cho việc Mining, và các Miner còn lại trong mạng. **Output:** một khối mới trên sổ cái
Bước 1	(1) m_i xác minh và đặt l giao dịch hợp lệ vào một khối mới. (2) m_i tạo chữ ký số trên khối mới này. (3) m_i quảng bá khối mới này cùng với chữ ký số đến các Miner khác trong mạng, đồng thời thêm khối mới này vào sổ cái của nó.
Bước 2	Các Miner khác xác minh chữ ký trên khối nhận được, nếu chữ ký số hợp lệ, khối mới này sẽ được thêm vào sổ cái của chúng.

Với thuật toán $A1$, để xác minh l giao dịch, m_i tốn lt_1 thời gian, thời gian tạo chữ ký số trên khối mới và quảng bá khối mới này tại *Bước 1* lần lượt là t_2, t_4. Thời gian xác minh chữ ký tại *Bước 2* là t_3. Thời gian Mining trung bình của thuật toán $A1$, được ký hiệu là T', được tính như sau:

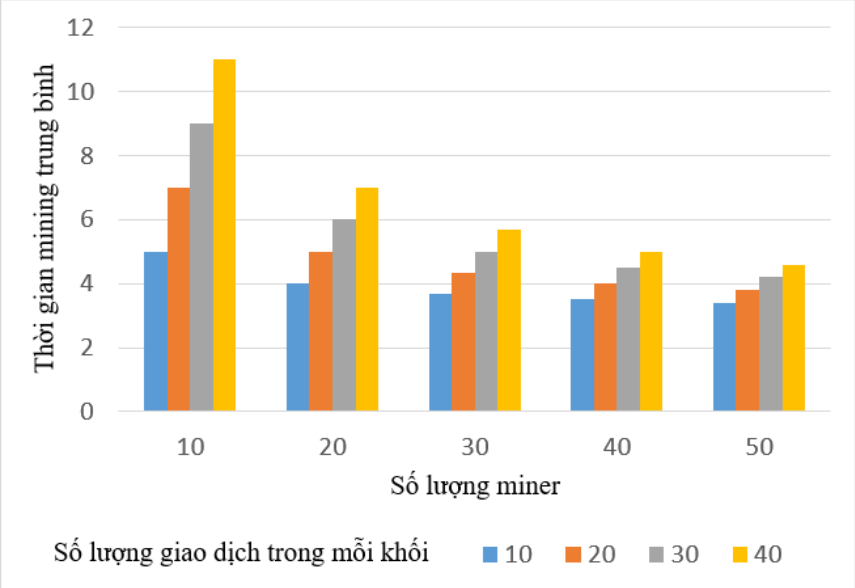
$$T' = lt_1 + t_2 + t_3 + t_4 \quad (2.2)$$



Hình 2.4: So sánh thời gian Mining trung bình trong trường hợp 1

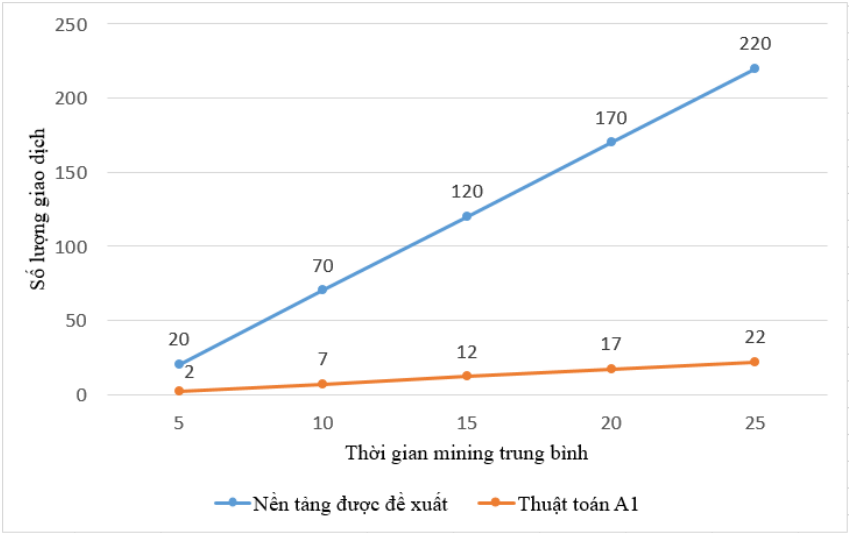
Xét $t_1 = 1$, $t_2 = 1$, $t_3 = 1$, $t_4 = 1$, và $l = 40$. Hình 2.4 thể hiện thời gian Mining trung bình của thuật toán $A1$ và của nền tảng được đề xuất trong trường hợp 1. Có thể thấy rằng thời gian Mining trung bình của nền tảng được đề xuất thấp hơn rất nhiều so với thuật toán $A1$. Cụ thể, thời gian Mining trung bình của thuật toán $A1$ là 43, trong khi thời gian Mining trung bình của nền tảng được đề xuất là 11 khi hệ thống Blockhain có 10 Miner ($n = 10$). Khi tăng số lượng Miner trong mạng lên 50, thời gian Mining trung bình của thuật toán $A1$ không thay đổi. Trong khi đó, thời gian Mining trung bình của nền tảng được đề xuất giảm đáng kể chỉ còn 4.6. Điều này có nghĩa là càng nhiều Miner tham gia vào mạng thì thời gian Mining trung bình càng giảm.

Một phân tích khác khi điều chỉnh tham số n và l của công thức (2.1) của nền tảng được đề xuất trong trường hợp 1. Với cùng số lượng Miner trong một mạng Blockchain, thời gian Mining trung bình tăng tỷ lệ thuận với số lượng giao dịch trong khối. Hơn nữa, khi số lượng Miner tăng lên thì thời gian Mining trung bình của nền tảng được đề xuất giảm đáng kể, kết quả phân tích được thể hiện ở Hình 2.5. Cụ thể, khi số lượng Miner $n = 10$, với số lượng giao dịch trong mỗi khối $l = 10$ thì thời gian Mining trung bình $T = 5$, với $l = 20$ thì $T = 7$, với $l = 30$ thì $T = 9$, và với $l = 40$ thì $T = 11$. Khi tăng số lượng Miner $n = 50$, với $l = 10$ thì $T = 3.4$, với $l = 20$ thì $T = 3.8$, với $l = 30$ thì $T = 4.2$, và với $l = 40$ thì $T = 4.6$.



Hình 2.5: So sánh thời gian Mining của nền tảng trong trường hợp 1

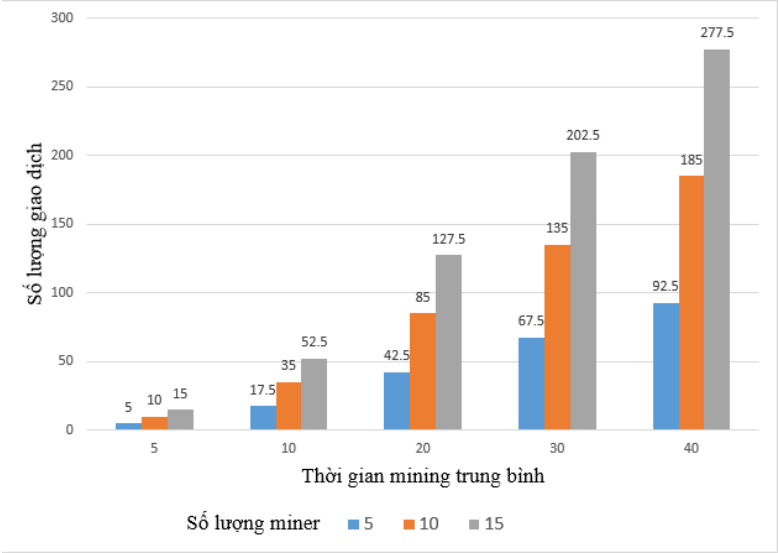
Theo kết quả so sánh được thể hiện ở Hình 2.6, khi thiết lập cùng thời gian Mining trung bình và cùng số lượng Miner $n = 20$, tổng số giao dịch đã được xác minh của nền tảng được đề xuất là cao hơn so với thuật toán $A1$. Khi tăng thời gian Mining trung bình của một khối thì mức độ chênh lệnh về số lượng giao dịch được xác minh giữa nền tảng được đề xuất với thuật toán $A1$ càng lớn.



Hình 2.6: So sánh số lượng giao dịch được xác minh trong trường hợp 1

Cụ thể, khi thiết lập cùng thời gian Mining trung bình $T = T' = 5$, tổng số giao dịch được xử lý của thuật toán $A1$ và nền tảng được đề xuất lần lượt là 2 và 20. Tuy nhiên, khi $T = T' = 25$, số lượng giao dịch được xử lý của thuật toán $A1$ tăng chỉ đạt 22

giao dịch, trong khi đó số lượng giao dịch được xử lý của nền tảng được đề xuất là 220 giao dịch.



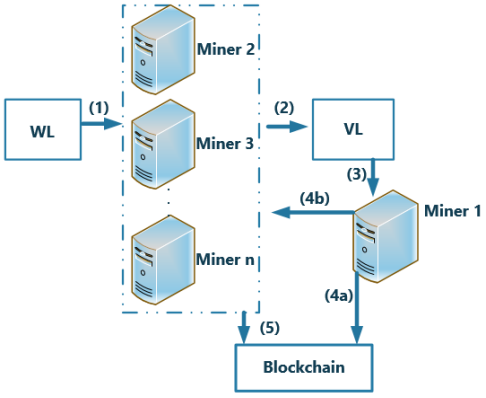
Hình 2.7: Số lượng giao dịch được xác minh của nền tảng trong trường hợp 1

Trong nền tảng được đề xuất, số lượng các giao dịch được xác minh tăng tỷ lệ thuận với số lượng Miner trong mạng, kết quả đánh giá được thể hiện ở Hình 2.7. Cụ thể, xét thời gian Mining trung bình $T = 5$, khi số lượng Miner trong mạng $n = 5$ thì tổng số giao dịch được xác minh từ các Miner này là $l = 5$, khi $n = 10$ thì $l = 10$, và $n = 15$ tương ứng với $l = 15$. Xét $T = 40$, với $n = 5$ thì $l \approx 93$ giao dịch, với $n = 10$ thì $l = 185$, và với $n = 15$ thì $l \approx 278$.

❖ **Thực nghiệm**

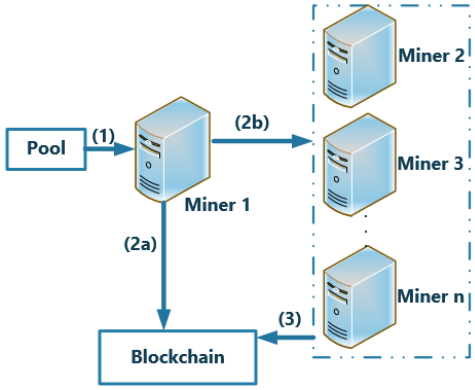
- Mô hình thực nghiệm:

- Mô hình thực nghiệm của nền tảng bảo mật được đề xuất:



Hình 2.8: Mô hình thực nghiệm của nền tảng trong trường hợp 1

- Mô hình thực nghiệm của thuật toán *A*1:



*Hình 2.9: Mô hình thực nghiệm của thuật toán A*1

- Thông số cấu hình:

- Các Miner có cùng thông số cấu hình như sau:

Cấu hình phần cứng	**Hệ điều hành và công cụ mô phỏng**
RAM: 2GB, Processors Intel (R) Core(TM) i7-4590 CPU 3,3 GHz	Hệ điều hành Centos 64-bit Ngôn ngữ lập trình Python3, thư viện: *json, datetime, Crypto, re, binascii*

Các Miner giao tiếp với nhau trong một mạng nội bộ có băng thông mạng 100 Megabits/giây.

- Mỗi giao dịch có cấu trúc và kích thước như sau:

Cấu trúc	*{'Sender':'<Public key của Sender>', 'Receiver':' <Public key của Receiver>',' Content':'<một số nguyên>'}*
Kích thước	*1,125 bytes (≈1,1 kilobyte)*

Mỗi giao dịch sẽ được tạo theo cấu trúc nêu trên và có gắn thêm chữ ký số của người thực hiện giao dịch (*Sender*). Chữ ký số trên giao dịch sẽ được dùng để xác minh tính hợp lệ của giao dịch. Sử dụng một tệp tin để làm chức năng của *WL/Pool*, tệp tin này lưu 20000 giao dịch và được chia sẻ giữa các Miner.

- Kịch bản thực nghiệm:

- *Kịch bản 1:* Thực nghiệm đánh giá thời gian Mining trung bình cho 30 khối đầu tiên của nền tảng được đề xuất và thuật toán *A*1 khi thay đổi số lượng các Miner

tham gia vào mạng. Mỗi vòng Mining sẽ bắt đầu khi số lượng các giao dịch được xác minh là $l = 100$, điều này có nghĩa là mỗi khối sẽ chứa 100 giao dịch. Số lượng các giao dịch trong *WL/Pool* là đủ để các Miner có thể thực hiện xác minh. Kết quả thực nghiệm được trình bày ở Bảng 2.1

Bảng 2.1 Kết quả thực nghiệm về thời gian Mining

Số lượng Miner	**Thời gian Mining trung bình cho 30 khối của nền tảng được đề xuất** (giây)	**Thời gian Mining trung bình cho 30 khối của thuật toán A1** (giây)	**Chênh lệch** (giây)
4	3.183041	4.730996	1.547955
5	2.554070	4.730663	2.176593
6	2.393606	4.730952	2.337346
7	2.123214	4.731036	2.607822
8	1.863560	4.731002	2.867442

Kết quả thực nghiệm của kịch bản này cho thấy rằng, thời gian Mining 30 khối đầu tiên của thuật toán $A1$ cao hơn so với nền tảng được đề xuất khi thiết lập cùng số lượng Miner. Khi tăng số lượng Miner tham gia vào hệ thống, thì thời gian Mining trung bình cho 30 khối đầu tiên của thuật toán $A1$ hầu như không thay đổi. Trong khi đó, thời gian Mining trung bình của nền tảng bảo mật được đề xuất giảm đáng kể.

- *Kịch bản 2:* Kịch bản thực nghiệm này để đánh giá số lượng các giao dịch được xác minh trong một khoảng thời gian Δ (1, 1.5, 2, 2.5 và 3 giây) của nền tảng bảo mật được đề xuất và thuật toán $A1$ khi có cùng số lượng Miner là 8 ($n = 8$). Kết quả thực nghiệm được trình bày ở Bảng 2.2.

Bảng 2.2 Kết quả thực nghiệm về số lượng giao dịch được xác minh

Δ *(giây)*	**Số lượng giao dịch được xác minh của nền tảng được đề xuất** *(giao dịch)*	**Số lượng giao dịch được xác minh của thuật toán A1** *(giao dịch)*	**Chênh lệch** (*giao dịch*)
1	3350	1646	1704
1.5	6434	2499	3935
2	9056	3376	5680
2.5	11809	4248	7561
3	14749	5138	9611

Kết quả thực nghiệm của kịch bản này cho thấy rằng, với cùng số lượng Miner là 8 và trong cùng một khoảng thời gian Δ, tổng số giao dịch được xác minh và đưa vào VL của nền tảng bảo mật được đề xuất cao hơn rất nhiều so với số lượng giao dịch được xác minh của thuật toán $A1$. Khi tăng khoảng thời gian Δ thì tổng số giao dịch được xác minh của nền tảng được đề xuất tăng lên đáng kể, và sự chênh lệnh về số lượng giao dịch được xác minh giữa nền tảng được đề xuất và thuật toán $A1$ càng lớn.

Dựa trên kết quả thực nghiệm của 2 kịch bản ở trên, nền tảng được đề của luận án ở trường hợp 1 đã đạt được các mục tiêu đã đề ra, đó là:

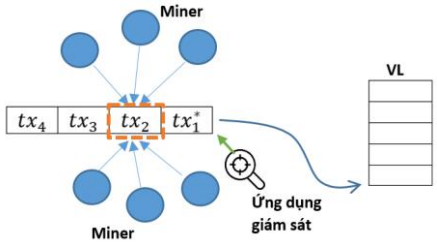
(1) Tăng số lượng giao dịch được xác minh khi tăng số lượng Miner trong nền tảng.

(2) Giảm thời gian Mining khi tăng số lượng Miner trong nền tảng.

(3) Tăng số lượng giao dịch được xác minh khi thời gian Mining một khối tăng lên trong khi số lượng Miner không thay đổi.

2.4.2. Đánh giá nền tảng đề xuất với trường hợp 2

Mỗi giao dịch được xem là hợp lệ nếu đạt được sự xác minh là hợp lệ của ít nhất 2/3 trong tổng số các Miner trong mạng. Nếu một giao dịch là hợp lệ, nó sẽ được di chuyển đến VL bởi một ứng dụng giám sát của nền tảng. Ngược lại, nó sẽ bị xóa khỏi WL. Trong trường hợp tốt nhất, giao dịch chỉ trải qua sự xác minh từ 2/3 trong tổng số Miner trong mạng. Trường hợp xấu nhất, khi các Miner không tin cậy đều đã bị thỏa hiệp bởi kẻ tấn công và chúng sẽ xác minh không trung thực, khi đó giao dịch sẽ phải trải qua sự xác minh từ tất cả các Miner trong mạng. Do đó, quá trình xác minh các giao dịch trong trường hợp này tương tự như các giao thức đồng thuận khác khi xem xét các Miner giống như một Miner, quá trình xác minh trong trường hợp xấu nhất được thể hiện ở Hình 2.10.



Hình 2.10: Quá trình xác minh các giao dịch tại giai đoạn 1 trong trường hợp 2

Trong trường hợp này, luận án so sánh nền tảng được đề xuất với giao thức *PBFT* và *Tendermint*. Vì cả hai giao thức này được sử dụng cho các mạng Blockchain có tồn tại một số Miner không tin cậy với số lượng ít hơn 1/3 trong tổng số các Miner. Có thể khái quát thuật toán đồng thuận của hai giao thức này, ký hiệu là $A2$, như sau:

Thuật toán: A2	
	Input: l giao dịch trong Pool và các Miner trong mạng **Output:** một khối mới trên sổ cái
Bước 1	(1) Lựa chọn một Miner tại mỗi vòng Mining. (2) Miner xác minh và đặt l giao dịch hợp lệ vào một khối mới. (3) Miner tạo một phiếu trên khối mới này. (4) Miner quảng bá khối mới này cùng với phiếu đến các Miner khác trong mạng.
Bước 2	Sau khi nhận được khối mới cùng phiếu, mỗi Miner thực hiện các công việc sau đây: (1) Xác minh các giao dịch trong khối. (2) Nếu tất cả các giao dịch là hợp lệ, Miner tạo một phiếu cho khối đó. (3) Quảng bá phiếu đến các Miner khác trong mạng. (4) Khi một Miner đã nhận được ít nhất 2/3 số phiếu trong tổng số các Miner trong mạng. Nó sẽ tạo một chứng chỉ cho khối này và quảng bá chứng chỉ đến các Miner khác
Bước 3	Các Miner xác minh các chứng chỉ nhận được, nếu Miner đã nhận được ít nhất 2/3 chứng chỉ hợp lệ trong tổng số các Miner trong mạng, Miner sẽ thêm khối này vào sổ cái của chúng.

Nhìn chung, cả thuật toán $A2$ và nền tảng bảo mật được đề xuất có cùng mức độ bảo mật khi tất cả các giao dịch phải được xác minh bởi ít nhất 2/3 trong tổng số Miner trong mạng. Cơ chế xác minh giao dịch và đồng bộ dữ liệu trên sổ cái của nền tảng bảo mật được đề xuất và thuật toán $A2$ không có sự khác biệt lớn về thời gian Mining và tốc độ xác minh giao dịch trong hệ thống.

Tuy nhiên, trong trường hợp một Miner không tin cậy được lựa chọn tại một vòng Mining để thực hiện việc đề xuất một khối mới cho mạng Blockchain thì nền tảng bảo mật được đề xuất của luận án sẽ tối ưu hơn thuật toán $A2$. Cụ thể, khi Miner được lựa chọn bị thỏa hiệp bởi kẻ tấn công, kẻ tấn công hoàn toàn có thể đặt một hoặc một vài giao dịch không hợp lệ cùng với các giao dịch hợp lệ khác vào trong một khối mới và sau đó quảng bá khối này đến các Miner khác trong mạng. Tất nhiên là khối mới này sẽ bị loại bỏ bởi những Miner tin cậy trong mạng. Tuy nhiên, đối với thuật toán $A2$, tất cả các giao dịch hợp lệ nằm trong khối không hợp lệ này sẽ phải xác minh lại tại các vòng Mining tiếp theo. Trong khi đó, đối với nền tảng bảo mật được đề xuất, các Miner không cần phải xác minh lại các giao dịch này bởi vì chúng vẫn còn lưu trong VL. Các giao dịch trong VL chỉ được xóa khi chúng đã được đưa vào sổ cái thành công.

Từ kết quả phân tích ở trên, có thể thấy rằng phương thức xác minh và đồng thuận dữ liệu trên sổ cái Blockchain của nền tảng được đề xuất tối ưu hiệu năng cho các Miner hơn so với thuật toán $A2$.

2.5. ĐÁNH GIÁ VỀ TÍNH CHÍNH XÁC

Tính chính xác là đảm bảo các dữ liệu lưu trữ trên sổ cái đều là các dữ liệu hợp lệ. Phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của nền tảng được đề xuất ở hai trường hợp đều đảm bảo được tính hợp lệ của dữ liệu trên sổ cái. Các Miner trong mạng Blockchain sẽ có trách nhiệm xác minh tính hợp lệ của dữ liệu trước khi lưu trữ chúng trên sổ cái. Quá trình xác minh tính hợp lệ của các giao dịch và khối mới tại mỗi vòng Mining của từng trường hợp như sau:

- Trường hợp 1: Các Miner trong một mạng Blockchain đều hoàn toàn tin cậy

- *Xác minh giao dịch*: Mỗi giao dịch chỉ cần được xác minh bởi một Miner trong mạng. Một giao dịch được xem là hợp lệ khi được sự xác minh là hợp lệ của một Miner, các giao dịch hợp lệ sẽ được lưu vào VL.
- *Xác minh khối mới*: Tại mỗi vòng Mining một Miner được lựa chọn để đặt các giao dịch trong VL vào một khối mới, sau đó tạo chữ ký số trên khối mới này và quảng bá chúng đến các Miner khác. Các Miner khác sẽ xác minh tính hợp

lệ của chữ ký số trên khối mới này. Nếu chữ ký số hợp lệ, các Miner sẽ thêm khối mới này vào sổ cái của chúng, ngược lại bỏ qua khối mới này.

- Trường hợp 2: Trong một mạng Blockchain có tồn tại một số Miner không đáng tin cậy nhưng số lượng ít hơn 1/3 trong tổng số Miner trong mạng.

  - *Xác minh giao dịch:* Một giao dịch được xem là hợp lệ nếu đạt được sự xác minh là hợp lệ của ít nhất 2/3 trong tổng số các Miner trong mạng, các giao dịch hợp lệ sẽ được lưu vào *VL*.

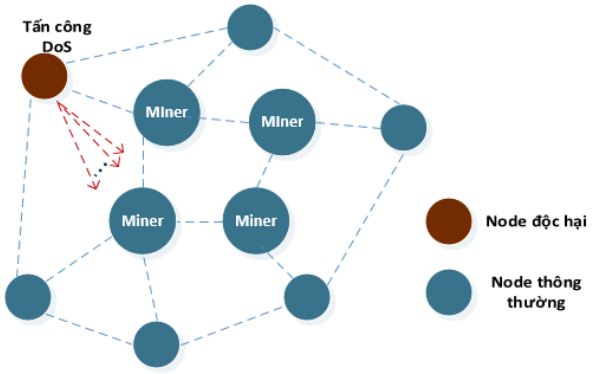
  - *Xác minh khối mới*: Tại mỗi vòng Mining một Miner được lựa chọn để đặt các giao dịch trong VL vào một khối mới, sau đó tạo chữ ký số trên khối mới này và quảng bá chúng đến các Miner khác. Các Miner khác sẽ xác minh tính hợp lệ của chữ ký số trên khối mới này và kiểm tra xem các giao dịch trong khối mới này có nằm trong VL hay không. Nếu chữ ký số hợp lệ và các giao dịch trong khối mới này đều thuộc VL, các Miner sẽ thêm khối mới này vào sổ cái của chúng, ngược lại bỏ qua khối mới này.

Các phân tích nêu trên cho thấy rằng, dữ liệu lưu trữ trên sổ cái của Miner ở hai trường hợp đều đảm bảo được tính chính xác của dữ liệu.

2.6. ĐỀ XUẤT ÁP DỤNG GIẢI PHÁP PHÁT HIỆN NHANH CÁC HOT-IP

Trong một mạng IoT sẽ có nhiều thiết bị tham gia vào, mỗi thiết bị có đặc tính và mức độ bảo mật khác nhau. Trong trường hợp một hoặc một vài thiết bị IoT bị nhiễm mã độc hoặc bị thỏa hiệp bởi kẻ tấn công, khi đó thiết bị này có thể thực hiện tấn công từ chối dịch vụ đến các Miner trong nền tảng. Việc tấn công từ chối dịch vụ có thể thực hiện bằng cách gửi rất nhiều giao dịch không hợp lệ trong một khoảng thời gian ngắn đến các Miner nhằm làm giảm hiệu suất trong việc xác minh các giao dịch của các Miner, hoặc có thể thực hiện bằng cách gửi nhiều gói dữ liệu có kích thước lớn trong một khoảng thời gian ngắn nhằm làm tràn ngập băng thông mạng của các Miner. Hình 2.11 thể hiện nguy cơ tấn công từ chối dịch vụ từ các Node độc hại lên các Miner trong nền tảng.

Nhằm phát hiện nhanh các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng, luận án đề xuất áp dụng giải pháp hiện nhanh các Hot-IP trên các Miner trong nền tảng được đề xuất. Hot-IP là những IP có tần suất xuất hiện cao trong mạng trong một khoảng thời gian rất ngắn. Các Hot-IP này có khả năng là tấn công từ chối dịch vụ đang xảy ra trong mạng [13]. Việc nhận diện nhanh các Hot-IP sẽ giúp người quản trị hệ thống Blockchain nhanh chóng đưa ra các giải pháp phòng thủ kịp thời nhằm duy trì tính ổn định của hệ thống.



Hình 2.11: Nguy cơ tấn công DoS từ các Node độc hại

Phương pháp phát hiện nhanh các Hot-IP trên mạng dựa vào phương pháp thử nhóm bất ứng biến và thuật toán được triển khai trên các Miner cho kết quả tốt khi xử lý dữ liệu trong thời gian thực.

Trong thuật toán này, tham số *current_timestamp* là thời gian các gói tin đến, *reference_timestamp* là điểm bắt đầu của chu kỳ thuật toán, Δ là thời gian một chu kỳ thuật toán, Hot-List là danh sách chứa địa chỉ các IP nghi ngờ, δ là ngưỡng tần suất cao.

Trong chu kỳ thực hiện thuật toán, các gói tin được trích xuất địa chỉ IP, nếu nó tồn tại trong danh sách này thì tăng bộ đếm tương ứng cho IP này. Nếu chưa tồn tại trong Hot-List thì việc cập nhật cho các nhóm thử chứa IP này được thực hiện bình thường như trong thuật toán thử nhóm bất ứng biến truyền thống. Khi bất kỳ một nhóm nào trong quá trình cập nhật IP mới vào làm vượt ngưỡng tần suất cao, địa chỉ IP đó được đưa vào danh sách nghi ngờ Hot-List, khởi tạo bộ đếm tương ứng bằng cách lấy giá trị nhỏ nhất trong các nhóm mà IP này thuộc về, các nhóm vượt ngưỡng sẽ dừng việc cập nhật. Thuật toán xuất các Hot-IP phát hiện được trong một chu kỳ

thuật toán trong Hot-List vượt ngưỡng. Thuật toán phát hiện nhanh các Hot-IP được luận án áp dụng như sau:

Thuật toán: Online Hot-IP Detecting	
	Input: Ma trận d-phân-cách, dòng gói tin IP trong khoảng thời gian Δ, ngưỡng δ **Ouput:** Các Hot-IP
1:	*Hot-List = {}*
2:	*For each IP* $j \in S_\Delta$
3:	*If (current_timestamp– reference_timestamp <* Δ*) then*
4:	*If IP* $j \in$ *Hot-List then*
5:	*Hot-List[j].count++*
6:	*Else*
7:	*For i = 1 to t //t là số nhóm thử hay số dòng của ma trận*
8:	*If* m_{ij} *= 1 and* $c_i < \delta$ *then* c_i*++*
9:	*If* $c_i \geq \delta$ *then*
10:	*Hot-List = Hot-List* $\cup$ *{j}*
11:	*Hot-List[j].count = min{*c_i *|* m_{ij}*=1}*
12:	*EndIf*
13:	*EndFor*
14:	*Else*
15:	*Return {j	Hot-List[j].count*$\geq \delta$*,* $1 \leq j \leq$ *| Hot-List |}*
16:	*Reference_timestamp=current_timestamp*
17:	*Reset Hot-List*
18:	*EndIf*

Từ các Hot-IP phát hiện được trong thời gian thực, các Miner có thể thực hiện các chính sách hạn chế hoạt động của chúng nhằm giảm các nguy cơ và đảm bảo hệ thống hoạt động ổn định và thông suốt. Đề xuất này được công bố trong công trình [CT7] trong danh mục các công trình nghiên cứu của tác giả.

2.7. KẾT LUẬN CHƯƠNG 2

Trong chương này, luận án giới thiệu về công nghệ Blockchain, một số giao thức đồng thuận thường được sử dụng trong các nền tảng bảo mật dựa trên Blockchain cho IoT, các loại mạng Blockchain và các hình thức tấn công bảo mật giả định trên Blockchain. Luận án trình bày kiến trúc, phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của các Miner trong nền tảng bảo mật được đề xuất. Trong đó, quá trình xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain dựa trên hai trường hợp về các Miner trong một mạng Blockchain. Trường hợp 1, tất cả các Miner là hoàn toàn tin cậy. Trường hợp 2, trong mạng có tồn tại một số Miner không tin cậy với số lượng ít hơn 1/3 trong tổng số các Miner trong mạng. Có thể áp dụng nền tảng bảo mật trong trường hợp 1 cho các mạng Private Blockchain và trường hợp 2 cho các mạng Consortium Blockchain.

Luận án khái quát thành thuật toán đồng thuận $A1$ cho các giao thức đồng thuận *PoW, PoS, PoA, PoAh, DPoS, PBFT*, và *Tendermint.* Bên cạnh đó, luận án cũng khái quát thuật toán đồng thuận *PBFT* và *Tendermint* thành thuật toán $A2$. Từ đó, luận án tiến hành so sánh phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái giữa nền tảng được đề xuất ở trường hợp 1 với thuật toán $A1$, và trường hợp 2 với thuật toán $A2$.

Kết quả đánh giá bằng thuật toán và bằng thực nghiệm cho thấy rằng, nền tảng bảo mật được đề xuất của luận án ở trường hợp 1 có hiệu năng cao hơn so với các nền tảng bảo mật sử dụng một trong các giao thức đồng thuận *PoW, PoS, PoA, PoAh, DPoS, PBFT,* và *Tendermint* trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain.

Đối với trường hợp 2, luận án đã so sánh nền tảng bảo mật được đề xuất với giao thức đồng thuận *PBFT* và *Tendermint.* Hai giao thức này đại diện cho nhóm các thức đồng thuận *PoW, PoS, PoA, PoAh, DPoS, PBFT,* và *Tendermint* vì chúng có thể được sử dụng trong một mạng Blockchain có tồn tại một số Miner không tin cậy với số lượng ít hơn 1/3 trong tổng số các Miner. Điều kiện này tương đồng với nền tảng bảo mật được đề xuất trong trường hợp 2. Kết quả so sánh cho thấy rằng nền tảng

được đề xuất tối ưu hơn trong việc xác minh các giao dịch trong trường hợp một Miner không tin cậy được chọn tại một vòng Mining. Bởi vì các giao dịch trong nền tảng được đề xuất không cần phải xác minh lại tại các vòng Mining kế tiếp.

Luận án đề xuất áp dụng giải pháp phát hiện nhanh các Hot-IP trên các Miner trong nền tảng để giảm thiểu tối đa các nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng.

Từ kiến trúc, phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain của nền tảng bảo mật được đề xuất, luận án tiến hành xây dựng các chức năng bảo mật cụ thể như: chức năng lưu trữ và chia sẻ dữ liệu đảm bảo tính riêng tư được trình bày ở Chương 3; và chức năng kiểm soát truy cập tài nguyên IoT theo thời gian được cấp phép được trình bày ở Chương 4.

CHƯƠNG 3: LƯU TRỮ VÀ CHIA SẺ DỮ LIỆU ĐẢM BẢO TÍNH RIÊNG TƯ

Chương này trình bày tổng quan về nền tảng lưu trữ phi tập trung IPFS, phương thức chữ ký nhóm. Từ đó, luận án đề xuất chức năng lưu trữ và chức năng chia sẻ dữ liệu đảm bảo tính riêng tư của nền tảng bảo mật, thực hiện đánh giá các tính chất bảo mật mà các phương thức đã đạt được. Chương này được tổng hợp từ các công trình [CT1], [CT4], [CT6] và [CT8] trong danh mục các công trình nghiên cứu của tác giả.

3.1. GIỚI THIỆU

Ngày nay, tốc độ tăng trưởng dữ liệu trên toàn thế giới tăng theo cấp số nhân. Theo đánh giá của Rydning và cộng sự [54] đến năm 2024 khoảng 6 tỷ người dùng tương tác với dữ liệu mỗi ngày. Do đó, nhu cầu lưu trữ và chia sẻ dữ liệu là rất lớn, điều này cũng đặt ra những thách thức liên quan đến an toàn bảo mật dữ liệu trong quá trình lưu trữ và chia sẻ.

Dữ liệu số được cấp chứng chỉ bởi những tổ chức có uy tín được xem là dữ liệu số có giá trị hoặc dữ liệu số đáng tin cậy. Các dữ liệu này được xem là một trong những tài sản có giá trị của các cá nhân và tổ chức, chúng có thể được lưu trữ hoặc chia sẻ/mua bán trên Internet. Tuy nhiên, các vấn đề đặt ra là: (1) làm sao đảm bảo được tính ẩn danh của thành viên trong tổ chức cấp chứng chỉ? (2) làm sao để đảm bảo các dữ liệu này được lưu trữ an toàn trên hệ thống lưu trữ? (3) làm thế nào để mọi người trên mạng có thể kiểm chứng được tính tin cậy của dữ liệu được chia sẻ nhưng vẫn đảm bảo được tính riêng tư và bí mật về nội dung? và (4) làm sao đảm bảo quá trình chia sẻ dữ liệu được an toàn, minh bạch và công bằng?

Xuất phát từ thực tế như vậy, luận án đề xuất phương thức tạo dữ liệu, phương thức lưu trữ dữ liệu và phương thức chia sẻ dữ liệu đảm bảo tính riêng tư. Hai phương thức lưu trữ dữ liệu và chia sẻ dữ liệu là hai chức năng của nền tảng bảo mật được đề xuất ở Chương 2.

Các khối trong sổ cái Blockchain không thể chứa các dữ liệu lớn (hàng chục/trăm Megabyte trở lên). Nếu kích thước khối lớn sẽ làm cho mạng Blockchain hoạt động không hiệu quả bởi vì thời gian đồng bộ dữ liệu trên sổ cái sẽ rất chậm do độ trễ từ mạng và tốn nhiều nguồn lực tính toán của các Miner. Do đó, luận án sử dụng một hệ thống lưu trữ để lưu các dữ liệu số có giá trị. Luận án chọn IPFS làm hệ thống lưu trữ bởi vì đây là một nền tảng lưu trữ phi tập trung, sẽ tránh được vấn đề một điểm chết so với các hệ thống lưu trữ tập trung. Các mô hình kết hợp giữa Blockchain và IPFS đã được công bố ở công trình [CT6] và [CT8] trong danh mục các công trình nghiên cứu của tác giả. Bên cạnh đó, luận án sử dụng phương thức chữ ký nhóm để đảm bảo tính ẩn danh cho tổ chức cấp chứng chỉ và tính riêng tư cho những người sử dụng dịch vụ từ các tổ chức cấp chứng chỉ.

Trong phần tiếp theo, luận án sẽ trình bày các thành phần được sử dụng trong các phương thức được đề xuất, bao gồm: nền tảng lưu trữ phi tập trung IPFS, phương thức chữ ký nhóm. Sau đó, luận án sẽ trình bày mô hình hệ thống, các phương thức đề xuất và đánh giá các tính chất bảo mật đạt được của các phương thức được đề xuất.

3.2. NỀN TẢNG LƯU TRỮ IPFS

IPFS được đề xuất bởi Juan Benet vào năm 2014 [6], là một hệ thống tệp phân tán ngang hàng cung cấp một phương tiện truyền dữ liệu hiệu quả trên một khoảng cách lớn. IPFS tìm cách kết nối tất cả các thiết bị (hay còn gọi là Node) tính toán thành một hệ thống tệp tin duy nhất. Vì vậy, IPFS còn được gọi là Web phân tán, hoặc Web cố định.

Trong mạng IPFS, các Node giao tiếp trực tiếp với nhau mà không cần thông qua bất kỳ hệ thống trung tâm nào. Mỗi Node được khởi tạo một cặp khóa gồm một khóa riêng và một khóa công khai tương ứng bởi một thuật toán mật mã khóa công khai. Trong đó, khóa riêng được sử dụng để tạo chữ ký trong dịch vụ IPNS, khóa công khai được dùng để tạo định danh cho Node và được công khai để các Node khác sử dụng trong việc xác minh chữ ký. Trước khi trao đổi dữ liệu, các Node phải thiết lập kết nối bằng cách trao đổi khóa công khai với nhau, sau đó các Node sẽ kiểm tra

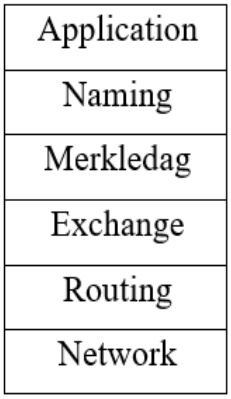
định danh của Node có tương ứng với khóa công khai đã trao đổi trước đó hay không, nếu thông tin không chính xác kết nối sẽ bị hủy bỏ.

Có 3 loại Node trong mạng IPFS là: Client Node, Retrieval Miner Node, và Storage Miner Node [21]:

- *Client Node:* loại Node này chỉ sử dụng mạng IPFS để lưu trữ và truy cập dữ liệu, chúng không cung cấp không gian lưu trữ cho mạng IPFS.
- *Retrieval Miner Node:* các Node thuộc loại này sẽ cung cấp không gian lưu trữ cho mạng. Loại Node này có nhiệm vụ lưu trữ dữ liệu tạm thời và phân phối dữ liệu cho các Node khác trong mạng.
- *Storage Miner Node:* loại Node này sẽ cung cấp dung lượng lưu trữ lớn, đóng vai trò quan trọng trong mạng. Các Node thuộc loại này có thể bật các chức năng Pinning và Clustering, hai chức năng này sẽ được trình bày tại mục 3.2.2.

3.2.1. Các tầng giao thức của IPFS

IPFS bao gồm một chồng các giao thức, mỗi giao thức đảm nhận các chức năng khác nhau [6], chồng giao thức IPFS được thể hiện ở Hình 3.1.



Hình 3.1: Các tầng giao thức của IPFS [73]

Mỗi Node trong mạng IPFS có một định danh NodeID, được khởi tạo thông qua phương thức S/kademlia [5]. Trong đó, NodeID được tạo phải thỏa mãn một độ khó cho trước nhằm chống hình thức tấn công Sybil và Eclipse. Độ khó ở đây chính là số lượng bit 0 đầu tiên trong chuỗi băm mật mã được tạo ra từ khóa công khai của Node. Chi tiết về thuật toán tạo NodeID như sau:

Thuật toán tạo NodeID	
	Input: *difficulty* **Output:** *NodeId*
1:	*difficulty = <integer parameter>*
2:	*n = Node{}*
3:	*do {*
4:	*n.PubKey, n.PrivKey = PKI.genKeyPair()*
5:	*n.NodeId = hash(hash(n.PubKey))*
6:	*p = count_preceding_zero_bits(n.NodeId)*
7:	*} while (p < difficulty)*

Chức năng của các tầng giao thức *Network, Routing, Exchange, Merkle Dag, Naming* trong IPFS như sau:

a. Network

Tầng này có chức năng quản lý và thiết lập các kết nối đến các Node trong mạng. Các giao thức mạng có thể được sử dụng ở tầng này như: TCP, UDP, WebRTC.

b. Routing

Định tuyến trong IPFS là quá trình xác định vị trí của các Node lưu trữ các tệp dữ liệu nhất định đang được yêu cầu từ các Node khác trong mạng. Mỗi tệp dữ liệu được định danh thông qua giá trị băm của nội dung tệp, chúng được gọi là key. Kết quả của quá trình truy vấn đến một key sẽ là địa chỉ của Node đang lưu trữ value tương ứng với key. IPFS sử dụng một trong các bảng băm phân tán như Kademlia, S/Kademlia, Coral để phục vụ định tuyến.

❖ *Kademlia DHT* [41]:

Kademlia là một hệ thống lưu trữ và truy vấn ngang hàng, lưu trữ các cặp <key, value>. Mỗi key và NodeID nằm trong không gian khóa 160 bit, mỗi Node chịu trách nhiệm lưu trữ cho các cặp <key, value> sao cho key "gần" với NodeID. Khái niệm "gần" được xác định thông qua phép XOR metric để đo khoảng cách giữa các Node trong không gian khóa. Thuật toán định tuyến dựa trên NodeID cho phép

xác định các Node gần khóa đích (key được truy vấn). Cho *x*, *y* thuộc không gian 160-bit, khoảng cách giữa *x* và *y* là: $d(x,y) = x \oplus y$. Với mọi điểm *x* và khoảng cách đã cho Δ **(**$\Delta > 0$**)**, có chính xác một điểm *y* sao cho $d(x,y) = \Delta$.

Mỗi Node lưu trữ *n* k-bucket (với *n* là số bít của NodeID), mỗi k-bucket có thể chứa tối đa *k* mục thông tin của các Node với một khoảng cách *d*, với $2^i \leq d < 2^{i+1}, 0 \leq i < n$**,** khoảng cách *d* được tính bằng cách XOR metric giữa hai Node. Mỗi mục thông tin bao gồm <địa chỉ IP, Protocol, Port, NodeID>. Hình 3.2 thể hiện k-bucket trong bảng băm phân tán.

Số lượng	Khoảng cách	K-bucket
0	$[2^0, 2^1)$	$k - bucket$
1	$[2^1, 2^2)$	$k - bucket$
2	$[2^2, 2^3)$	$k - bucket$
...		
n-1	$[2^{n-1}, 2^n)$	$k - bucket$

Hình 3.2: K-bucket trong bảng băm phân tán

Khi một Node nhận một thông điệp từ một Node khác, nó sẽ trích xuất thông tin địa chỉ của Node gửi. Thông qua việc tính khoảng cách giữa NodeID của nó với NodeID của Node gửi, Node sẽ cập nhật thông tin này vào k-bucket tương ứng trong bảng băm phân tán của nó. Nếu thông tin của Node gửi đã có trong một k-bucket thì Node sẽ di chuyển thông tin này vào cuối danh sách trong k-bucket tương ứng. Nếu thông tin của Node gửi chưa có và k-bucket chưa đầy thì thêm thông tin này vào cuối danh sách, ngược lại nếu k-bucket đã đầy thì Node sẽ kiểm tra trạng thái của Node ít được nhìn thấy gần nhất. Nếu Node đó không phản hồi thì xóa khỏi danh sách và cập nhật thông tin Node gửi vào danh sách, ngược lại nếu Node được kiểm tra đang hoạt động thì xóa thông tin của Node gửi.

Có 4 thủ tục gọi từ xa của giao thức Kademlia bao gồm: Ping, Store, Find_Node, Find_Value. Trong đó, thủ tục Ping được sử dụng để kiểm tra trạng thái hoạt động của Node, được sử dụng trong việc cập nhật k-bucket; thủ tục Store được sử dụng để yêu cầu một Node lưu trữ cặp <key, value>; Find_Node được sử dụng khi một Node muốn truy vấn đến một NodeID. Khi một Node *P* tra cứu đến một

NodeID (gọi là *T*), *P* lấy *α* Node trong các k-bucket gần với *T* trong bảng băm phân tán của nó. Trong trường hợp không đủ *α* Node thì *P* chỉ lấy các Node mà nó biết. *P* thực hiện gọi thủ tục Find_Node và truy vấn song song trên *α* Node này. Node nhận thủ tục này trả lại thông tin của nhiều nhất *k* Node gần với *T*. Khi *P* nhận được phản hồi từ một Node, nó cập nhật vào k-bucket thích hợp về NodeID của Node gửi, và tiếp tục gửi α yêu cầu mới đến những Node mà chưa từng truy vấn từ danh sách phản hồi. Các Node không phản hồi sẽ được xóa khỏi k-bucket tương ứng.

Nếu trong một vòng truy vấn mà *P* không nhận được một Node gần hơn so với các Node mà nó đã có, *P* sẽ gửi truy vấn đến *k* Node gần *T* mà nó chưa truy vấn trong danh sách phản hồi. Quá trình truy vấn kết thúc khi *P* đã thực hiện truy vấn và nhận được phản hồi từ *k* Node này. Đối với thủ tục Find_Value, khi một Node cần truy vấn một value của một key, Node sẽ gửi thủ tục Find_Value đến *k* Node gần với key, quá trình truy vấn sẽ kết thúc ngay lập tức khi có bất kỳ Node nào phản hồi về giá trị value tương ứng. Các cặp <key, value> trong bộ nhớ cache sẽ hết hạn trong vòng 24 giờ. Giá trị *k* và *α* được khuyến nghị chọn là *k* =20, α=3.

- S/*Kademlia*: Giao thức này được cải tiến từ giao thức Kademlia tại các điểm sau:
  - Phương thức tạo NodeID cho Node phải đáp ứng yêu cầu về độ khó nhằm chống hình thức tấn công Sybil và Eclipse.
  - Phương thức truy vấn value: truy vấn song song trên nhiều đường dẫn khác nhau để tăng tỉ lệ truy vấn thành công.
- *Coral distributed sloppy hash table (Core DSHT)*: Giao thức này được mở rộng từ giao thức Kademlia với các cải tiến sau:
  - Kademlia lưu các giá trị tại các Node có NodeID gần nhất với key, điều này gây lãng phí băng thông và không gian lưu trữ. Coral cải tiến bằng cách chỉ cho Node lưu các địa chỉ của Node có thể cung cấp các khối dữ liệu.
  - Coral sử dụng phương thức get_any_value(key) thay vì dùng get_value(key). Khi đó một tập con của các value sẽ được phân phối từ các Node gần nhất. Cách này sẽ tránh trường hợp tắt nghẽn khi phục vụ các value phổ biến đến các Node khác trong mạng.

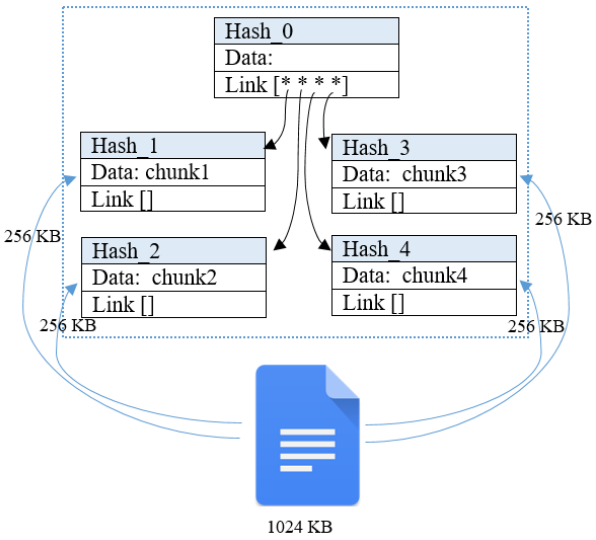
- Coral tổ chức một hệ thống phân cấp, mỗi cấp được quản lý bởi một cluster. Các Node thực hiện truy vấn đến Node Cluster trong khu vực của Node mà không cần truy vấn trực tiếp đến các Node ở xa. Cách này làm giảm độ trễ của truy vấn.

c. Exchange

Tầng này sử dụng giao thức Bitswap để trao đổi các khối dữ liệu. Các Node trao đổi dữ liệu thông qua 2 danh sách: Want_list chứa các khối muốn được nhận, Have_list chứa danh sách các khối đang sở hữu và dùng để gửi cho các Node khác đang cần. Lịch sử trao đổi các khối dữ liệu sẽ được lưu trong sổ cái Bitswap. Khi thiết lập kết nối, các Node trao đổi thông tin sổ cái Bitswap, các chỉ số này được sử dụng để đánh giá sự tin cậy của các Node trong mạng. Từ đó có thể xác định độ ưu tiên trong việc trao đổi dữ liệu giữa các Node trong mạng.

d. Merkle Dag

Merkle Dag là một đồ thị không chu trình phân tán. Trong đó, các liên kết đến các đối tượng (hay còn gọi là Object) là các giá trị băm mật mã của đối tượng. Khi tải một tệp lên IPFS, nội dung của tệp sẽ được đặt vào trong các Object. Mỗi Object là một cấu trúc dữ liệu gồm 2 trường: trường data được sử dụng để lưu trữ dữ liệu dạng nhị phân; trường link là một mảng của các liên kết đến các Object có liên quan khác.



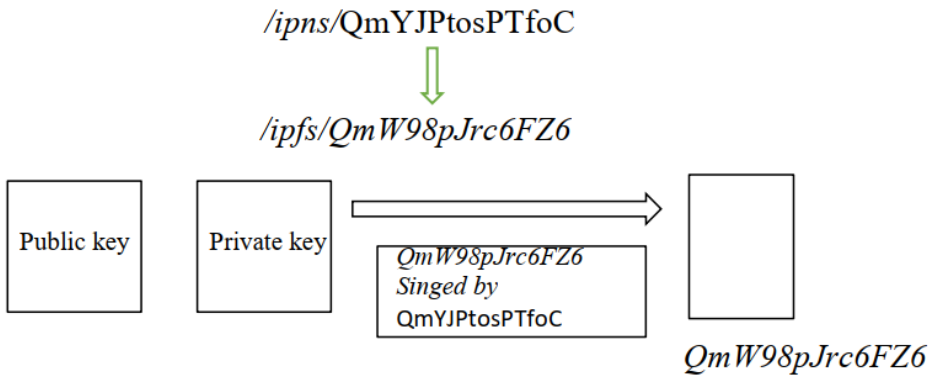
Hình 3.3: Cấu trúc một Object trong Merkle Dag

Mỗi Object có kích thước tối đa 256 kilobyte. Nếu một tệp có kích thước nhỏ hơn 256 kilobyte sẽ được lưu trong một Object với phần link của Object trống. Ngược lại, tệp đó sẽ được chia ra thành các phần có kích thước nhỏ hơn 256 kilobyte được gọi là các Chunk, và sử dụng cấu trúc cây Merkle Dag để quản lý các Chunk này.

Cấu trúc của một link gồm 3 phần: Name là tên của link, Hash chứa giá trị băm của Object được liên kết, và Size là kích thước của đối tượng được liên kết. Ví dụ về cấu trúc Merkle Dag của một Object được thể hiện ở Hình 3.3.

e. Naming

Mỗi Object trong IPFS được định danh thông qua giá trị băm của nội dung của nó. Giá trị băm này được xem như là địa chỉ truy cập của Object đó trong mạng, các Node khác truy cập Object thông qua định danh này. Khi một Object thay đổi nội dung để tạo thành một phiên bản mới thì Object đó cũng sẽ tạo ra một định danh mới. Để có thể sử dụng một địa chỉ truy cập cho một Object thường hay thay đổi nội dung, IPFS sử dụng hệ thống đặt tên IPNS. Hệ thống đặt tên này được xây dựng dựa trên hệ thống tập tin tự chứng nhận (Self-Certified File System -SFS). Trong đó, mỗi Node được gắn một không gian tên có thể thay đổi */ipns/NodeID*, mỗi Node có thể công khai một Object đến đường dẫn này và được ký bởi khóa riêng của Node. Cách thức hoạt động của IPNS được thể hiện ở Hình 3.4. Trong đó, một Object có địa chỉ truy cập *ipfs/QmW98pJrc6FZ6* sẽ được ánh xạ đến một định danh của Node */ipns/QmYJPtosPTfoC*. Khi một Node nhận được Object này, Node sẽ kiểm tra tính hợp lệ của chữ ký với khóa công khai và NodeID.



Hình 3.4: Cách thức hoạt động của tầng IPFS Naming

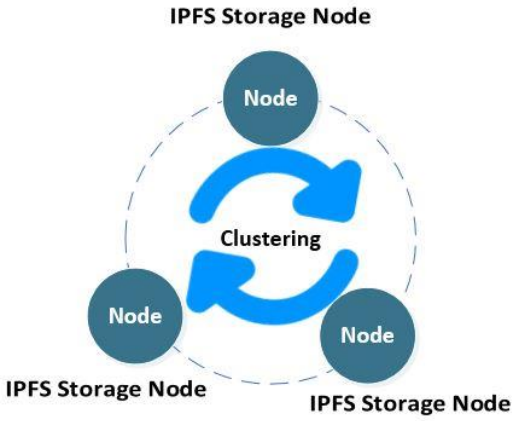
3.2.2. Các dịch vụ trong IPFS

a. IPFS Pinning

Dữ liệu lưu trữ trên IPFS mặc định sẽ xóa bởi chức năng thu gom rác nhằm tạo không gian trống để lưu trữ dữ liệu mới. Chức năng thu gom rác sẽ thực thi định kỳ trên các Node hoặc khi dữ liệu trong bộ nhớ đạt đến một giới hạn được thiết lập trong cấu hình. Để lưu trữ dữ liệu lâu dài trên Node, IPFS cung cấp chức năng ghim dữ liệu, các dữ liệu quan trọng sau khi được ghim sẽ không bị xóa bởi chức năng thu gom rác. Dữ liệu cũng có thể được ghim trên nhiều Node, điều này làm tăng tính dự phòng cho dữ liệu [28].

b. IPFS Clustering

IPFS clustering cung cấp chức năng đồng bộ dữ liệu và ghim dữ liệu giữa các storage Miner Node. Các Node chạy chức năng này thường có dung lượng lưu trữ lớn và hiệu năng xử lý cao. Các Node chạy cùng một Cluster chia sẻ cùng nhau một khóa bí mật [27]. Hình 3.5 thể hiện dịch vụ IPFS Clustering.



Hình 3.5: Dịch vụ IPFS Clustering

3.3. CHỮ KÝ NHÓM

Chữ ký nhóm được đề xuất bởi Chaum và van Heyst vào năm 1991 [12]. Các thành phần tham gia trong một phương thức chữ ký nhóm bao gồm: các thành viên của nhóm (Group members), một người quản lý nhóm (Membership manager) và một người quản lý thu hồi (Revocation manager). Phương thức chữ ký nhóm cho phép một thành viên trong nhóm đại diện cho nhóm ký ẩn danh lên các thông điệp. Người

xác minh chữ ký chỉ kiểm tra được tính hợp lệ của chữ ký nhóm nhưng không thể biết chính xác thành viên nào trong nhóm đã ký. Người quản lý nhóm có trách nhiệm thiết lập chữ ký và thêm thành viên trong nhóm. Trong khi đó, người quản lý thu hồi có khả năng thu hồi tính ẩn danh của chữ ký.

Định nghĩa 1 (Chữ ký nhóm). *Một phương thức chữ ký nhóm GS=(KeyGen, Sign, Verify, Tracing, Vertracing) bao gồm 5 thuật toán sau [10][12]:*

- $(gpk, gmk, grk, gsk) \leftarrow KeyGen(1^{\lambda}, 1^{n})$: đầu vào của thuật toán bao gồm 1^{λ} và 1^{n}. Trong đó, λ là một tham số bảo mật, n là số lượng thành viên trong nhóm. Đầu ra là một khóa công khai của nhóm gpk, một khóa bí mật của người quản lý nhóm gmk, một khóa bí mật của người quản lý thu hồi grk, và gsk là một vector n phần tử của các khóa thành viên, với $gsk[i]$ là khóa bí mật của thành viên thứ i, $1 \leq i \leq n$.
- $\sigma \leftarrow Sign(gpk, gsk[i], M)$: đầu vào của thuật toán bao gồm một khóa công khai của nhóm gpk, một khóa bí mật của thành viên thứ i $gsk[i]$, và một thông điệp M. Đầu ra của thuật toán là một chữ ký σ.
- $0, 1 \leftarrow Verify(gpk, M, \sigma)$: đầu vào của thuật toán bao gồm một khóa công khai của nhóm gpk, một thông điệp M, và một chữ ký σ. Đầu ra là 1 nếu chữ ký là hợp lệ và 0 nếu chữ ký không hợp lệ.
- $(i, arg) \leftarrow Tracing(\sigma, M, grk, gpk)$: đầu vào của thuật toán bao gồm một chữ ký σ, một thông điệp M, một khóa bí mật của người quản lý thu hồi grk và một khóa công khai của nhóm gpk. Đầu ra gồm một định danh $i \in \{1, \dots, n\}$ và một tham số arg.
- $0, 1 \leftarrow Vertracing(\sigma, M, gpk, i, arg)$: đầu vào của thuật toán bao gồm một chữ ký σ, một thông điệp M, một khóa công khai của nhóm gpk, một định danh i và một tham số arg. Đầu ra là giá trị 1 nếu arg đã được tạo từ thuật toán *Tracing*, ngược lại trả về giá trị 0.

Trong đó, thuật toán *KeyGen* được dùng để thiết lập khóa cho các đối tượng trong nhóm; thuật toán *Sign* được sử dụng để tạo chữ ký nhóm; thuật toán *Verify* được

sử dụng để xác minh chữ ký; thuật toán *Tracing* được người quản lý thu hồi sử dụng để xác minh định danh của người thực hiện chữ ký; thuật toán *Vertracing* được người quản lý nhóm sử dụng để xác minh tính chính xác của thuật toán *Tracing*, từ đó biết được danh tính của thành viên có định danh được cung cấp từ thuật toán *Tracing*.

Một phương thức chữ ký nhóm cần phải đáp ứng các yêu cầu bảo mật [12]: *unforgeability*, *anonymity*, *unlinkability*, *no framing*, và *unforgeability of tracing verification*.

3.4. CÁC PHƯƠNG THỨC ĐỀ XUẤT

Gọi $H: \{0,1\}^* \rightarrow \{0,1\}^r$ là một hàm băm mật mã nhận một chuỗi bit có độ dài tùy ý hữu hạn và tạo ra một chuỗi bít có độ dài cố định bằng r bit. Ký hiệu || là phép kết nối chuỗi. Gọi $make\_proc(x)$ là hàm tạo ra một dữ liệu số từ một dữ liệu thô x. Ký hiệu $:\equiv$ là một thủ tục có thể thực hiện bằng sự tương tác của con người. Gọi $Rand\_key(\cdot)$ là hàm tạo khóa ngẫu nhiên. $E_K(M)$ và $D_K(M)$ lần lượt là thuật toán mã hóa và giải mã tương ứng của thông điệp M với cùng một khóa bí mật K. $PCS(M, K)$ là một hệ mật mã khóa công khai với thông điệp M và một khóa K.

3.4.1. Mô hình hệ thống

Hệ thống bao gồm 5 thành phần, được thể hiện ở Hình 3.6.

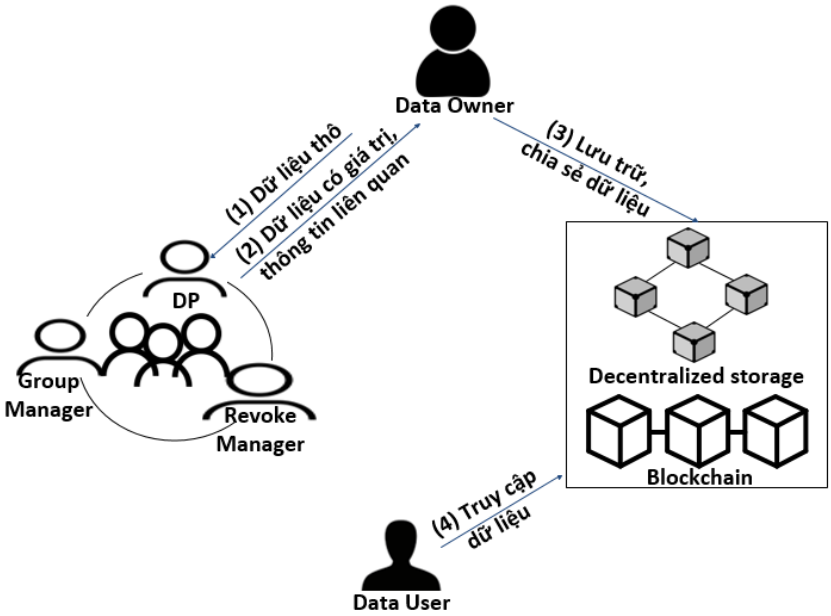
(i) **Data Owner (DO)**: Người sở hữu dữ liệu được ký hiệu là DO, DO là một cá nhân sở hữu dữ liệu thô (ký hiệu là RD). DO cung cấp RD cho một nhà cung cấp dữ liệu cụ thể để tạo ra dữ liệu có nghĩa (ký hiệu là MD), DO là người sở hữu dữ liệu nên DO có quyền lưu trữ hoặc chia sẻ MD đến người có nhu cầu sử dụng;

(ii) **Một nhóm các Data Provider**: Một nhóm các nhà cung cấp dữ liệu được tạo từ một người quản lý nhóm, mỗi Data Provider (ký hiệu là DP) là một tổ chức có chức năng và phương tiện để tạo ra MD từ RD của DO. DP không phải là người sở hữu MD nên không có quyền cung cấp hoặc sử dụng MD mà không có sự đồng ý của DO. Các DP trong cùng một nhóm cung cấp cùng một loại dịch vụ, ví dụ: một nhóm các bệnh viện, một nhóm các trường đại học, …

(iii) **Data User (DU)**: Người dùng dữ liệu được ký hiệu là DU, DU là người muốn sử dụng MD được tạo bởi DP.

(iv) **Decentralized Storage (DS)**: Hệ thống lưu trữ phi tập trung được ký hiệu là DS, DS lưu trữ bản mã hóa của MD (ký hiệu là EMD) và trả về địa chỉ truy cập của EMD đến DU. Luận án sử dụng mạng public IPFS để làm DS.

(v) **Blockchain:** Blockchain chính là nền tảng bảo mật được đề xuất ở Chương 2. Trong đó, có thể sử dụng nền tảng bảo mật theo trường hợp 1 hoặc trường hợp 2. Ở chương này, luận án chỉ tập trung vào vấn đề chính là trình bày các phương thức tạo dữ liệu, lưu trữ và chia sẻ dữ liệu. Blockchain được sử dụng để lưu trữ các thông tin của MD và phục vụ cho quá trình chia sẻ dữ liệu. Người quản lý nhóm sẽ triển khai các chính sách chia sẻ dữ liệu thông qua một hợp đồng thông minh trên Blockchain.



Hình 3.6: Mô hình hệ thống lưu trữ và chia sẻ dữ liệu

Hệ thống cung cấp ba phương thức: phương thức tạo dữ liệu, phương thức lưu trữ dữ liệu và phương thức chia sẻ dữ liệu.

❖ Phương thức tạo dữ liệu: Dữ liệu đầu vào là RD từ DO, dữ liệu đầu ra được tạo từ DP bao gồm: MD, chứng chỉ của dữ liệu, thông tin của DP. Để đảm bảo tính

bí mật cho MD, DP sẽ mã hóa MD thành EMD. Dữ liệu đầu ra của phương thức này sẽ được chuyển đến DO.

- Phương thức lưu trữ dữ liệu: Cho EMD, chứng chỉ của dữ liệu và một số thông tin quản lý làm dữ liệu đầu vào. EMD sẽ được lưu trữ trên IPFS và một giao dịch lưu trữ dữ liệu trên Blockchain chứa các thông tin: địa chỉ truy cập của EMD trên IPFS, chứng chỉ của dữ liệu, và môt số thông tin quản lý.
- Phương thức chia sẻ dữ liệu: Cho trước một giao dịch lưu trữ dữ liệu trên Blockchain làm dữ liệu đầu vào, kết quả là một hợp đồng thông minh được thực hiện giữa DO và DU để DU có được MD.

3.4.2. Xác định các mối đe dọa

Luận án xem xét các mối đe dọa của từng phương thức như sau:

- Phương thức tạo dữ liệu: Phương thức này bao gồm DO và DP tham gia vào. Luận án giả định DO và DP là hoàn toàn tin cậy.
- Phương thức lưu trữ dữ liệu: Phương thức bao gồm các thành phần DO, IPFS và hệ thống Blockchain tham gia vào. Luận án giả định DO là hoàn toàn tin cậy, các Node của hệ thống IPFS và hệ thống Blockchain sẽ thực hiện theo đúng giao thức đã được định nghĩa nhưng chúng có thể truy cập nội dung của dữ liệu được lưu trữ trên chúng. Mục tiêu của những Node này là thỏa hiệp tính bí mật của dữ liệu lưu trữ.
- Phương thức chia sẻ dữ liệu: Phương thức bao gồm các thành phần DO, DU, IPFS và hệ thống Blockchain tham gia vào. Luận án giả định DO và DU là không tin cậy. Cụ thể, DO có thể cung cấp khóa giải mã không hợp lệ của EMD đến DU; và DU có thể thực hiện một yêu cầu xử lý tranh chấp trong khi DU đã nhận được một khóa giải mã hợp lệ của EMD. Giả định đối với các Node của hệ thống IPFS và hệ thống Blockchain là tương tự như trong phương thức lưu trữ dữ liệu.

3.4.3. Các chức năng bảo mật

Hệ thống cung cấp các chức năng bảo mật như sau:

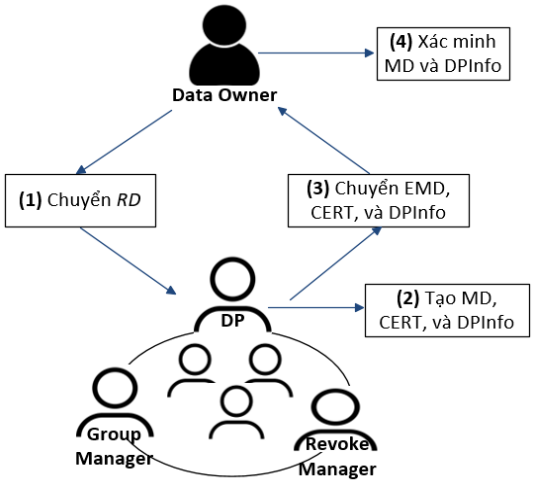
- *Tính bí mật*: Chỉ những người có thẩm quyền mới có thể đọc được nội dung của EMD trên IPFS và có được khóa giải mã được lưu trữ trên sổ cái Blockchain.
- *Tính toàn vẹn*: DO không thể giả mạo dữ liệu nhận được từ DP.
- *Tính riêng tư*: Từ các dữ liệu lưu trữ trên Blockchain, mọi người trên hệ thống không thể biết được DO đã sử dụng dịch vụ của DP nào.
- *Tính không chối bỏ*: Các đối tượng không thể chối bỏ các giao dịch mà họ đã thực hiện trong phương thức chia sẻ dữ liệu.
- *Tính ẩn danh*: Tất cả mọi người trong hệ thống không thể biết được danh tính thực sự của các bên tham gia trong phương thức lưu trữ và chia sẻ dữ liệu, và cũng không thể phân biệt được DP nào đã tạo ra MD.

3.4.4. Thiết lập hệ thống

- Thiết lập một nhóm các DP: Người quản lý nhóm chọn một tham số bảo mật λ và một phương thức chữ ký nhóm GS để khởi tạo các khóa cho n thành viên nhóm và một người quản lý thu hồi. Trong đó, người quản lý nhóm có một cặp khóa, khóa riêng và khóa công khai (PK_{GM}, SK_{GM}); người quản lý thu hồi sở hữu một khóa riêng SK_{RM} và một khóa công khai tương ứng PK_{RM}; $gsk[i]$ và $IdDP[i]$ lần lượt là khóa riêng và định danh của thành viên thứ i trong nhóm, với $1 \leq i \leq n$; và một khóa công khai của nhóm gpk.
- Hệ thống Blockchain: mỗi DO, DU và người người quản lý nhóm thiết lập một tài khoản trên Blockchain. Cụ thể, DO sở hữu một khóa công khai PK_{DO} và một khóa riêng tương ứng SK_{DO}; DU cũng có một khóa công khai PK_{DU} và một khóa riêng SK_{DU}; và người quản lý nhóm có một cặp khóa công khai và khóa riêng trên Blockchain $(PKBC_{GM}, SKBC_{GM})$. Trên hệ thống Blockchain, người dùng sử dụng khóa công khai của mình làm địa chỉ giao dịch, ví dụ PK_{DU} chính là địa chỉ Blockchain của DU. Mỗi giao dịch phải được ký bởi người thực hiện giao dịch. Hệ thống Blockchain cũng cung cấp một địa chỉ giao dịch công khai của hệ thống có tên là *Public BC*.

3.4.5. Phương thức tạo dữ liệu

Trong phương thức này, DO chuyển RD đến một DP cụ thể trong nhóm, ví dụ như DP thứ i. Sau khi nhận được RD, DP thực hiện thuật toán *Produce* để tạo MD, chứng chỉ CERT, và thông tin của DP DPInfo. Để đảm bảo tính bí mật của MD cho phương thức lưu trữ và chia sẻ dữ liệu, DP sẽ mã hóa MD để tạo thành EMD và sau đó cấp CERT trên EMD. Sau đó, DP gửi EMD, CERT, DPInfo đến DO. Sau khi nhận được dữ liệu từ DP, DO xác minh tính chính xác của MD và DPInfo. Việc truyền dữ liệu giữa DO và DP được thực hiện thông qua một kênh an toàn. Trong phương thức này, DO và DP được xem như là biết nhau. Do đó không cần thiết phải bảo mật danh tính của nhau. Điều này có nghĩa là DO biết định danh $IdDP[i]$ và khóa công khai của nhóm của DP. Các bước của phương thức tạo dữ liệu được thể hiện ở Hình 3.7.



Hình 3.7: Phương thức tạo dữ liệu

Chi tiết các bước như sau:

(1) DO gửi RD đến một DP trong nhóm thông qua một kênh an toàn.

(2) Sau khi nhận được RD, DP sử dụng thuật toán *Produce* để tạo EMD, CERT và DPInfo. Thuật toán *Produce* bao gồm chín bước như sau:

- *Bước 1*: DP sử dụng một hàm tạo dữ liệu $make\_proc$ cùng với một thủ tục $:\equiv$ để tạo MD dưới dạng dữ liệu số:

$$MD :\equiv make\_proc(RD)$$

- *Bước 2*: DP tạo định danh cho MD bằng cách sử dụng hàm băm mật mã được cung cấp bởi hệ thống, dữ liệu đầu ra được ký hiệu là IdMD:

$$IdMD \leftarrow H(MD)$$

- *Bước 3*: DP thực hiện hàm $Rand\_Key$ để tạo ra một khóa K:

$$K \leftarrow Rand\_Key(\cdot)$$

- *Bước 4*: DP mã hóa MD bằng thuật toán mã hóa được cung cấp bởi hệ thống và khóa K, dữ liệu đầu ra là EMD:

$$EMD \leftarrow E_K(MD)$$

- *Bước 5*: DP mã hóa định danh của $IdDP$[i] của DP và khóa K sử dụng PK_{DO} và PCS được cung cấp bởi hệ thống. Dữ liệu đầu ra được ký hiệu là DPInfo:

$$DPInfo \leftarrow PCS(IdDP[i]||K, PK_{DO})$$

- *Bước 6*: DP mã hóa DPInfo và IdMD sử dụng PK_{RM} và PCS. Dữ liệu đầu ra được ký hiệu là EId:

$$EId \leftarrow PCS(DPInfo||IdMD, PK_{RM})$$

- *Bước 7*: DP tạo một chữ ký số trên EMD sử dụng thuật toán Sign của phương thức chữ ký nhóm GS, khóa công khai của nhóm gpk và khóa riêng của thành viên nhóm $gsk[i]$. Dữ liệu đầu ra được ký hiệu là SD:

$$SD \leftarrow \text{GS. Sign}(gpk, gsk[i], EMD)$$

- *Bước 8:* Chứng chỉ CERT của MD bao gồm SD và EId:

$$CERT = (SD, EId)$$

- *Bước 9*: Thuật toán xuất ra EMD, CERT, và DPInfo.

Thuật toán *Produce* được trình bày tóm tắt trong Thuật toán 1.

Thuật toán 1: Produce	
	Input: RD, IdDP[i], gsk[i], gpk, PK_{DO}, PK_{RM} **Output: EMD, CERT, DPInfo**
1:	Tạo MD từ RD $MD: \equiv make\_proc(RD)$
2:	Tạo định danh cho MD $IdMD \leftarrow H(MD)$
3:	Tạo một khóa ngẫu nhiên *K:* $K \leftarrow Rand\_Key(\cdot)$

4:	Mã hóa MD sử dụng khóa *K* và một thuật toán mã hóa của hệ thống $EMD \leftarrow E_K(MD)$
5:	Mã hóa định danh của DP và *K* sử dụng khóa công khai của DO và PCS $DPInfo \leftarrow PCS(IdDP[i]\|\|K, PK_{DO})$
6:	Mã hóa $DPInfo$ và $IdMD$ sử dụng khóa công khai của người quản lý thu hồi và PCS $EId \leftarrow PCS(DPInfo\|\|IdMD, PK_{RM})$
7:	Tạo chữ ký số trên EMD sử dụng gpk, $gsk[i]$, và $GS.Sign$. $SD \leftarrow \text{GS. Sign}(gpk, gsk[i], EMD)$
8:	Chứng chỉ $CERT$ bao gồm (SD, EId) $CERT = (SD, EId)$
9:	Return $(EMD, CERT, DPInfo)$

(3) DP gửi EMD, CERT và DPInfo đến DO thông qua một kênh an toàn.

(4) Sau khi nhận được dữ liệu từ DP, DO xác minh tính chính xác của MD và DPInfo như sau:

- *Bước 1*: DO giải mã DPInfo sử dụng khóa riêng của DO và PCS

$$IdDP[i]||K \leftarrow PCS(DPInfo, SK_{DO})$$

- *Bước 2*: DO so sánh giá trị $IdDP[i]$ với thông tin mà DO đã biết từ trước. Nếu chúng giống nhau, DO thực hiện bước tiếp theo. Ngược lại, ngừng hoạt động xác minh.
- *Bước 3*: DO giải mã EMD sử dụng khóa *K* có được ở bước 1và thuật toán giải mã của hệ thống.

$$MD \leftarrow D_K(EMD)$$

- *Bước 4*: Tính lại định danh cho MD

$$IdMD \leftarrow H(MD)$$

- *Bước 5*: Kiểm tra tính chính xác của thông tin DP

$$True/False \leftarrow (PCS(DPInfo||IdMD, PK_{RM}) == CERT.EId)$$

Nếu kết quả trả về $True$, thông tin của DP là hoàn toàn chính xác và chuyển sang bước kế tiếp. Ngược lại, ngừng hoạt động kiểm tra.

❖ *Bước 6*: Kiểm tra tính hợp lệ của MD sử dụng thuật toán Verify của phương thức chữ ký nhóm GS:

$$True/False \leftarrow GS.Verify(gpk, CERT.SD, EMD)$$

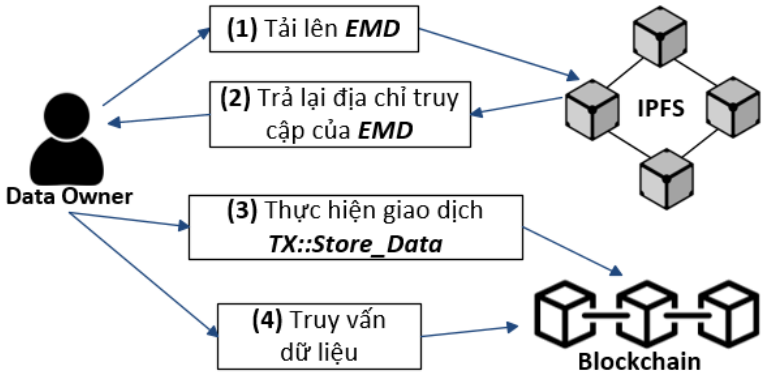
Nếu kết quả trả về $True$, DO đã nhận được dữ liệu chính xác và tin cậy. Ngược lại, loại bỏ giao dịch này.

#TX::Store_Data
From: *DO's BC address*
To: *Public BC Address*
Content:
- *EMD_Link*
- *CERT*
- *DPInfo*
- *Paymentadd*
- *Price*
- *SC*

Hình 3.8: Giao dịch trong phương thức lưu trữ dữ liệu

3.4.6. Phương thức lưu trữ dữ liệu

Sau khi nhận được dữ liệu từ DP, DO có thể sử dụng phương thức lưu trữ dữ liệu để lưu chúng trên một hệ thống lưu trữ an toàn. Trong phương thức này, DO lưu trữ EMD trên IPFS, sau đó lưu địa chỉ truy cập của EMD trên IPFS và các thông tin liên quan trong một giao dịch Blockchain. Các thông tin lưu trữ trong giao dịch này cũng sẽ phục vụ cho phương thức chia sẻ dữ liệu.



Hình 3.9: Phương thức lưu trữ dữ liệu

Hình 3.9 thể hiện phương thức lưu trữ dữ liệu, chi tiết các bước của phương thức này như sau:

(1) DO tải EMD lên IPFS.

(2) Sau khi tải lên thành công, IPFS trả về địa chỉ truy cập của EMD (được ký hiệu EMD_Link) đến DO.

(3) DO thực hiện giao dịch $TX::Store\_Data$ lên Blockchain, giao dịch được thể hiện ở Hình 3.8, nội dung của giao dịch bao gồm các trường thông tin chính như sau:

- $DO's\ BC\ address$: là địa chỉ Blockchain của DO.
- $Public\ BC\ address$: là địa chỉ Blockchain của hệ thống Blockchain.
- EMD_Link: là địa chỉ truy cập của EMD trên IPFS
- *DPInfo* và *CERT*: đây là các dữ liệu kết quả nhận được từ DP.
- *Paymentadd:* là địa chỉ thanh toán của DO
- $Price$: là số tiền mà người mua phải trả cho DO (được dùng trong phương thức chia sẻ dữ liệu).
- SC: là địa chỉ của hợp đồng thông minh được dùng cho quá trình chia sẻ dữ liệu.

Nếu chữ ký trên giao dịch này là hợp lệ, các Miner sẽ lưu nó vào sổ cái Blockchain của chúng.

(4) DO truy vấn giao dịch $TX::Store\_Data$ trên sổ cái của bất kỳ Miner nào mạng:

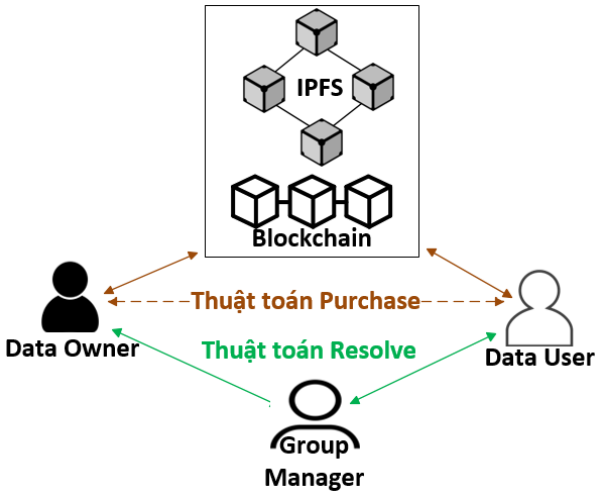
$$TX \leftarrow Ledger$$

Sau đó, DO kiểm tra kết quả truy vấn, nếu TX khác $null$, DO đã lưu trữ dữ liệu thành công trên sổ cái.

3.4.7. Phương thức chia sẻ dữ liệu

Trong phương thức này, quá trình chia sẻ dữ liệu giữa DO và DU được thực hiện thông qua thuật toán *Purchase*, và sử dụng thuật toán *Resolve* để giải quyết tranh chấp khi nhận được yêu cầu giải quyết tránh chấp. Trong phương thức này, EMD được xem như dữ liệu được chia sẻ và Blockchain giống như là một chợ mua bán dữ liệu. Mọi người trên hệ thống có thể tìm và mua các dữ liệu mà họ cần.

Trong quá trình chia sẻ dữ liệu, các bên tham gia phải thực hiện nộp tiền ký quỹ cho một hợp đồng thông minh được triển khai bởi người quản lý nhóm. Nếu bên nào bị phát hiện gian dối, tiền ký quỹ của họ sẽ bị mất. Hình 3.10 thể hiện phương thức chia sẻ dữ liệu.



Hình 3.10: Phương thức chia sẻ dữ liệu

Chi tiết các bước của hai thuật toán trong phương thức chia sẻ dữ liệu như sau:

(1) Thuật toán *Purchase*:

DU thực hiện thuật toán *Purchase* để tìm và mua dữ liệu chia sẻ mà họ cần, thuật toán này được trình bày tóm tắt trong Thuật toán 2. Cụ thể các bước như sau:

- *Bước 1*: DU tìm dữ liệu mà họ cần trên các giao dịch $TX::Store\_Data$ trong sổ cái Blockchain.
- *Bước 2*: Khi đã tìm được dữ liệu, DU truy cập EMD_Link trong giao dịch $TX::Store\_Data$ và tải xuống EMD từ IPFS.
- *Bước 3:* DU xác minh tính hợp lệ của EMD bằng cách sử dụng thuật toán Verify của phương thức chữ ký nhóm GS:

$$True/False \leftarrow GS.Verify(gpk, CERT.SD, EMD)$$

  Chú ý, DU chỉ có thể xác minh tính hợp lệ của dữ liệu chia sẻ nhưng không thể đọc được nội dung của dữ liệu.
- *Bước 4:* Nếu dữ liệu chia sẻ là hợp lệ, DU bắt đầu thực hiện hợp đồng thông minh $Contract::Share\_Data$ được chỉ định trong giao dịch

$TX::Store\_Data$. Cụ thể, DU thực hiện giao dịch $TX::Request\_Buy\_Data$, nội dung giao dịch này được thể hiện ở Hình 3.11(a). Thao tác này tương tự như việc gửi yêu cầu chia sẻ dữ liệu đến DO. Trong giao dịch này, DU cũng sẽ nộp tiền ký quỹ cho hợp đồng thông minh.

- *Bước 5:* Thông tin của hợp đồng sẽ được thông báo đến DO bởi một ứng dụng hệ thống. Nếu DO chấp nhận yêu cầu chia sẻ dữ liệu này, DO sẽ thực hiện giao dịch $TX::Reply\_Buy\_Data$ của hợp đồng $Contract::Share\_Data$, nội dung giao dịch này được thể hiện ở Hình 3.11(b). Trong đó, DO cũng phải thực hiện nộp tiền ký quỹ cho hợp đồng thông minh.
- *Bước 6:* Sau khi nhận được thông tin của hợp đồng thông qua một ứng dụng hệ thống, DU thực hiện giao dịch $TX::transfer\_Money$ đến DO, nội dung của giao dịch được thể hiện ở Hình 3.11(c). Trong giao dịch này, trường $Money$ là số tiền mà DU sẽ phải chuyển cho DO.
- *Bước 7:* DU gửi thông tin hóa đơn thông qua giao dịch $TX::Transfer\_Bill$ của hợp đồng $Contract::Share\_Data$, nội dung của giao dịch này được trình bày ở Hình 3.11(d).
- *Bước 8:* Nếu DO đã nhận được đúng số tiền theo thông tin của hóa đơn được chuyển từ DU, DO thực hiện giao dịch $TX::Transfer\_Key$ để gửi khóa bí mật K đến DU để giải mã dữ liệu chia sẻ, nội dung của giao dịch này được trình bày ở Hình 3.11(e). Trong đó, khóa bí mật K được mã hóa bằng khóa công khai của DU và hệ mật mã khóa công khai PCS của hệ thống, dữ liệu đầu ra được ký hiệu là k'.

$$k' \leftarrow PCS(K, PK_{DU})$$

- *Bước 9:* Sau khi nhận được thông tin của khóa, DU sử dụng khóa riêng của mình để giải mã k' và lấy được K, sau đó sử dụng K để giải mã dữ liệu chia sẻ EMD.

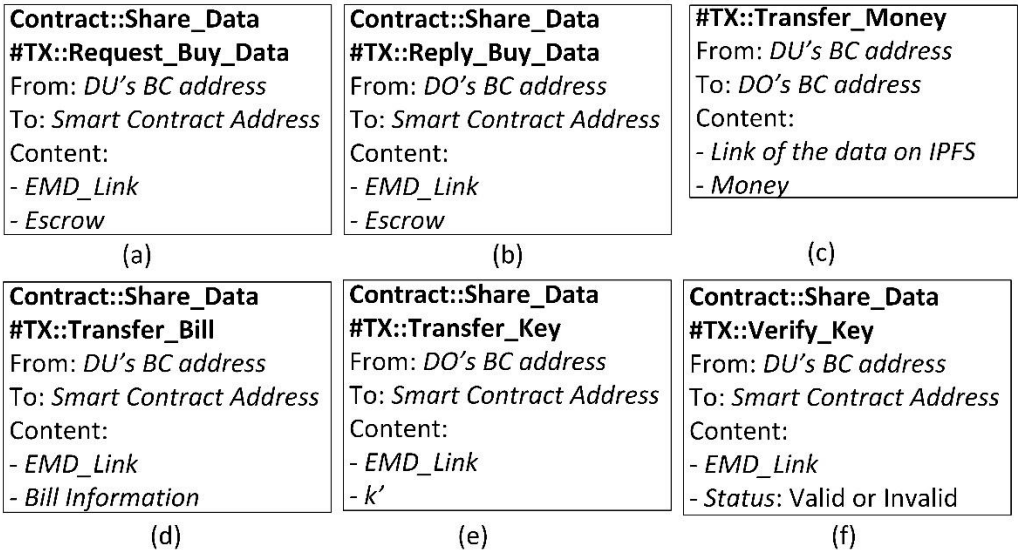
$$K \leftarrow PCS(k', SK_{DU})$$

$$MD \leftarrow D_K(EMD)$$

❖ *Bước 10:* Nếu khóa *K* là hợp lệ, DU thực hiện giao dịch $TX::Verify\_key$ của hợp đồng $Contract::Share\_Data$, nội dung của giao dịch này được trình bày ở Hình 3.11(f). Trong đó, trường $Status$ được thiết lập là $Valid$ để thể hiện khóa nhận được là hợp lệ. Khi đó quá trình chia sẻ dữ liệu đã được hoàn thành. Ngược lại, nếu khóa *K* không hợp lệ thì cả DO và DU sẽ chuyển sang phương thức giải quyết tranh chấp với thuật toán *Resolve*.

Thuật toán 2: Purchase	
	Input: ***TX'*** **Output:** ***MD***
DU:	
1:	Tìm dữ liệu chia sẻ trên Blockchain
2:	Tải xuống *EMD* trên IPFS
3:	Xác minh tính hợp lệ của EMD
	if $(GS.Verify(gpk, CERT.SD, EMD) == True)$ **then**
4:	Thực hiện giao dịch $TX::Request\_Buy\_Data$ của hợp đồng $Contract::Share\_Data$
5:	**end**
DO:	
6:	Thực hiện giao dịch $TX::Reply\_Buy\_Data$ của hợp đồng $Contract::Share\_Data$
DU:	
7:	Thực hiện giao dịch $TX::Transfer\_Money$ đến DO. Trong đó, trường $Money$ là chí phí mà DU phải trả cho DO
8:	Thực hiện giao dịch $TX::Transfer\_Bill$ của hợp đồng $Contract::Share\_Data$
DO:	
9:	Thực hiện giao dịch $TX::Transfer\_Key$ của hợp đồng $Contract::Share\_Data$
DU:	

10:	Giải mã k' để lấy khóa K $K \leftarrow PCS(k', SK_{DU})$
11:	Sử dụng khóa K và thuật toán giải mã để giải mã *EMD* $MD \leftarrow D_K(EMD)$
12:	**if** (*K* là hợp lệ) **then**
13:	Thực hiện giao dịch $TX::Verify\_Key$ của hợp đồng $Contract::Share\_Data$. Trong đó, trường $Status$ được thiết lập là $Valid$
14:	**else**
15:	Thực hiện thuật thuật toán Resolve
16:	**end**
17	**return** (MD)



Hình 3.11: Các giao dịch trong thuật toán Purchase

(2) Thuật toán *Resolve*:

Khi nhận được yêu cầu giải quyết tranh chấp, người quản lý nhóm thực hiện thuật toán *Resolve* để xác minh người nào không trung thực trong quá trình chia sẻ. Người quản lý nhóm là người đã triển khai hợp đồng thông minh và đóng vai trò như một trọng tài trong hợp đồng thông minh. Vì mọi giao dịch Blockchain đều được công khai nên người quản lý nhóm sẽ biết thông tin của dữ liệu chia sẻ (như

EMD_Link, *CERT*) và các giao dịch đã được thực hiện của hợp đồng. Chi tiết các bước của thuật toán *Resolve* như sau:

- *Bước 1*: Người quản lý nhóm thực hiện giao dịch $TX::Dispute\_Key\_Request$ đến DO để yêu cầu DO cung cấp khóa giải mã của dữ liệu chia sẻ, nội dung của giao dịch này được thể hiện ở Hình 3.12 (a).
- *Bước 2*: Sau khi nhận được giao dịch yêu cầu cung cấp khóa giải mã từ người quản lý nhóm, DO thực hiện giao dịch $TX::Dispute\_Key\_Reply$ đến người quản lý nhóm, nội dung của giao dịch này được thể hiện ở Hình 3.12(b). Trong đó, khóa K sẽ được mã hóa bởi khóa công khai của người quản lý nhóm và PCS:

$$EK' \leftarrow PCS(K, PKBC_{GM})$$

- *Bước 3*: Khi nhận được phản hồi từ DO, người quản lý nhóm giải mã EK' bằng cách sử dụng khóa riêng của mình và PCS, dữ liệu đầu ra là khóa K:

$$K \leftarrow PCS(EK', SKBC_{GM})$$

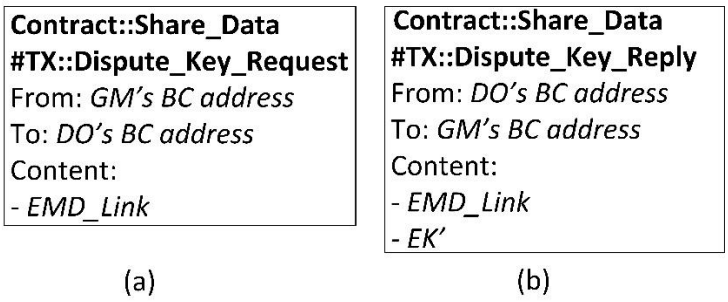
- *Bước 4*: Người quản lý nhóm sử dụng K để giải mã *EMD:*

$$MD \leftarrow D_K(EMD)$$

- *Bước 5*: Nếu khóa K không hợp lệ, người quản lý nhóm kết luận rằng DO là người không trung thực. Ngược lại, chuyển sang bước 6.
- *Bước 6*: Người quản lý nhóm kiểm tra xem khóa này có đúng là khóa mà DO đã gửi cho DU hay không bằng cách mã hóa khóa K sử dụng khóa công khai của DU và PCS, dữ liệu đầu ra được ký hiệu là $EK1'$:

$$EK1' \leftarrow PCS(K, PK_{DU})$$

- *Bước 7*: Người quản lý nhóm lấy k' từ giao dịch $TX::Transfer\_Key$ và so sánh k' với $EK1'$. Nếu chúng giống nhau, người quản lý nhóm kết luận DU là người không trung thực vì đã thực sự nhận được khóa hợp lệ nhưng vẫn yêu cầu giải quyết tranh chấp. Ngược lại, DO là người không trung thực vì đã gửi khóa không hợp lệ cho DU. Trong trường hợp này người quản lý nhóm cũng sẽ gửi khóa hợp lệ đến DU.



Hình 3.12: Các giao dịch trong thuật toán Resolve

Thuật toán *Resolve* được trình bày tóm tắt trong Thuật toán 3.

Thuật toán 3: Resolve	
	Input: ***TX'*** **Output:** ***DO, DU***
Người quản lý nhóm:	
1:	Thực hiện giao dịch $TX :: Dispute\_Key\_Request$ đến DO
DO:	
2:	Thực hiện giao dịch $TX:: Dispute\_Key\_Reply$ đến người quản lý nhóm
Người quản lý nhóm:	
3:	Truy cập EMD_Link và tải xuống *EMD* trên IPFS
4:	Lấy các giao dịch liên quan đến hợp đồng thông minh
5:	Giải mã EK' sử dụng $SKBC_{GM}$ và PCS để nhận được K $K \leftarrow PCS(EK', SKBC_{GM})$
6:	Giải mã *EMD* $MD \leftarrow D_K(EMD)$
7:	**if** (*K* không hợp lệ) **then**
8:	$SCA \leftarrow DO$
9:	**else**
10:	Mã hóa K sử dụng PK_{DU} và PCS: $EK1' \leftarrow PCS(K, PK_{DU})$

11:	Lấy k' trong giao dịch $TX::Transfer\_Key$ của $Contract::Share\_Data$
12:	**if** ($EK1' == k'$) **then**
13:	$SCA \leftarrow DU$
14:	**else**
15:	$SCA \leftarrow DO$
16:	Gửi khóa K đến DU
17:	**end**
18:	**end**
19:	**Return** (SCA)

Các luật được sử dụng trong phương thức chia sẻ dữ liệu như sau:

- Tiền ký quỹ phải gấp 2 đến 3 lần giá tiền ($Price$) của dữ liệu chia sẻ. Điều này sẽ khuyến khích các bên trung thực trong quá trình chia sẻ dữ liệu.
- Nếu DU đã thực hiện ký quỹ và đã thực hiện giao dịch $TX::Request\_Buy\_Data$, tuy nhiên DO không thực hiện giao dịch $TX::Reply\_Buy\_Data$ thì sau một khoảng thời gian nhất định, hợp đồng thông minh sẽ tự động gửi trả lại tiền ký quỹ cho DU.
- Nếu cả hai DO và DU đã thực hiện ký quỹ, tuy nhiên DU không thực hiện giao dịch $TX::Transfer\_Money$ đến DO thì sau một khoảng thời gian nhất định, hợp đồng thông minh sẽ chuyển lại tiền ký quỹ cho DU và DO.
- Nếu DU đã thực hiện giao dịch $TX::Transfer\_Bill$ nhưng DO không thực hiện giao dịch $TX::Transfer\_Key$ của hợp đồng $Contract::Share\_Data$ trong một khoảng thời gian quy định, tiền ký quỹ của DO sẽ mất, đồng thời tiền ký quỹ của DU cũng sẽ được chuyển lại cho DU.
- Nếu DU đã nhận được một khóa giải mã của *EMD* từ DO, nhưng DU không thực hiện giao dịch $TX::Verify\_Key$ trong một khoảng thời gian quy định, thì khóa này được xem là hợp lệ và hoàn tất hợp đồng.

❖ Sau khi người không trung thực được xác định bởi thuật toán *Resolve*, tiền ký quỹ của người không trung thực sẽ bị mất và tiền ký quỹ của bên trung thực sẽ được gửi trả lại.

3.5. PHÂN TÍCH VÀ ĐÁNH GIÁ

Trong phần này, luận án sẽ phân tích các ưu điểm và các tính năng bảo mật đạt được của phương thức lưu trữ dữ liệu và phương thức chia sẻ dữ liệu. Luận án cũng sẽ thực hiện đánh giá các tính năng liên quan đến hiệu năng của hệ thống.

3.5.1. Ưu điểm

❖ *Tính chủ động*

- Trong phương thức lưu trữ dữ liệu, DO chủ động trong việc lưu trữ EMD trên hệ thống IPFS. Cụ thể, DO có thể sử dụng một hoặc một vài thiết bị như: máy chủ, máy trạm, … để tham gia vào mạng IPFS, sau đó DO tải EMD của mình lên các thiết bị này và bật tính năng Pinning để lưu trữ chúng lâu dài. Bên cạnh đó, DO cũng có thể chủ động bỏ tính năng Pinning để xóa EMD đã được lưu trữ từ các thiết bị này.
- Trong phương thức chia sẻ dữ liệu, DU có thể chủ động xác minh tính tin cậy của những dữ liệu được chia sẻ trên hệ thống mà họ cần trước khi thực hiện hợp đồng $Contract::Share\_Data$ của thuật toán *Purchase*. Cụ thể, DU truy cập *EMD_Link* và tải xuống EMD, sau đó DU sử dụng thuật toán Verify của phương thức chữ ký nhóm GS được cung cấp bởi hệ thống, khóa công khai của nhóm gpk, và SD trong $CERT$ của giao dịch $TX::Store\_Data$ để xác minh tính tin cậy của EMD:

  $$True/False \leftarrow GS.Verify(gpk, CERT.SD, EMD)$$

  Bên cạnh đó, quá trình chia sẻ được thực hiện trực tiếp giữa DU và DO mà không phụ thuộc vào bất kỳ bên trung gian nào.

❖ *Tính minh bạch và công bằng trong chia sẻ dữ liệu*

- Tất cả các giao dịch trong phương thức chia sẻ dữ liệu đều được lưu lại trên số cái Blockchain. Điều này có nghĩa là mọi người đều có thể theo dõi bất kỳ giao dịch nào khi họ cần.

- Các bên tham gia vào quá trình chia sẻ dữ liệu phải chuyển tiền ký quỹ đến hợp đồng thông minh để khuyến khích sự trung thực. Trong trường hợp có tranh chấp, người quản lý nhóm sẽ giải quyết tranh chấp này thông qua thuật toán *Resolve* trong phương thức chia sẻ dữ liệu. Kết quả là người không trung thực sẽ phải mất tiền ký quỹ.

3.5.2. Tính năng bảo mật

❖ *Tính bí mật*

- Trong phương thức lưu trữ dữ liệu, MD được mã hóa để tạo thành EMD trước khi tải lên IPFS. Để đọc được nội dung của EMD, kẻ tấn công cần phải có được khóa bí mật để giải mã EMD. Vì khóa bí mật này được mã hóa bởi khóa công khai của DO trước khi lưu trữ trên Blockchain. Do đó, kẻ tấn công sẽ không thể có được khóa giải mã của EMD.
- Trong phương thức chia sẻ dữ liệu, khóa giải mã của EMD cũng sẽ được mã hóa bởi khóa công khai của DU trong hợp đồng thông minh. Do đó, chỉ DU mới có thể giải mã và có được khóa bí mật để giải mã cho EMD. Trong thuật toán *Resolve*, khóa giải mã của EMD cũng sẽ được mã hóa bằng khóa công khai của người quản lý nhóm trước khi gửi lên Blockchain. Có thể thấy rằng, tính bí mật của MD được đảm bảo khi chỉ những người có thẩm quyền mới có thể đọc được nội dung của MD.

❖ *Tính toàn vẹn*

Trong phương thức chia sẻ dữ liệu, chứng chỉ CERT được cấp bởi DP sẽ được sử dụng để xác minh tính hợp lệ của EMD. Do đó, DO có thể chỉnh sửa MD để tạo thành một phiên bản mới của MD nhưng sẽ không thể tạo một chứng chỉ hợp lệ cho phiên bản chỉnh sửa MD này, vì DO không phải là thành viên của nhóm nhà cung cấp dữ liệu.

❖ *Tính riêng tư*

Từ các dữ liệu lưu trữ trên Blockchain, mọi người có thể xác minh tính chính xác và tính tin cậy của MD nhưng không thể hiểu được nội dung của nó và

cũng không thể biết chính xác DP nào trong nhóm mà DO đã sử dụng dịch vụ. Tính chất này được đảm bảo bởi phương thức chữ ký nhóm.

- *Tính chống chối bỏ*

  Trong phương thức lưu trữ dữ liệu và phương thức chia sẻ dữ liệu, người thực hiện giao dịch sử dụng khóa riêng của mình để ký xác nhận trên các giao dịch. Các giao dịch với chữ ký không hợp lệ sẽ bị loại bỏ bởi các Miner của mạng Blockchain. Do đó, kẻ tấn công không thể mạo danh người khác để thực hiện các giao dịch. Bên cạnh đó, các giao dịch hợp lệ đều được lưu lại trong sổ cái và dữ liệu trên sổ cái là bất biến. Vì vậy mọi người không thể chối bỏ các giao dịch mà họ đã thực hiện.

- *Tính ẩn danh*

  Trong mạng Blockchain, mỗi người dùng được định danh bằng khóa công khai của mình mà không cần thêm bất kỳ thông tin nào khác và khóa riêng tương ứng sẽ được sử dụng để ký trên các giao dịch. Do đó, tất cả mọi người trên mạng Blockchain đều không thể biết được các thông tin cá nhân của người khác. Bên cạnh đó, phương thức chữ ký nhóm đảm bảo tính ẩn danh của DP. Cụ thể, tất cả mọi người trong hệ thống, các DP trong nhóm thậm chí cả người quản lý nhóm cũng không thể biết danh tính của thành viên nhóm đã tạo và phát hành chứng chỉ cho MD. Tính ẩn danh của thành viên nhóm chỉ được tiết lộ khi và chỉ khi người quản lý nhóm và người quản lý thu hồi cộng tác với nhau.

3.5.3. Tính năng hệ thống

Trong hệ thống đề xuất, hệ thống giao dịch Blockchain và hệ thống lưu trữ IPFS đạt được các tính chất như sau:

- *Tính sẵn sàng*

  Trong mô hình hệ thống, cả hệ thống lưu trữ IPFS và hệ thống Blockchain đều là mạng ngang hàng với rất nhiều Node trong hệ thống, kẻ tấn công có thể làm sập một vài Node nhưng sẽ rất khó để làm sập toàn bộ hệ thống. Trong hệ thống IPFS, tính sẵn sàng của dữ liệu lưu trữ cũng sẽ được đảm bảo. Cụ thể,

khi kẻ tấn công làm sập một Node đang ghim EMD, EMD này có thể được lưu vào bộ nhớ đệm tại một số Node khác trên mạng IPFS trong một khoảng thời gian nhất định. Hơn nữa mạng IPFS là một mạng mở, nên DO hoàn toàn có thể sử dụng một số thiết bị của mình để tham gia mạng này và có thể kích hoạt các dịch vụ Pinning và Clustering trên các Node này để nâng cao tính sẵn sàng của dữ liệu lưu trữ. Đối với hệ thống giao dịch Blockchain, dữ liệu trong sổ cái được đồng bộ giữa các Miner, do đó nếu một số Miner không hoạt động do các cuộc tấn công từ chối dịch vụ hoặc lỗi phần cứng, dữ liệu trên sổ cái Blockchain sẽ được duy trì bởi các Miner khác.

- *Tính toàn vẹn*

  Đối với hệ thống lưu trữ IPFS, dữ liệu được lưu trữ trên IPFS sẽ được định danh bằng giá trị băm của nội dung của nó. Giá trị băm này được sử dụng để xác minh tính toàn vẹn của dữ liệu được lưu trữ và cũng là địa chỉ truy cập của dữ liệu trên IPFS. Do đó, khi dữ liệu bị sửa đổi thì cũng sẽ tạo ra một địa chỉ truy cập mới. Đối với hệ thống giao dịch Blockchain, dữ liệu được lưu trữ trên sổ cái là bất biến và được đồng bộ giữa các Miner. Kẻ tấn công có thể sửa đổi dữ liệu trên sổ cái khi và chỉ khi chúng thỏa hiệp đến phần lớn các Miner hoặc tất cả Miner, tuy nhiên điều này rất khó thực hiện.

- *Khả năng mở rộng*

  Cả hệ thống lưu trữ IPFS và hệ thống Blockchain đều là mạng ngang hàng. Do đó, việc mở rộng chỉ đơn giản là thêm một số Node vào mạng.

3.6. KẾT LUẬN CHƯƠNG 3

Trong chương này, luận án đã trình bày tổng quan về hệ thống lưu trữ phi tập trung IPFS, phương thức chữ ký nhóm. Luận án trình bày mô hình hệ thống của phương thức lưu trữ và phương thức chia sẻ dữ liệu. Trong mô hình này, luận án sử dụng một mạng public IPFS để lưu trữ các bản mã hóa của dữ liệu có giá trị; sử dụng hệ thống Blockchain để lưu trữ địa chỉ truy cập, chứng chỉ của dữ liệu và một số thông tin quản lý. Luận án sử dụng phương thức chữ ký nhóm để thiết lập khóa cho

một nhóm các nhà cung cấp dữ liệu. Sử dụng phương thức chữ ký nhóm giúp đảm bảo tính ẩn danh cho các DP và đảm bảo tính riêng tư cho DO.

Luận án đã đề xuất phương thức tạo dữ liệu, phương thức lưu trữ dữ liệu và phương thức chia sẻ dữ liệu. Trong phương thức tạo dữ liệu, một DP sử dụng thuật toán *Produce* để tạo EMD, CERT và DPInfo từ RD của DO. Trong phương thức lưu trữ dữ liệu, DO lưu trữ EMD trên IPFS, sau đó thực hiện một giao dịch $TX::Store\_Data$ để lưu địa chỉ truy cập của EMD trên IPFS, CERT và các thông tin khác lên mạng Blockchain. Trong phương thức chia sẻ dữ liệu, DU có thể kiểm chứng tính tin cậy của dữ liệu được chia sẻ trước khi quyết định thực hiện hợp đồng $Contract::Share\_Data$ đến DO. Hợp đồng thông minh $Contract::Share\_Data$ được xây dựng bởi người quản lý nhóm. Phương thức chia sẻ dữ liệu bao gồm hai thuật toán: thuật toán *Purchase* được sử dụng cho quá trình chia sẻ dữ liệu; thuật toán *Resolve* được sử dụng để giải quyết tranh chấp. Luận án cũng đã xây dựng các chính sách cho phương thức chia sẻ dữ liệu.

Phương thức lưu trữ dữ liệu và chia sẻ dữ liệu được đề xuất là hai chức năng trong nền tảng bảo mật được xây dựng ở Chương 2. Hai phương thức này đạt được các lợi ích như: *tính chủ động, tính minh bạch và công bằng trong chia sẻ dữ liệu*. Kết quả đánh giá bảo mật cũng cho thấy rằng hai phương thức này cũng đảm bảo các tính chất bảo mật như: *tính bí mật, tính toàn vẹn, tính riêng tư, tính chống chối bỏ* và *tính ẩn danh*. Về mặt hệ thống, hệ thống đã đạt được các tính chất như: *tính sẵn sàng, tính toàn vẹn* và *khả năng mở rộng*.

Chương tiếp theo trình bày giải pháp kiểm soát truy cập theo thời gian được cấp phép bởi chủ sở hữu thiết bị. Giải pháp này cũng là một chức năng của nền tảng bảo mật được đề xuất ở Chương 2.

CHƯƠNG 4: GIẢI PHÁP KIỂM SOÁT TRUY CẬP DỰA TRÊN THỜI GIAN ĐƯỢC CẤP PHÉP CHO IoT

Chương này trình bày giải pháp kiểm soát truy cập dựa trên thời gian được cấp phép cho IoT. Giải pháp được áp dụng vào ngữ cảnh cụ thể là kiểm soát truy cập cho hệ thống Camera trong các khu vực công cộng trong hệ thống nhà thông minh/thành phố thông minh. Trong đó, luận án trình bày quy trình đăng ký thiết bị Camera từ người sở hữu và quy trình quản lý các truy cập vào các Camera trong hệ thống. Giải pháp này là một chức năng của nền tảng bảo mật được đề xuất ở Chương 2. Nội dung của chương này được tổng hợp từ công trình [CT2] trong danh mục các công trình nghiên cứu của tác giả.

4.1. GIỚI THIỆU

Kiểm soát truy cập là phương thức bảo mật để giám sát, cấp quyền hoặc từ chối quyền truy cập vào tài nguyên từ người sở hữu đến người yêu cầu truy cập tài nguyên. Chương này sẽ trình bày giải pháp kiểm soát truy cập cho các thiết bị IoT, giải pháp này là một chức năng trong nền tảng bảo mật được đề xuất ở Chương 2. Giải pháp kiểm soát truy cập được đề xuất dựa trên ngữ cảnh cụ thể là việc kiểm soát truy cập các thiết bị Camera trong các khu vực công cộng của hệ thống nhà thông minh/thành phố thông minh, các thiết bị IoT khác có thể được áp dụng tương tự.

Thiết bị Camera là thành phần phổ biến và không thể thiếu trong hệ thống nhà thông minh/thành phố thông minh. Nhu cầu truy xuất các thiết bị Camera trong các khu vực công cộng là rất lớn. Ví dụ như: phụ huynh đôi lúc cần giám sát việc học tập sinh hoạt của con mình trong trường học; cư dân có thể truy cập Camera của sân thể thao, hồ bơi, bãi đỗ xe tại khu chung cư mình sinh sống để xem có đông người không, có còn sân thể thao trống hay không, bãi đỗ xe có còn chỗ trống hay không.

Đơn vị triển khai các thiết bị Camera công cộng được gọi là chủ sở hữu thiết bị, một chủ sở hữu thiết bị có thể quản lý nhiều thiết bị Camera. Chủ sở hữu sẽ công bố thông tin về vị trí địa lý và định danh của từng thiết bị Camera. Người dùng có thể gửi yêu cầu truy cập đến chủ sở hữu thiết bị và sẽ phải trả chi phí truy cập. Chủ sở

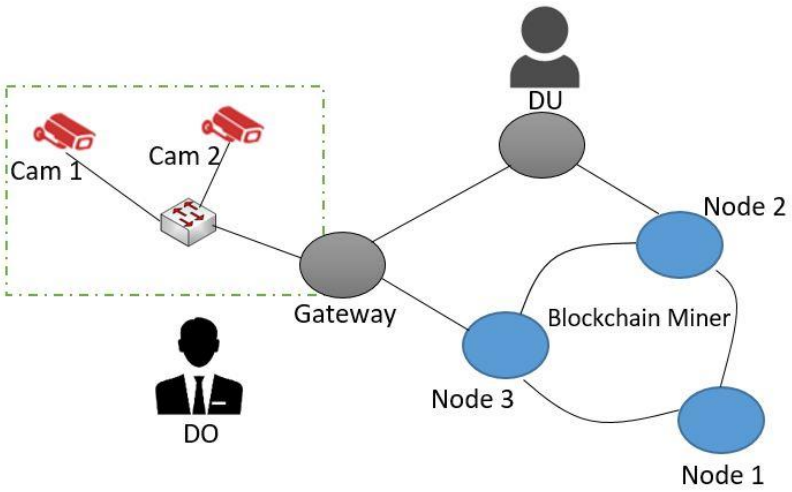
hữu thiết bị cấp quyền truy cập Camera theo thời gian được định trước. Hết khoảng thời gian này, kết nối sẽ tự động bị ngắt.

Giải pháp này sử dụng đặc tính bất biến của sổ cái Blockchain để làm một cơ sở dữ liệu bảo mật. Bên cạnh đó, công nghệ Blockchain có các ưu điểm như: *tính phi tập trung, tính ẩn danh, tính minh bạch, và tính kiểm toán* [1][70]. Chủ sở hữu thiết bị và người dùng có thể sử dụng Blockchain để thực hiện các giao dịch như: đăng ký thiết bị, yêu cầu và cấp quyền truy cập Camera.

Trong chương này, luận án chỉ trình bày về mặt kỹ thuật, các vấn đề liên quan đến việc tính toán chi phí phải trả để truy cập thiết bị Camera sẽ không được đề cập.

4.2. MÔ HÌNH HỆ THỐNG

Mô hình tổng quan của hệ thống kiểm soát truy cập, được thể hiện ở Hình 4.1, gồm các thành phần như sau: (i) nền tảng bảo mật được đề xuất ở Chương 2, hay còn được gọi là Blockchain; (ii) người dùng; (iii) các thiết bị Camera; (iv) thiết bị gateway, thiết bị này có thể là máy trạm hoặc máy chủ; và (v) chủ sở hữu thiết bị.



Hình 4.1: Mô hình hệ thống kiểm soát truy cập

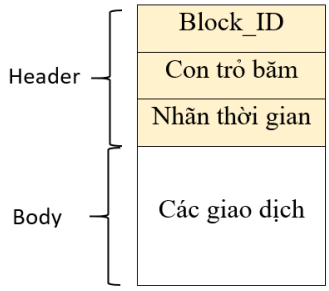
Chức năng cụ thể của từng thành phần như sau:

- *Chủ sở hữu thiết bị*: Chủ sở hữu thiết bị được ký hiệu là DO, sở hữu các thiết bị Camera để phục vụ nhu cầu truy cập từ người dùng. Mỗi DO trong hệ thống được thiết một cặp khóa (PK_{DO}, SK_{DO}) bởi một thuật toán mật mã khóa công

khai được cung cấp bởi hệ thống. Trong đó, PK_{DO} là khóa công khai của DO, SK_{DO} là khóa riêng tương ứng của DO.

- *Người dùng:* Là những người có nhu cầu truy xuất Camera, ví dụ: phụ huynh truy xuất Camera của trường mầm non; cư dân truy xuất Camera của khu vực công cộng. Người dùng được ký hiệu là DU và cũng có một khóa công khai PK_{DU} và khóa riêng tương ứng SK_{DU}.
- *Gateway***:** Là một thiết bị của DO, thiết bị này là một User Node trong mạng Blockchain. Thiết bị gateway đóng vai trò là một proxy giám sát các kết nối đến các thiết bị Camera. Tùy vào số lượng thiết bị Camera được sử dụng trong mạng và số lượng truy cập mà DO sẽ bố trí một số lượng Gateway phù hợp, sao cho tránh trường hợp quá tải trên các Gateway.
- *Camera:* Các thiết bị Camera sẽ kết nối với gateway và chúng không tham gia vào mạng Blockchain.
- *Blockchain*: Hệ thống Blockchain được dùng để phục vụ cho việc giao dịch. Trong hệ thống này, DO và DU sử dụng khóa công khai của mình để định danh và làm địa chỉ giao dịch trên mạng Blockchain. Khóa riêng sẽ được dùng để ký trên các giao dịch của họ. Hệ thống cũng cung cấp một địa chỉ Blockchain công khai của hệ thống có tên là *Public B*C. Một giao dịch được xem là hợp lệ khi chữ ký trên giao dịch đó là hợp lệ và nó sẽ được lưu trên sổ cái của các Miner trong mạng. Sổ cái Blockchain chứa các dữ liệu sau: (1) thông tin của các thiết bị Camera; (2) thông tin đăng ký truy cập thiết bị Camera của DU; và (3) thông tin cấp quyền truy cập từ DO. Cấu trúc một khối được thể hiện ở Hình 4.2, bao gồm phần Header chứa thông tin quản lý khối và phần Body chứa danh sách các giao dịch, mỗi khối được giới hạn một số lượng nhất định các giao dịch để đảm bảo tính hiệu quả cho mạng Blockchain.

Hệ thống cung cấp thuật toán mã hóa và giải mã tương ứng được ký hiệu lần lượt là $E_K(M)$ và $D_K(M)$, với M là một thông điệp và K là một khóa bí mật; và $PCS(M, K)$ là một hệ thống mật mã khóa công khai với thông điệp M và một khóa K.

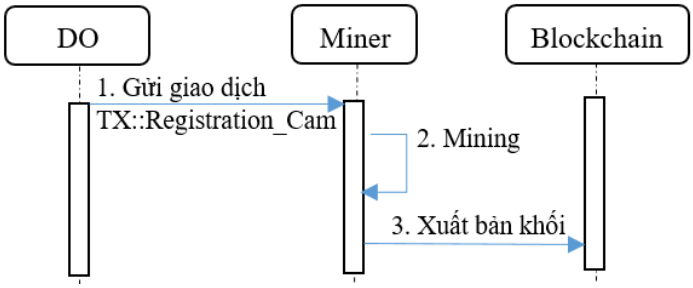


Hình 4.2: Cấu trúc của mỗi khối

4.3. CÁC QUY TRÌNH

4.3.1. Quy trình đăng ký thiết bị

Quy trình đăng ký thiết bị được sử dụng bởi DO để công bố thông tin về các thiết bị Camera trong hệ thống đến người dùng, quy trình này và được thể hiện ở Hình 4.3, chi tiết các bước như sau:



Hình 4.3: Quy trình đăng ký thiết bị

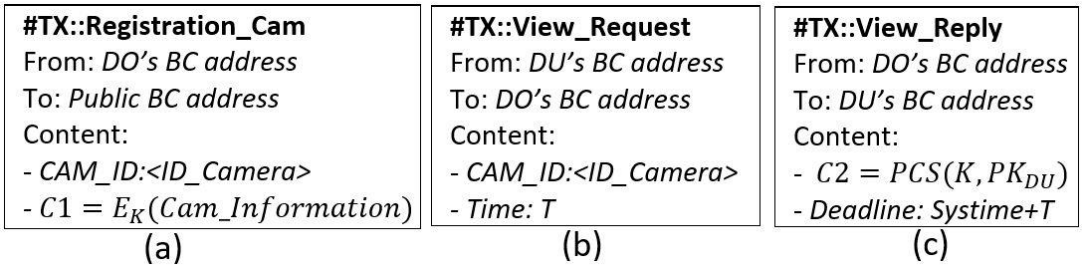
❖ *Bước 1:* DO thực hiện một giao dịch đăng ký thiết bị có tên là $TX::Registration\_cam$ đến hệ thống. Nội dung của giao dịch này được thể hiện ở Hình 4.4(a), bao gồm các trường thông tin sau:

- *DO's BC address*: là địa chỉ Blockchain của DO.
- *Public BC address*: là địa chỉ Blockchain của hệ thống Blockchain.
- *CAM_ID*: dùng để phân biệt các Camera trong hệ thống của DO, trường thông tin này nhằm phục vụ cho sự lựa chọn sử dụng Camera của DU.
- *C1*: chứa bản mã hóa của các thông tin cần thiết để kết nối đến Camera. Các thông tin kết nối được ký hiệu là *Cam_Information* được DO mã hóa bằng thuật toán mã hóa đối xứng được cung cấp bởi hệ thống cùng với khóa bí mật K.

$$C1 = E_K(Cam\_Information)$$

- *Bước 2:* Các Miner xác minh tính hợp lệ của giao dịch bằng cách kiểm tra chữ ký số của người thực hiện giao dịch.
- *Bước* 3: Nếu giao dịch này hợp lệ, nó sẽ được lưu vào sổ cái Blockchain của các Miner trong mạng.

Bên cạnh các thông tin được công bố trên Blockchain, DO cũng sẽ cung cấp sơ đồ vị trí các thiết bị Camera thông qua các kênh truyền thông, ví dụ như thông qua website hoặc một ứng dụng trên điện thoại di động, để mọi người dễ dàng biết và lựa chọn chính xác Camera nào mà họ đang quan tâm.



Hình 4.4: Các giao dịch đăng ký và truy cập Camera

4.3.2. Quy trình quản lý truy cập

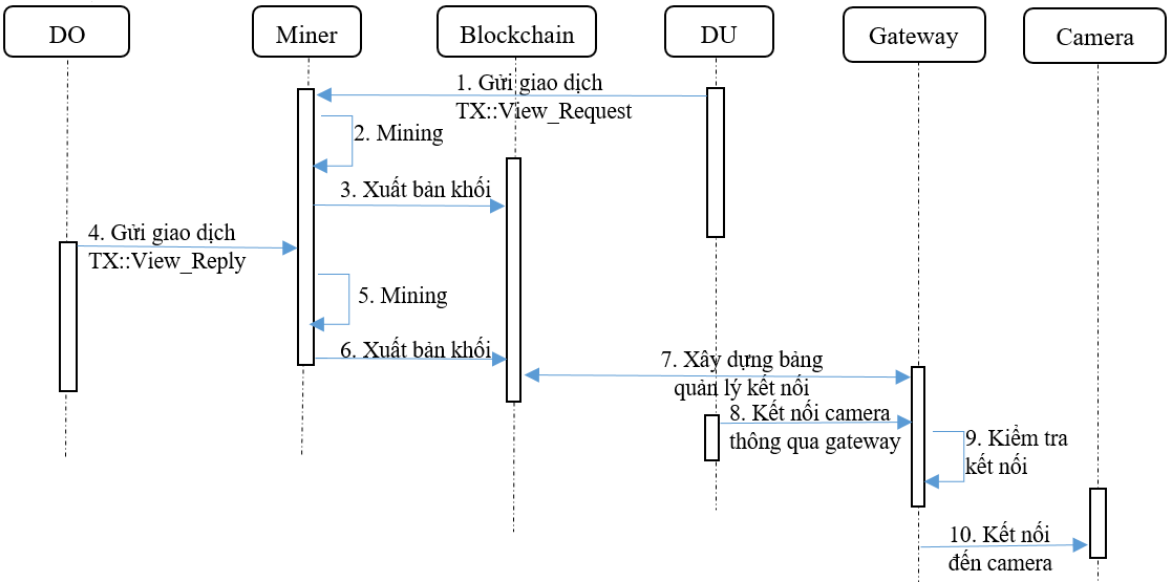
Khi DU có nhu cầu truy cập một Camera, DU sẽ gửi yêu cầu truy cập đến DO, sau đó DO sẽ cấp quyền truy cập cho DU. Các kết nối đến Camera sẽ được thiết bị Gateway kiểm tra quyền truy cập, giám sát và thu hồi quyền truy cập một cách tự động. Trình tự các bước của quy trình quản lý truy cập thiết bị được thể hiện ở Hình 4.5, chi tiết các bước như sau:

- *Bước 1:* Giao dịch yêu cầu xem Camera được thực hiện bởi DU. Khi DU muốn xem một Camera cụ thể của DO, DU thực hiện một giao dịch có tên $TX::View\_Request$ đến DO, nội dung của giao dịch được thể hiện ở Hình 4.4(b). Trong giao dịch này, DU phải chỉ ra định danh Camera (*CAM_ID)* nào muốn xem và thời gian xem là bao lâu. Đối với thời gian xem, hệ thống có thể thiết lập cố định hoặc sẽ đưa ra các mức thời gian tùy chọn cho DU, mỗi mức thời gian tương ứng với số tiền chi trả khác nhau. Tuy nhiên, trong phần trình bày giải pháp này

chỉ đưa ra ý tưởng, khi triển khai cho mục đích thương mại sẽ tính toán mức phí cụ thể. Nội dung của giao dịch bao gồm các trường thông tin chính như sau:

- *DU's BC address*: là địa chỉ Blockchain của DU.
- *DO's BC address:* là địa chỉ Blockchain của DO.
- *CAM_ID:* là Camera được yêu cầu.
- *Time:* là khoảng thời gian yêu cầu (có thể thiết lập cố định, hoặc cho nhiều tùy chọn).

❖ *Bước 2 và 3*: Giao dịch được xác minh và lưu vào sổ cái Blockchain của các Miner.



Hình 4.5: Quy trình quản lý truy cập

❖ *Bước 4*: Khi nhận được giao dịch yêu cầu truy cập Camera từ DU, nếu DO đồng ý với yêu cầu truy xuất của DU thì DO thực hiện một giao dịch phản hồi đến DU. Giao dịch phản hồi có tên $TX::View\_Reply$, được thể hiện ở Hình 4.4(c), nội dung của giao dịch gồm các trường sau:

- *DO's BC address:* là địa chỉ Blockchain của DO.
- *DU's BC address:* là địa chỉ Blockchain của DU.
- *C2:* khóa bí mật *K* được mã hóa bằng một thuật toán khóa công khai được cung cấp bởi hệ thống PCS cùng với khóa công khai của DU PK_{DU}:

$$C2 = PCS(K, PK_{DU})$$

- *Deadline:* là thời gian giới hạn được phép truy cập được tính bằng công thức:

$$Deadline = Systime + T$$

Trong đó, *Systime* là thời gian hiện tại của hệ thống, *T* là khoảng thời gian yêu cầu truy cập.

❖ *Bước 5 và 6*: Giao dịch được xác minh và lưu vào sổ cái Blockchain của các Miner. Khi $TX::View\_Reply$ được xác minh bởi Miner và công bố khối mới trên Blockchain thì thời gian xem Camera bắt đầu tính.

❖ *Bước 7:* Thiết bị Gateway của DO sẽ xây dựng bảng quản lý kết nối (Connection Management Table - CMT) dựa trên các giao dịch $TX::View\_Reply$. Thiết bị Gateway sẽ lọc thông tin theo các trường *DO's BC address* với các khối có *Timestamp* trong phần Header của khối nhỏ hơn *Timestamp* của khối mới nhất trong sổ cái *T* thời gian. Nội dung của bảng CMT được thể hiện ở Hình 4.6, gồm các trường thông tin sau: *CAM_ID*, địa chỉ Blockchain của DU (chính là khóa công khai của DU) và *Deadline*. Vì lý do bảo mật nên bảng CMT sẽ được cập nhật định kỳ trong khoảng thời gian bằng với thời gian trung bình một khối mới tạo ra.

Bảng quản lý kết nối		
CAM_ID	**DU**	**Hạn chót**
1	PK_{DU1}	9:00 10/06/2020
2	PK_{DU2}	10:00 10/06/2020
	...	...

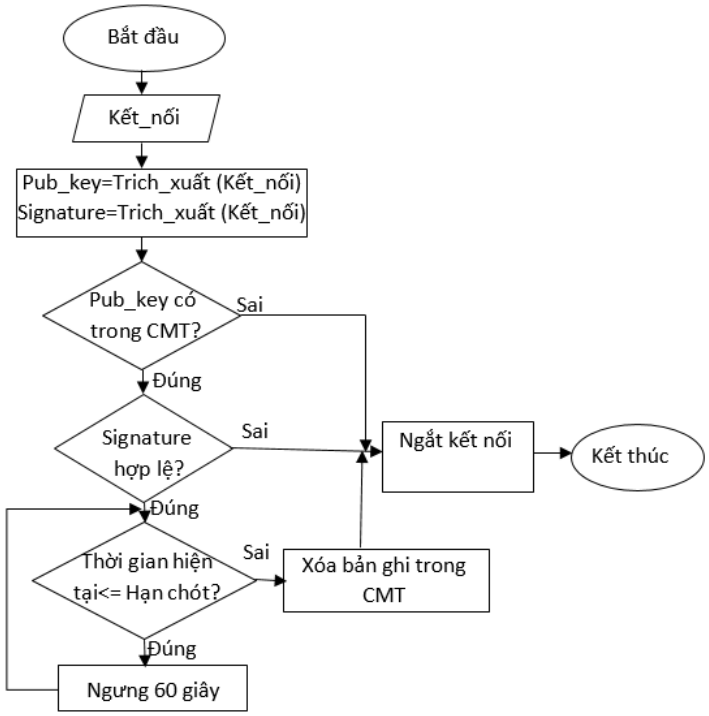
Hình 4.6: Bảng quản lý kết nối trên Gateway

❖ *Bước 8*: Khi nhận được giao dịch $TX::View\_Reply$ từ DO, DU sử dụng khóa riêng của mình để giải mã $C2$ và có được khóa K, sau đó dùng khóa K này để giải mã thông tin truy cập Camera.

$$K = PCS(C2, SK_{DU})$$
$$Cam\_Information = D_K(C1)$$

Sau khi có được thông tin truy cập Camera, DU sẽ kết nối đến Camera theo định dạng: *http://ip_gateway/Cam_ID/timestamp/public_key/signature_on _this_link* hoặc có thể truy cập *http://ip_gateway/Cam_ID/timestamp/public_key* trong khi *signature_on _this_link* được gửi kèm trong phần thân (*body)* của gói HTTP

Request. Trong đó, *ip_gateway* là thông tin trong *Cam_Information*, *public_key* là khóa công khai của DU; và *signature_on _this_link* là chữ ký số của DU trên địa chỉ truy cập.



Hình 4.7: Lưu đồ kiểm tra kết nối

❖ *Bước 9*: Khi có một kết nối đến Gateway, thiết bị này sẽ trích xuất khóa công khai *public_key* và chữ ký số *signature_on _this_link* có trong gói HTTP Request, sau đó thực hiện kiểm tra:

(1) Kiểm tra khóa công khai có nằm trong CMT không?

(2) Kiểm tra chữ ký số của DU có hợp lệ không?

(3) Kiểm tra thời gian truy xuất có còn hợp lệ hay không?

Nếu ba điều kiện trên đáp ứng thì kết nối sẽ được chuyển đến Camera tương ứng. Trong trường hợp này, luận án giả định thời gian trung bình tạo khối mới trên sổ cái Blockchain là 60 giây, vì vậy các kết nối sẽ được kiểm tra định kỳ mỗi 60 giây. Lưu đồ kiểm tra kết nối tại Gateway được thể hiện ở Hình 4.7.

4.4. ĐÁNH GIÁ BẢO MẬT

Bên cạnh các tính chất bảo mật của Blockchain được trình bày ở Chương 3 như tính sẵn sàng, tính toàn vẹn, và khả năng mở rộng. Giải pháp kiểm soát truy cập

cho IoT này cũng đạt được tính bí mật khi thông tin thiết bị Camera được lưu trữ trên sổ cái ở dạng mã hóa. Các kết nối từ người dùng đến thiết bị Camera cũng có thể được bảo vệ bằng cách sử dụng giao thức HTTPS.

4.5. KẾT LUẬN CHƯƠNG 4

Trong chương này, luận án trình bày giải pháp kiểm soát truy cho IoT dựa trên thời gian được cấp phép bởi chủ sở hữu thiết bị. Giải pháp được áp dụng vào ngữ cảnh cụ thể là kiểm soát truy cập cho các thiết bị Camera trong các khu vực công cộng của hệ thống nhà thông minh/thành phố thông minh. Trong đó, chủ sở hữu thiết bị Camera có thể công khai thông tin các thiết bị của họ để cho phép mọi người có thể gửi yêu cầu truy cập. Mỗi yêu cầu truy cập từ người dùng sẽ được chủ sở hữu thiết bị cấp quyền truy cập thông qua giao dịch $TX::View\_Reply$. Khi nhận được giao dịch phản hồi từ chủ sở hữu, người dùng có thể kết nối đến thiết bị Camera ngay lập tức. Để quản lý các kết nối đến các thiết bị Camera, chủ sở hữu sử dụng thiết bị Gateway hoạt động như là một proxy giữa các thiết bị Camera với người dùng, các kết nối đến thiết bị Camera sẽ phải thông qua Gateway. Thiết bị Gateway này là một User Node trong mạng Blockchain.

Giải pháp kiểm soát truy cập được đề xuất phù hợp với các hệ thống mạng Camera phục vụ cho cộng đồng. Với sự ràng buộc thời gian kết nối, mỗi kết nối đều phải trả chi phí cho chủ sở hữu dựa trên thời gian truy cập. Các kết nối khi hết hạn sẽ tự động bị loại bỏ khỏi hệ thống bởi thiết bị Gateway. Bên cạnh đó, hệ thống không phụ thuộc vào chủng loại Camera kết nối, chỉ cần các thiết bị thuộc loại Camera IP là có thể tham gia vào hệ thống.

Giải pháp kiểm soát truy cập được đề xuất giúp tối ưu công việc cho người sở hữu vì không cần phải thực hiện thêm bất kỳ giao dịch thu hồi quyền truy cập nào. Hơn nữa, các thiết bị Gateway sẽ tự động giải phóng các kết nối khi chúng hết thời gian quy định, điều này giúp hạn chế tối đa vấn đề tắc nghẽn trên các Gateway. Giải pháp này là một chức năng trong nền tảng bảo mật được đề xuất của luận án.

KẾT LUẬN

Luận án đề xuất một nền tảng bảo mật dựa trên Blockchain cho IoT. Mục tiêu chính của luận án là xây dựng phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain đảm bảo tối ưu về hiệu năng cho các Miner trong mạng, xây dựng chức năng lưu trữ dữ liệu, chia sẻ dữ liệu và kiểm soát truy cập theo thời gian được cấp phép cho nền tảng bảo mật được đề xuất.

Khi số lượng các thiết bị IoT tham gia vào mạng tăng trưởng nhanh chóng, việc sử dụng công nghệ Blockchain trong nền tảng bảo mật cho IoT có thể là giải pháp phù hợp với xu thế phát triển này. Bởi vì công nghệ Blockchain có các ưu điểm như: tính phi tập trung, tính ẩn danh, tính minh bạch, và tính kiểm toán. Vấn đề tối ưu hiệu năng cho các Miner trong việc xác minh giao dịch, đồng thuận dữ liệu trên sổ cái Blockchain và số lượng các chức năng bảo mật được cung cấp có ý nghĩa quan trọng trong một nền tảng bảo mật cho IoT.

Luận án đã đề xuất kiến trúc của nền tảng bảo mật dựa trên Blockchain cho IoT với phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain dựa trên hai trường hợp về các Miner trong một mạng Blockchain. Trường hợp 1, tất cả các Miner đều hoàn toàn tin cậy. Trường hợp 2, trong mạng có tồn tại một số Miner không tin cậy với số lượng ít hơn 1/3 trong tổng số các Miner trong mạng.

Luận án đã xây dựng chức năng lưu trữ dữ liệu và chức năng chia sẻ dữ liệu đảm bảo tính riêng tư cho nền tảng bảo mật được đề xuất. Trong đó, sử dụng hệ thống lưu trữ phi tập trung IPFS để lưu trữ các dữ liệu lớn; sử dụng Blockchain để lưu trữ địa chỉ truy cập của dữ liệu trên IPFS, các thông tin quản lý và để thực hiện các giao dịch. Bên cạnh đó, luận án sử dụng phương thức chữ ký nhóm để đảm bảo tính ẩn danh cho các thành viên trong nhóm các nhà cung cấp dữ liệu và đảm bảo tính riêng tư cho người sử dụng dịch vụ. Khi số lượng các thành viên trong nhóm càng nhiều thì tính ẩn danh và tính riêng tư càng cao.

Luận án cũng đã trình bày chức năng kiểm soát truy cập của nền tảng bảo mật được đề xuất. Trong đó, chủ sở hữu thiết bị có thể cấp quyền truy cập vào thiết bị IoT của họ cho người yêu cầu truy cập trong một khoảng thời gian xác định. Hết khoảng

thời gian này, kết nối sẽ tự động bị loại bỏ bởi thiết bị Gateway mà không cần người sở hữu thực hiện thêm bất kỳ giao dịch thu hồi quyền nào.

Để phát hiện sớm nguy cơ tấn công từ chối dịch vụ từ các Node độc hại trong mạng, luận án đã đề xuất triển khai giải pháp phát hiện nhanh các Hot-IP trên các Miner trong nền tảng, từ đó có thể kết hợp với tường lửa trên các Miner để khóa các kết nối từ những Node nghi ngờ.

Nền tảng bảo mật được đề xuất có ý nghĩa quan trọng trong việc đáp ứng các nhu cầu sử dụng hiện nay trong khi vẫn đảm bảo các yêu cầu bảo mật. So với các nền tảng bảo mật tương tự đã khảo sát, nền tảng bảo mật được luận án đề xuất đạt hiệu quả cao hơn trong việc xác minh các giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain trong cả hai trường hợp về các Miner trong mạng, đặc biệt đối với trường hợp 1. Đồng thời, nền tảng bảo mật được đề xuất cung cấp nhiều tính năng bảo mật hơn và có thể dễ dàng tích hợp thêm nhiều chức năng bảo mật mới. Đây là nền tảng có thể áp dụng vào thực tiễn với các mạng IoT của hệ thống nhà thông minh/thành phố thông minh.

1. CÁC KẾT QUẢ ĐẠT ĐƯỢC

Xuất phát từ các hạn chế trong việc xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain của các nền tảng bảo mật tương tự đã khảo sát, cũng như các điểm hạn chế của các giải pháp kiểm soát truy cập, lưu trữ và chia sẻ dữ liệu, luận án đã đề xuất một nền tảng bảo mật mới dựa trên Blockchain cho IoT. Các kết quả chính của luận án được tóm tắt như sau:

(1) Luận án đề xuất một nền tảng bảo mật mới dựa trên Blockchain cho IoT. Trong đó, đề xuất phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain. Phương thức xác minh giao dịch và đồng thuận dữ liệu trên sổ cái của nền tảng được đề xuất dựa trên hai trường hợp về các Miner trong một mạng Blockchain. Trường hợp 1: tất cả các Miner trong một mạng Blockchain đều hoàn toàn tin cậy. Trường hợp 2: trong một mạng Blockchain có tồn tại một số Miner không đáng tin cậy nhưng số lượng ít hơn 1/3 trong tổng số các Miner trong mạng. Kết quả đánh giá cho thấy rằng hiệu năng của các Miner

trong việc xác minh các giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain trong nền tảng bảo mật được đề xuất tối ưu hơn so với các nền tảng bảo mật tương tự đã khảo sát. Đối với trường hợp 1, càng nhiều Miner tham gia vào mạng, số lượng các giao dịch được xác minh càng lớn và thời gian Mining khối mới càng giảm. Tăng số lượng giao dịch được xác minh khi thời gian Mining một khối tăng lên trong khi số lượng Miner không thay đổi. Đối với trường hợp 2, các giao dịch chỉ phải xác minh một lần.

(2) Luận án đề xuất chức năng lưu trữ và chia sẻ dữ liệu đảm bảo tính riêng tư trong nền tảng bảo mật được đề xuất. Trong chức năng lưu trữ dữ liệu, dữ liệu số được lưu trữ an toàn trên IPFS và Blockchain. Trong chức năng chia sẻ dữ liệu, thông tin của dữ liệu chia sẻ được công khai trên Blockchain sao cho mọi người trên hệ thống đều có thể kiểm chứng tính chính xác và tin cậy của dữ liệu chia sẻ những vẫn đảm bảo tính bí mật của dữ liệu. Quá trình chia sẻ dữ liệu đảm bảo tính chính xác, tính minh bạch và công bằng. Hai chức năng này đạt được các tính chất bảo mật như: tính bí mật, tính toàn vẹn, tính riêng tư, tính chống chối bỏ và tính ẩn danh.

(3) Luận án đề xuất chức năng kiểm soát truy cập trong nền tảng bảo mật được đề xuất. Trong đó, chủ sở hữu thiết bị có thể cấp phép một khoảng thời gian truy cập nhất định trên một thiết bị IoT của họ cho những người có nhu cầu truy cập. Việc cấp phép truy cập sẽ được thực hiện thông qua một giao dịch Blockchain. Khi hết thời gian được phép truy cập, kết nối sẽ tự động loại bỏ mà không cần người sở hữu thực hiện thêm bất kỳ giao dịch thu hồi quyền nào.

Các kết quả cho thấy rằng nền tảng bảo mật được đề xuất cải thiện đáng kể hiệu năng của các Miner trong việc xác minh các giao dịch và đồng thuận dữ liệu trên sổ cái Blockchain; chức năng lưu trữ và chia sẻ dữ liệu đảm bảo được các tính chất bảo mật: tính bí mật, tính toàn vẹn, tính riêng tư, tính chống chối bỏ, tính ẩn danh; giải pháp kiểm soát truy cập đạt được tính linh hoạt trong việc cấp phép quyền truy cập tài nguyên theo thời gian thực. Các kết quả chính của luận án được công bố ở các công trình [CT1]-[CT8] trong danh mục các công trình nghiên cứu của tác giả.

2. HƯỚNG PHÁT TRIỂN

Luận án đã trình bày nền tảng bảo mật cùng các chức năng tích hợp trong nền tảng. Để có thể áp dụng hiệu quả nền tảng này vào thực tiễn, cần phải nghiên cứu sâu hơn các vấn đề như sau:

(1) Nghiên cứu cách tối ưu trong việc tổ chức *WL* và *VL* trong kiến trúc của nền tảng bảo mật được đề xuất cho từng ứng dụng cụ thể.

(2) Nghiên cứu chi tiết cách thức xây dựng và triển khai các hợp đồng thông minh trong chức năng chia sẻ dữ liệu trong nền tảng bảo mật được đề xuất.

(3) Nghiên cứu tối ưu phương thức chữ ký nhóm để nâng cao hiệu quả tính toán trong chức năng chia sẻ dữ liệu trong nền tảng bảo mật được đề xuất.

(4) Nghiên cứu các hạn chế của mạng IPFS, nghiên cứu cách xây dựng và triển khai các thuật toán đề xuất và xây dựng quy trình cài đặt và thực nghiệm nền tảng. Từ đó, thực hiện đánh giá có tính định lượng hiệu năng bảo mật của các giải pháp đề xuất ở Chương 3, 4.

CÁC CÔNG TRÌNH NGHIÊN CỨU CỦA TÁC GIẢ

TẠP CHÍ KHOA HỌC

[CT1] **Huynh Thanh Tam**, Dang Hai Van, and Nguyen Dinh Thuc (2020). A Solution for Privacy-Preserving Data Sharing on Peer-To-Peer Networks. *Tạp chí Khoa học Trường Đại học Sư phạm Thành phố Hồ Chí Minh*, tập 17, số 9, trang 1713-1724.

[CT2] **Huynh Thanh Tam**, Nguyen Dinh Thuc, Tan Hanh (2020). A Blockchain-Based Access Control Solution for IoT. *Tạp chí Khoa học Công nghệ Thông tin và Truyền thông*, số 03(CS.01), trang 15-23.

[CT3] **Huynh Thanh Tam**, Nguyen Dinh Thuc, Dang Hai Van, Huynh Nguyen Chinh. A Novel Security Framework Based On Blockchain for IoT Networks. *Tạp chí Phát triển Khoa học và Công nghệ*. (đã chấp nhận đăng).

[CT4] **Tam T. Huynh**, Thuc D. Nguyen, Thang Hoang, Lam Tran, Deokjai Choi (2021). A Reliability Guaranteed Solution for Data Storing and Sharing. *IEEE Access*, vol. 9, pp. 108318-108328. (ISI, IF 3.367).

HỘI NGHỊ KHOA HỌC QUỐC TẾ

[CT5] **Huynh, Tam T.**, Thuc D. Nguyen, and Hanh Tan (2019). A Survey on Security and Privacy Issues of Blockchain Technology. In *2019 International Conference on System Science and Engineering (ICSSE)*. IEEE, pp. 362-367.

[CT6] **Huynh, Tam T.**, Thuc D. Nguyen, and Hanh Tan (2019). A decentralized solution for web hosting. In *2019 6th NAFOSTED Conference on Information and Computer Science (NICS)*. IEEE, pp. 82-87.

[CT7] **Huynh, Tam T.**, Chinh N. Huynh, and Thuc D. Nguyen (2020). A Novel Security Solution for Decentralized Web Systems with Real Time Hot-IPs Detection. *In International Conference on Green Technology and Sustainable Development*. Springer, Cham, pp. 39-48.

[CT8] **Huynh, Tam T.**, Thuc D. Nguyen, Nguyen, Nhung T. H., and Hanh Tan. (2020). Privacy-Preserving for Web Hosting. *In International Conference on Industrial Networks and Intelligent Systems*. Springer, Cham, pp. 314-323.

TÀI LIỆU THAM KHẢO

[1] Antonopoulos, A. M. Mastering Bitcoin: unlocking digital cryptocurrencies. In *2014, O'Reilly Me-dia, Inc*.

[2] Bae, J., & Lim, H. (2018, June). Random mining group selection to prevent 51% attacks on bitcoin. In 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). IEEE, pp. 81-82.

[3] Banerjee, A., Sufyanf, F., Nayel, M. S., & Sagar, S. (2018). Centralized framework for controlling heterogeneous appliances in a smart home environment. In 2018 International Conference on Information and Computer Technologies (ICICT). IEEE, pp. 78-82.

[4] Bastiaan, M. (2015). Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin. [Online] https://fmt.ewi.utwente.nl/media/175.pdf.

[5] Baumgart, I., & Mies, S. (2007). S/kademlia: A practicable approach towards secure key-based routing. In 2007 International Conference on Parallel and Distributed Systems. IEEE, pp. 1-8.

[6] Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561.

[7] Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. ACM SIGMETRICS Performance Evaluation Review, 42(3), pp. 34-37.

[8] Bouij-Pasquier, I., Abou El Kalam, A., Ouahman, A. A., & De Montfort, M. (2015). A security framework for internet of things. In International Conference on Cryptology and Network Security. Springer, Cham, pp. 19-31.

[9] Buterin, V. (2015). On public and private Blockchains (2015). [online]: https://blog.ethereum.org/2015/08/07/on-public-and-private-Blockchains (ngày truy cập 10/2020).

[10] Camenisch, J., & Michels, M. (1998). A group signature scheme based on an RSA-variant. BRICS Report Series, 5(27).

[11] Castro, M., & Liskov, B. (1999). Practical byzantine fault tolerance. In Proceedings of the 13rd Symposium on Operating Systems Design and Implementation, vol. 99, 1999, pp. 173-186.

[12] Chaum, D., & Van Heyst, E. (1991). Group signatures. In Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, pp. 257-265.

[13] Chinh, H. N., Thuc, N. D., & Hanh, T. (2014). Early detection and limitation Hot-IPs using Non-Adaptive Group Testing and dynamic firewall rules. In 2014 International Conference on Computing, Management and Telecommunications (ComManTel). IEEE, pp. 286-290.

[14] Dang, T. L. N., & Nguyen, M. S. (2018). An approach to data privacy in smart home using blockchain technology. In 2018 International Conference on Advanced Computing and Applications (ACOMP), IEEE, pp. 58-64.

[15] Dennis, R., Owenson, G., & Aziz, B. (2016). A temporal Blockchain: a formal analysis. In 2016 International Conference on Collaboration Technologies and Systems (CTS). IEEE, pp. 430-437.

[16] Ding, S., Cao, J., Li, C., Fan, K., & Li, H. (2019). A novel attribute-based access control scheme using Blockchain for IoT. IEEE Access, 7, pp. 38431-38441.

[17] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). 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, pp. 618-623.

[18] Duy, P. T., Do Hoang, H., Nguyen, A. G. T., & Pham, V. H. (2022). B-DAC: A decentralized access control framework on Northbound interface for securing SDN using blockchain. Journal of Information Security and Applications, 64, 103080.

[19] Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin Mining is vulnerable. In International conference on financial cryptography and data security, Springer, Berlin, Heidelberg, pp. 436-454.

[20] Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via Blockchain. Journal of medical systems, 42(8), 136.

[21] Filecoin: A Decentralized Storage Network. [online]: https://filecoin.io/filecoin.pdf (ngày truy cập 10/2020).

[22] Fischer, M. J., Lynch, N. A., & Merritt, M. (1986). Easy impossibility proofs for distributed consensus problems. Distributed Computing, 1(1), pp. 26-39.

[23] Han, D., Kim, H., & Jang, J. (2017). Blockchain based smart door lock system. In 2017 International conference on information and communication technology convergence (ICTC). IEEE, pp. 1165-1167.

[24] Heilman, E. (2014). One weird trick to stop selfish Miners: Fresh bitcoins, a solution for the honest Miner. In International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, pp. 161-162.

[25] Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on bitcoin's peer-to-peer network. In 24th {USENIX} Security Symposium ({USENIX} Security 15, pp. 129-144.

[26] Hoang, V. H., Lehtihet, E., & Ghamri-Doudane, Y. (2020, June). Privacy-Preserving Blockchain-Based Data Sharing Platform for Decentralized Storage Systems. In 2020 IFIP Networking Conference (Networking). IEEE, pp. 280-288.

[27] IPFS cluster, [online]: https://cluster.ipfs.io (ngày truy cập 07/2020).

[28] IPFS Pinning service, [online]: https://docs.ipfs.io/concepts/persistence/#pinning-services (ngày truy cập 07/2020).

[29] Karame, G. O., Androulaki, E., & Capkun, S. (2012). Double-spending fast payments in bitcoin. In Proceedings of the 2012 ACM conference on Computer and communications security, pp. 906-917.

[30] Khan, M. I., & Lawal, I. A. (2020). Sec-IoT: A framework for secured decentralised IoT using Blockchain-based technology. In International Congress on Information and Communication Technology (pp. 269-277). Springer, Singapore.

[31] Kwon, J. (2014). Tendermint: Consensus without Mining.

[32] Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. ACM Transactions on Programming Languages and Systems, 4(3), pp. 382-401.

[33] Larimer, D. (2014). Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. ACM SIGMETRICS Performance Evaluation Review, 42 (3), pp. 34-37.

[34] Larimer, D. (2014). Delegated proof-of-stake (dpos). Bitshare whitepaper.

[35] Li, J., Li, N., Peng, J., Cui, H., & Wu, Z. (2019). Energy consumption of cryptocurrency Mining: A study of electricity consumption in Mining cryptocurrencies. Energy, 168 (pp. 160-168).

[36] Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating Blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC). IEEE, pp. 1-5.

[37] Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain based data integrity service framework for IoT data. In 2017 IEEE International Conference on Web Services (ICWS). IEEE, pp. 468-475.

[38] Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizani, M. (2018, December). BPDS: A Blockchain based privacy-preserving data sharing for electronic medical records. In 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, pp. 1-6.

[39] Liu, X., Zhao, M., Li, S., Zhang, F., & Trappe, W. (2017). A security framework for the internet of things in the future internet architecture. Future Internet, 9(3), 27.

[40] Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). PrivySharing: A Blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security, 88, 101653.

[41] Maymounkov, P., & Mazieres, D. (2002, March). Kademlia: A peer-to-peer information system based on the xor metric. In International Workshop on Peer-to-Peer Systems. Springer, Berlin, Heidelberg, pp. 53-65.

[42] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Manubot.

[43] Naz, M., Al-zahrani, F. A., Khalid, R., Javaid, N., Qamar, A. M., Afzal, M. K., & Shafiq, M. (2019). A secure data sharing platform using Blockchain and interplanetary file system. Sustainability, 11(24), 7054.

[44] Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), pp. 1184-1195.

[45] Nuss, M., Puchta, A., & Kunz, M. (2018, September). Towards Blockchain-based identity and access management for internet of things in enterprises. In International Conference on Trust and Privacy in Digital Business. Springer, Cham, pp. 167-181.

[46] Ouaddah, A., Abou Elkalam, A., & Ouahman, A. A. (2017). Towards a novel privacy-preserving access control model based on Blockchain technology in IoT. In Europe and MENA cooperation advances in information and communication technologies. Springer, Cham, pp. 523-533.

[47] Ourad, A. Z., Belgacem, B., & Salah, K. (2018, June). Using Blockchain for IOT access control and authentication management. In International Conference on Internet of Things. Springer, Cham, pp. 150-164.

[48] Outchakoucht, A., Hamza, E. S., & Leroy, J. P. (2017). Dynamic access control policy based on Blockchain and machine learning for the internet of things. Int. J. Adv. Comput. Sci. Appl, 8(7), pp. 417-424.

[49] Panda, S. S., Satapathy, U., Mohanta, B. K., Jena, D., & Gountia, D. (2019). Blockchain Based Decentralized Authentication Framework for Resource Constrained IOT devices. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, pp. 1-6.

[50] Pease, M. Shostak, R. & Lamport, L. (1980). Reaching agreement in the presence of faults. Journal of the ACM (JACM), 27(2), pp. 228-234.

[51] Pham, H. A., Le, T. K., & Le, T. V. (2019). Enhanced security of IoT data sharing management by smart contracts and blockchain. In 2019 19th International Symposium on Communications and Information Technologies (ISCIT), IEEE, pp. 398-403.

[52] Pinno, O. J. A., Gregio, A. R. A., & De Bona, L. C. (2017). Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, pp. 1-6.

[53] Puthal, D., Mohanty, S. P., Nanda, P., Kougianos, E., & Das, G. (2019). Proof-of-authentication for scalable Blockchain in resource-constrained distributed systems. In 2019 IEEE International Conference on Consumer Electronics (ICCE). IEEE, pp. 1-5.

[54] Rydning, D. R. J. G. J. (2018). The digitization of the world from edge to core. Framingham: International Data Corporation.

[55] Sheron, P. F., Sridhar, K. P., Baskar, S., & Shakeel, P. M. (2019). A decentralized scalable security framework for end-to-end authentication of future IoT communication. Transactions on Emerging Telecommunications Technologies, 31(12), e3815.

[56] Shirer, M., & MacGillivray, C. (2019). The Growth in Connected IoT Devices Is Expected to Generate 79.4 Zb of Data in 2025, according to a new IDC forecast.

[57] Singh, P. K., Singh, R., Nandi, S. K., & Nandi, S. (2020). Designing a Blockchain Based Framework for IoT Data Trade. In International Conference on Innovations for Community Services. Springer, Cham, pp. 295-308.

[58] Son, N. M., Nguyen, T. L., Huong, P. T., & Hien, L. T. (2021). Novel System Using Blockchain for Origin Traceability of Agricultural Products. Sensors and Materials, 33(2), 601-613.

[59] Sukhwani, H., Martínez, J. M., Chang, X., Trivedi, K. S., & Rindos, A. (2017). Performance modeling of PBFT consensus process for permissioned Blockchain network (hyperledger fabric). In 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS). IEEE, pp. 253-255.

[60] Vasek, M., Thornton, M., & Moore, T. (2014, March). Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In International conference on financial cryptography and data security (pp. 57-71). Springer, Berlin, Heidelberg.

[61] Wang, S., Zhang, Y., & Zhang, Y. (2018). A Blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access, 6, pp. 38437-38450.

[62] Wu, X., Han, Y., Zhang, M., & Zhu, S. (2019, October). Secure Personal Health Records Sharing Based on Blockchain and IPFS. In Chinese Conference on Trusted Computing and Information Security. Springer, Singapore, pp. 340-354.

[63] Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information, 8(2), 44.

[64] Xu, R., Chen, Y., Blasch, E., & Chen, G. (2018). Blendcac: A Blockchain-enabled decentralized capability-based access control for iots. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, pp. 1027-1034.

[65] Yi, H., & Wei, F. (2019). Research on a suitable Blockchain for IoT platform. In Recent Developments in Intelligent Computing, Communication and Devices. Springer, Singapore, pp. 1063-1072.

[66] Yu, X., Shiwen, M. T., Li, Y., & Huijie, R. D. (2017). Fair deposits against double-spending for bitcoin transactions. In 2017 IEEE Conference on Dependable and Secure Computing, IEEE, pp. 44-51.

[67] Zhang, C., Sun, J., Zhu, X., & Fang, Y. (2010). Privacy and security for online social networks: challenges and opportunities. IEEE network, 24(4), pp. 13-18.

[68] Zhang, R., & Preneel, B. (2017). Publish or perish: A backward-compatible defense against selfish Mining in bitcoin. In Cryptographers' Track at the RSA Conference. Springer, Cham, pp. 277-292.

[69] Zheng, X., Mukkamala, R. R., Vatrapu, R., & Ordieres-Mere, J. (2018). Blockchain-based personal health data sharing system using cloud storage. In 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1-6.

[70] Zheng, Z., Xie, S., Dai, H. N., Wang, H. (2018). Blockchain challenges and opportunities: A survey. In International Journal of Web and Grid Services, 14(4), pp. 352-375.

[71] https://www.designnews.com/electronics-test/centralized-or-decentralized-autonomous-vehicles-are-forcing-key-architectural

[72] https://en.bitcoinwiki.org/wiki/Merkle_tree

[73] https://ipfs.io/ipfs/QmRU1jJ1kNd9fTzjFwM4X9YtA2wfXN1W2eFK7mgTMJ8xgK