

**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT VĨNH LONG**  
**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO MÔN HỌC ĐỒ ÁN CNTT 2**

**TÊN ĐỀ TÀI:**

**ĐẢM BẢO AN TOÀN VÀ QUYỀN RIÊNG TƯ TRONG BLOCKCHAIN:**

- **NGHIÊN CỨU CÁC GIẢI PHÁP ĐỂ ĐẢM BẢO AN TOÀN VÀ QUYỀN RIÊNG TƯ TRONG CÁC GIAO DỊCH BLOCKCHAIN**
- **SO SÁNH VÀ PHÂN TÍCH CÁC MÔ HÌNH QUYỀN RIÊNG TƯ KHÁC NHAU TRÊN BLOCKCHAIN**

Sinh viên thực hiện: 20004223 – Văn Thị Mỹ Trang

Lớp: ĐH CNTT 2020 A2

Khóa: 45

Người hướng dẫn: Th.S Nguyễn Thị Hồng Yến

*Vĩnh Long, năm 2023*



## **LỜI CẢM ƠN**

Trước hết, em xin chân thành cảm ơn Trường Đại học Sư phạm kỹ thuật Vĩnh Long. Các Thầy, Cô trong Khoa Công nghệ Thông tin đã tạo điều kiện thuận lợi cho em trong suốt quá trình học tập tại trường.

Em xin bày tỏ lòng biết ơn sâu sắc của mình đối với cô Nguyễn Thị Hồng Yến, người đã giảng dạy và hướng dẫn em trong học phần Đồ án CNTT 2. Nhờ có sự chỉ dạy của cô em mới có đủ kiến thức để hoàn thành bài báo cáo này.

## MỤC LỤC

LỜI NÓI ĐẦU .....	vi
<b>CHƯƠNG 1: TỔNG QUAN VỀ ĐỀ TÀI.....</b>	<b>1</b>
1.1 Lý do chọn đề tài.....	1
1.2 Mục tiêu nghiên cứu .....	1
1.3 Phạm vi nghiên cứu .....	1
1.4 Phương pháp nghiên cứu .....	2
1.5 Tầm quan trọng của đề tài trong ngữ cảnh công nghệ hiện đại.....	2
<b>CHƯƠNG 2: CƠ SỞ LÝ THUYẾT.....</b>	<b>4</b>
2.1 Khái niệm cơ bản về blockchain.....	4
2.2 Đặc điểm nổi bật của blockchain.....	5
2.3 Tìm hiểu về phân loại và các thể hệ của blockchain.....	5
2.3.1. Phân loại blockchain.....	5
2.3.2 Các thể hệ blockchain.....	8
2.4 Ứng dụng thực tiễn của blockchain .....	9
2.4.1. Tiền mã hóa - tiền điện tử .....	9
2.4.2. Ứng dụng chuyển tiền.....	9
2.4.3. Chuỗi cung ứng .....	10
2.4.4 Chăm sóc sức khỏe.....	10
2.4.5 Nhận dạng kỹ thuật số.....	11
2.4.6 Sử dụng vân tay để thực hiện các giao dịch trong nền tảng blockchain..	11
2.4.7 Ứng dụng bán lẻ .....	11
2.4.8 Bỏ phiếu .....	11
2.4.9 Hồ sơ tài sản .....	11
2.4.10 Tài chính ngân hàng .....	12
2.5 Ưu điểm và nhược điểm của công nghệ blockchain .....	13
2.5.1 Ưu điểm của blockchain .....	13
2.5.2 Nhược điểm của blockchain.....	13
2.6. Cách thức hoạt động của blockchain .....	13
2.7 Mục tiêu của an toàn và quyền riêng tư trong blockchain .....	14
<b>CHƯƠNG 3: AN TOÀN VÀ QUYỀN RIÊNG TƯ TRONG BLOCKCHAIN....</b>	<b>16</b>
3.1 Thế nào là an toàn và quyền riêng tư trong blockchain?.....	16

3.1.1 An toàn trong blockchain .....	16
3.1.2 Quyền riêng tư trong blockchain.....	16
3.1.3 Các mối đe dọa liên quan đến an toàn và quyền riêng tư trong blockchain .....	17
3.1.3.1 Tấn công 51%: .....	17
3.1.3.2 Tấn công Sybil:.....	18
3.1.3.3 Tấn công Eclipse: .....	19
3.1.3.4 Tấn công Replay: .....	19
3.1.3.5 Tấn công Phishing: .....	19
3.2 Một số vụ tấn công blockchain trong thực tế .....	19
3.2.1 Một số vụ tấn công vào hệ thống blockchain ở nước ngoài .....	19
3.2.2 Một số vụ tấn công vào hệ thống blockchain ở Việt Nam .....	21
3.2.3 Đánh giá .....	22
<b>CHƯƠNG 4. NGHIÊN CỨU CÁC GIẢI PHÁP ĐỂ ĐẢM BẢO AN TOÀN VÀ QUYỀN RIÊNG TƯ TRONG CÁC GIAO DỊCH BLOCKCHAIN .....</b>	<b>23</b>
4.1 Các giải pháp đảm bảo an toàn và quyền riêng tư trong các giao dịch blockchain .....	23
4.1.1 Mã hóa dữ liệu.....	23
4.1.2 Hashing .....	23
4.1.3 Cryptography (mật mã học) .....	24
4.1.3.1 Giới thiệu về Cryptography .....	24
4.1.3.2 Nguồn gốc của Cryptography .....	25
4.1.3.3 Các loại Cryptography trong Blockchain.....	25
4.1.3.4 Ứng dụng của cryptography trong blockchain .....	27
4.1.3.5 Ưu nhược điểm của cryptography .....	28
4.1.4 Cơ chế đồng thuận:.....	28
4.1.4.1 Tổng quan về cơ chế đồng thuận trong blockchain .....	28
4.1.4.2 Tầm quan trọng của thuật toán đồng thuận đối với Blockchain .....	29
4.1.4.3 Các cơ chế đồng thuận phổ biến.....	30
4.1.4.3.1 Proof of Work (PoW).....	31
4.1.4.3.2 Proof of Stake (PoS).....	32
4.1.4.3.3 Delegated Proof of Stake (DPoS).....	34

4.1.4.3.4 Proof of Authority (PoA) .....	35
4.1.4.3.5 Proof of Contribution (PoC) .....	35
4.1.5 Xác thực Blockchain .....	36
4.1.5.1 Xác thực Blockchain là gì? .....	36
4.1.5.2 Ví dụ về xác thực Blockchain .....	36
4.1.5.3 Xác thực 2 yếu tố là gì? .....	37
4.1.5.4 Tầm quan trọng của xác thực hai yếu tố .....	39
4.1.5.5 Blockchain cho xác thực 2 yếu tố .....	39
4.1.6 Tích hợp AI và Blockchain để bảo vệ quyền riêng tư .....	41
4.1.6.1 Khái quát .....	41
4.1.6.2 Bảo vệ quyền riêng tư thông qua việc tích hợp công nghệ Blockchain và AI .....	42
4.1.7 Sử dụng các giải pháp riêng tư: .....	44
<b>CHƯƠNG 5: SO SÁNH VÀ PHÂN TÍCH CÁC MÔ HÌNH QUYỀN RIÊNG TƯ KHÁC NHAU TRÊN BLOCKCHAIN .....</b>	<b>46</b>
5.1 Tìm hiểu và phân tích các mô hình quyền riêng tư trên blockchain: .....	46
5.1.1 Mô hình quyền riêng tư Zero-knowledge proof (ZKP) .....	46
5.1.1.1 Tổng quan về ZKP .....	46
5.1.1.2 Phương thức hoạt động của Zero-knowledge Proof .....	48
5.1.1.3 Ưu điểm và hạn chế của Zero-knowledge Proof .....	49
5.1.1.4 Phân loại loại Zero-knowledge Proof .....	50
5.1.1.4.1 ZK-SNARK .....	50
5.1.1.4.2 ZK-STARK .....	51
5.1.1.5 Ứng dụng phổ biến của Zero-knowledge Proof .....	51
5.1.2 Mô hình quyền riêng tư Ring Signatures (chữ ký dạng vòng) .....	54
5.1.2.1 Giới thiệu về Ring Signatures (chữ ký dạng vòng) .....	54
5.1.2.2 Cách thức hoạt động của Ring Signatures .....	54
5.1.2.3 Ưu nhược điểm của chữ ký vòng .....	56
5.1.2.4 Ứng dụng của chữ ký dạng vòng .....	56
5.1.3 Mô hình quyền riêng tư Mimblewimble .....	57
5.1.3.1 Những điều cơ bản về giao thức Mimblewimble Blockchain .....	57
5.1.3.2 Cách thức hoạt động: .....	58

5.1.3.3 Mật mã của Mimblewimble .....	60
5.1.3.4 Các tính năng cốt lõi của Mimblewimble: .....	62
5.1.3.5 Ứng dụng thực tế: .....	62
5.1.3.6 Ưu, nhược điểm của Mimblewimble .....	62
5.2. So sánh các mô hình quyền riêng tư: .....	63
5.2.1 Mimblewimble vs Monero .....	63
5.2.2 So sánh Zero-knowledge Proof với Ring Signatures .....	65
<b>CHƯƠNG 6: TRIỂN KHAI THỰC NGHIỆM .....</b>	<b>68</b>
6.1 Thực nghiệm cách hoạt động của blockchain và mã hóa bảo mật bằng hàm băm (hash) .....	68
6.1.1 Hàm băm (SHA256 Hash) .....	68
6.1.2 Block .....	68
6.1.3 Blockchain .....	69
<b>CHƯƠNG 7: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN .....</b>	<b>72</b>
7.1. Những điều làm được .....	72
7.2 Những điều chưa làm được .....	72
7.3 Hướng phát triển .....	72
<b>TÀI LIỆU THAM KHẢO .....</b>	<b>73</b>

## **LỜI NÓI ĐẦU**

Công nghệ blockchain đã và đang phát triển mạnh mẽ trong những năm gần đây, với nhiều ứng dụng tiềm năng trong các lĩnh vực khác nhau, bao gồm tài chính, thương mại điện tử, y tế,... Tuy nhiên, blockchain cũng tồn tại một số hạn chế, trong đó có vấn đề về an toàn và quyền riêng tư. Về an toàn, blockchain có thể bị tấn công bởi các hacker để đánh cắp tiền, dữ liệu hoặc thay đổi lịch sử giao dịch. Về quyền riêng tư, Blockchain là một hệ thống phi tập trung, vì vậy tất cả các giao dịch đều được công khai trên mạng lưới. Điều này khiến cho các giao dịch blockchain có thể bị theo dõi và phân tích bởi các bên thứ ba, gây ra những rủi ro về quyền riêng tư cho người dùng. Để khắc phục những hạn chế này việc hiểu rõ các rủi ro và các giải pháp đảm bảo an toàn và quyền riêng tư trong blockchain là rất cần thiết.



## **CHƯƠNG 1: TỔNG QUAN VỀ ĐỀ TÀI**

### **1.1 Lý do chọn đề tài**

Blockchain là một công nghệ mới với nhiều tiềm năng và đang được ứng dụng rộng rãi trong nhiều lĩnh vực khác nhau, từ tài chính, ngân hàng đến y tế, giáo dục. Tuy nhiên, một trong những thách thức lớn nhất của blockchain là vấn đề đảm bảo an toàn và quyền riêng tư. Về an toàn, blockchain được thiết kế với cơ chế đồng thuận phân tán, giúp chống lại các cuộc tấn công mạng như giả mạo, chối bỏ giao dịch,... Tuy nhiên, blockchain vẫn có thể bị tấn công bởi các lỗ hổng bảo mật trong các thuật toán mã hóa hoặc các lỗi phần mềm. Về quyền riêng tư, blockchain được thiết kế để minh bạch, tức là mọi giao dịch đều được ghi lại trên sổ cái công khai. Điều này có thể khiến các thông tin nhạy cảm của người dùng bị rò rỉ. Do đó, việc nghiên cứu các giải pháp để đảm bảo an toàn và quyền riêng tư trong blockchain là rất cần thiết. Đề tài “Đảm bảo an toàn và quyền riêng tư trong blockchain” với hai nội dung chính: Nghiên cứu các giải pháp để đảm bảo an toàn và quyền riêng tư trong các giao dịch blockchain, so sánh và phân tích các mô hình quyền riêng tư khác nhau trên blockchain.

Việc nghiên cứu các giải pháp để đảm bảo an toàn và quyền riêng tư trong blockchain là một đề tài mang tính thực tiễn cao, góp phần thúc đẩy sự phát triển của công nghệ này cũng như bảo vệ người dùng tránh khỏi các nguy cơ bị đánh cắp dữ liệu và tấn công mạng.

### **1.2 Mục tiêu nghiên cứu**

- Nghiên cứu về các mối đe dọa liên quan đến an toàn và quyền riêng tư trong Blockchain
- Nghiên cứu các giải pháp để đảm bảo an toàn và quyền riêng tư trong các giao dịch Blockchain
- Nghiên cứu, so sánh, đánh giá ưu nhược điểm của các mô hình quyền riêng tư trên Blockchain
- Triển khai thực nghiệm và đánh giá kết quả

### **1.3 Phạm vi nghiên cứu**

Phạm vi nghiên cứu về “Đảm bảo An toàn và Quyền riêng tư trong Blockchain” bao gồm những khía cạnh sau:

–Tập trung vào việc nghiên cứu các giải pháp để đảm bảo an toàn và quyền riêng tư trong các giao dịch trên blockchain. Bao gồm xem xét các phương pháp mã hóa phức tạp và các mô hình quản lý quyền riêng tư khác nhau trên blockchain.

–Nghiên cứu về quyền riêng tư trong blockchain: Tìm hiểu các mô hình và giải pháp nhằm bảo vệ quyền riêng tư của người dùng trong môi trường blockchain.

–Phân tích các ứng dụng blockchain và vấn đề an toàn/quyền riêng tư liên quan: Nghiên cứu các lĩnh vực ứng dụng của blockchain, như tài chính, y tế, chuỗi cung ứng và xem xét các vấn đề an toàn và quyền riêng tư cụ thể mà các lĩnh vực này đang đối mặt. Từ đó, đưa ra các giải pháp phù hợp để đảm bảo an toàn và quyền riêng tư trong từng ngữ cảnh cụ thể.

#### **1.4 Phương pháp nghiên cứu**

–Đánh giá và phân tích các công trình nghiên cứu có liên quan: Xem xét các nghiên cứu đã được công bố trước đây về an toàn và quyền riêng tư trong blockchain. Đánh giá các phương pháp và giải pháp đã được đề xuất và xác định các hạn chế và điểm mạnh của chúng.

–Đánh giá hiệu quả và ưu điểm của các phương pháp nghiên cứu: Dựa trên việc so sánh và phân tích các giải pháp và mô hình quyền riêng tư khác nhau, tiến hành đánh giá hiệu quả và ưu điểm của từng phương pháp nghiên cứu. Điều này giúp xác định các phương pháp nào có hiệu quả nhất và phù hợp nhất trong việc đảm bảo an toàn và quyền riêng tư trên blockchain.

–Đề xuất và phát triển các giải pháp và mô hình quyền riêng tư: Dựa trên kết quả đánh giá, đề xuất và phát triển các giải pháp và mô hình quyền riêng tư mới hoặc cải tiến để cải thiện an toàn và quyền riêng tư trong các giao dịch blockchain. Các giải pháp này có thể bao gồm việc sử dụng các phương pháp mã hóa tiên tiến, phát triển mô hình quản lý quyền riêng tư thông minh và các công nghệ mới khác.

–Nghiên cứu thực nghiệm và phân tích dữ liệu: Thực hiện các thí nghiệm và nghiên cứu thực tế để đánh giá hiệu quả của các giải pháp an toàn và quyền riêng tư trong blockchain. Phân tích dữ liệu thu thập được từ các giao dịch blockchain và đánh giá các tiêu chí liên quan đến an toàn và quyền riêng tư.

#### **1.5 Tầm quan trọng của đề tài trong ngữ cảnh công nghệ hiện đại**

–Trong bối cảnh công nghệ ngày càng phát triển, đề tài “Đảm bảo an toàn và quyền riêng tư trong Blockchain” đóng vai trò vô cùng quan trọng. Blockchain, một

công nghệ mới đầy tiềm năng, đã thay đổi cách chúng ta thực hiện giao dịch và quản lý thông tin. Tuy nhiên, điều này cũng đặt ra những thách thức về an toàn và quyền riêng tư.

–Đầu tiên, nghiên cứu các giải pháp để đảm bảo an toàn và quyền riêng tư trong các giao dịch Blockchain là rất cần thiết. Với tính chất phân tán và công khai của blockchain, việc bảo vệ dữ liệu và thông tin cá nhân trở nên phức tạp hơn bao giờ hết. Các nhà nghiên cứu cần tìm hiểu và phân tích các phương pháp, giao thức và công nghệ mới để đảm bảo rằng các giao dịch trên blockchain không bị xâm phạm và thông tin cá nhân của người dùng được bảo vệ một cách tối đa.

–Tiếp theo, so sánh và phân tích các mô hình quyền riêng tư khác nhau trên blockchain cũng là một mặt quan trọng của đề tài này. Có nhiều cách tiếp cận để đảm bảo quyền riêng tư trên blockchain, từ các giao thức mã hóa đến các mô hình quản lý quyền riêng tư phức tạp. Bằng cách so sánh và phân tích các mô hình này, chúng ta có thể đánh giá hiệu quả và ưu điểm của từng phương pháp và đưa ra những khuyến nghị và hướng phát triển tiếp theo.

–Với những điều trên, đề tài “Đảm bảo an toàn và quyền riêng tư trong Blockchain” trở nên vô cùng cần thiết trong ngữ cảnh công nghệ hiện đại. Việc nghiên cứu và áp dụng các giải pháp và mô hình quyền riêng tư trong blockchain sẽ đảm bảo rằng công nghệ này có thể phát triển một cách bền vững và đáng tin cậy, đồng thời bảo vệ quyền lợi và thông tin cá nhân của người dùng.

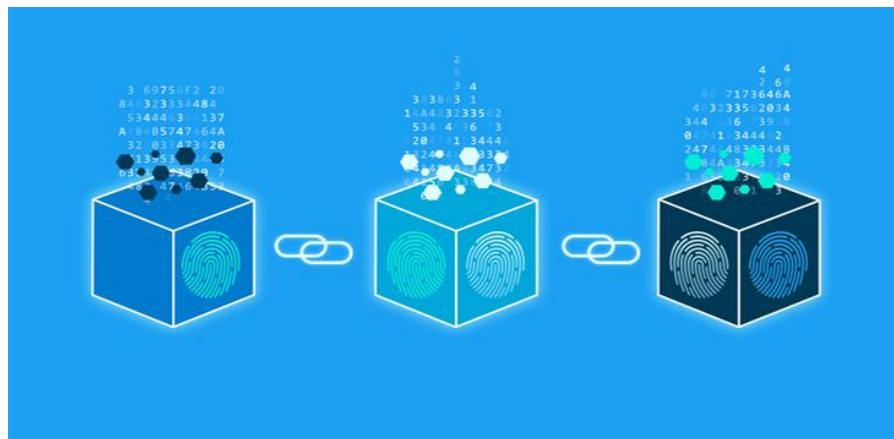
## CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

### 2.1 Khái niệm cơ bản về blockchain

–Blockchain là công nghệ chuỗi – khối, cho phép truyền tải dữ liệu một cách an toàn dựa trên hệ thống mã hóa vô cùng phức tạp, tương tự như cuốn sổ cái kế toán của một công ty, nơi mà tiền được giám sát chặt chẽ và ghi nhận mọi giao dịch trên mạng ngang hàng. Điều này thấy được rằng trong toàn bộ hệ thống thông tin được tạo thành nhiều phiên bản và được lưu trữ ở nhiều nơi.

–Mỗi khối (block) đều chứa thông tin về thời gian khởi tạo và được liên kết với khối trước đó, kèm theo đó là một mã thời gian và dữ liệu giao dịch. Vì các khối blockchain được liên kết với nhau nên không thể chỉnh sửa, thay đổi hoặc xóa các thông tin có sẵn bằng bất kỳ cách nào, vì điều này sẽ làm vô hiệu hoá tất cả các khối dữ liệu theo sau chúng. Blockchain được thiết kế để chống lại việc gian lận, thay đổi của dữ liệu.

–Đây là một hệ thống tương tự như P2P (Peer to Peer), loại bỏ tất cả các giao dịch trung gian, giúp tăng cường an ninh, sự minh bạch và ổn định cũng như giảm chi phí và lỗi giao dịch do người dùng gây ra. Bằng cách phân chia dữ liệu cho tất cả người dùng vì thế thông tin khó có thể bị chỉnh sửa, phá hủy hoặc thay đổi. Công nghệ blockchain đã tạo ra xương sống cho loại hình internet mới và còn được phát triển hơn trong tương lai.



Hình 2.1. Hình ảnh minh họa blockchain

#### Công nghệ Blockchain – sự kết hợp giữa 3 loại công nghệ:

–**Mật mã học:** để đảm bảo tính minh bạch, toàn vẹn và riêng tư thì công nghệ Blockchain đã sử dụng public key và hàm hash function

–**Mạng ngang hàng:** Mỗi một nút trong mạng được xem như một client và cũng là server để lưu trữ bản sao ứng dụng

–**Lý thuyết trò chơi:** Tất cả các nút tham gia vào hệ thống đều phải tuân thủ luật chơi đồng thuận (giao thức PoW, PoS,...) và được thúc đẩy bởi động lực kinh tế.

## 2.2 Đặc điểm nổi bật của blockchain

–**Không thể làm giả, không thể phá hủy các chuỗi Blockchain:** theo như lý thuyết thì chỉ có máy tính lượng tử mới có thể giải mã Blockchain và công nghệ Blockchain biến mất khi không còn Internet trên toàn cầu.

–**Tính bất biến:** dữ liệu đã được thêm vào blockchain không thể chỉnh sửa và được lưu trữ mãi mãi.

–**Tính bảo mật:** thông tin và dữ liệu lưu trong blockchain sẽ được phân tán cho tất cả người dùng và đảm bảo an toàn tuyệt đối.

–**Tính minh bạch:** người dùng đều có thể theo dõi các dữ liệu có trong sổ cái blockchain, có thể thống kê toàn bộ lịch sử giao dịch có trên nền tảng.

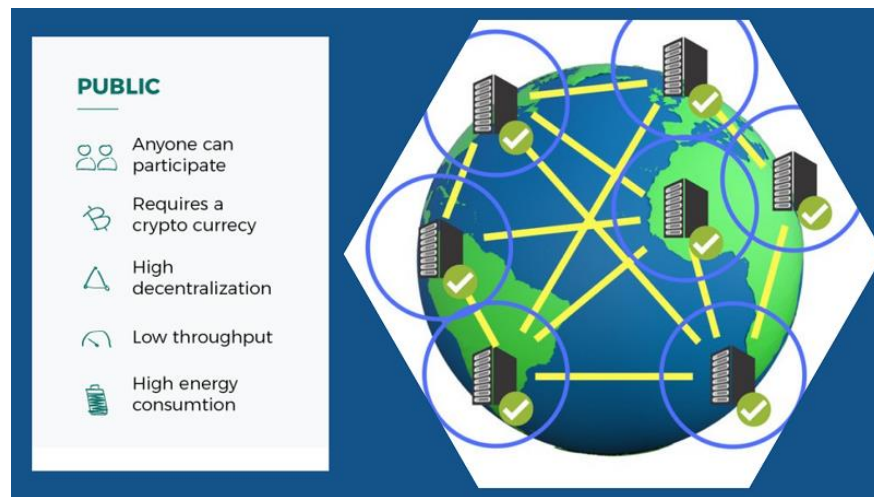
–**Hợp đồng thông minh (Smart Contract):** là hợp đồng kỹ thuật số cho phép người dùng giao dịch, thực thi mà không cần qua trung gian.

## 2.3 Tìm hiểu về phân loại và các thể hệ của blockchain

### 2.3.1. Phân loại blockchain

Hệ thống Blockchain chia thành 3 loại chính:

**Blockchain công khai (Public Blockchain):** Đây là loại Blockchain mở và công khai cho tất cả mọi người tham gia. Bất kỳ ai cũng có thể tham gia vào việc xác minh và thực hiện giao dịch trên Blockchain này. Các ví dụ điển hình của Blockchain công khai là Bitcoin, Ethereum (trước khi chuyển sang Ethereum 2.0), và nhiều loại tiền điện tử công cộng khác. Trên Blockchain công khai, mọi giao dịch đều được công khai, minh bạch và không thể thay đổi sau khi đã được ghi lại.



Hình 2.2 Public blockchain cho phép mọi người dùng truy cập và kiểm tra dữ liệu

**Blockchain riêng tư (Private Blockchain):** Đây là loại Blockchain được giới hạn và chỉ cho phép một số lượng nhất định các bên tham gia được chọn trước. Thông thường, việc xác minh và thực hiện giao dịch trên Blockchain riêng tư được quy định bởi một nhóm hoặc tổ chức cụ thể. Blockchain riêng tư thường được sử dụng trong các doanh nghiệp và tổ chức nơi các bên tham gia đã được xác định và tin cậy. Các giao dịch trên Blockchain riêng tư có thể được bảo mật hơn và có thể yêu cầu sự xác minh trước khi được thực hiện.

–So với các blockchain công khai, các nền tảng blockchain riêng tư cung cấp hiệu suất được cải thiện, chi phí giao dịch thấp hơn và khả năng mở rộng tốt hơn. Chúng cũng phù hợp hơn cho các doanh nghiệp yêu cầu tuân thủ các quy định và yêu cầu pháp lý cụ thể, chẳng hạn như các doanh nghiệp trong ngành tài chính và chăm sóc sức khỏe.

–Ví dụ: Một số ứng dụng Blockchain trong doanh nghiệp hoặc các hệ thống quản lý tài chính nội bộ.

**Consortium (Blockchain kết hợp):** Là sự kết hợp giữa Public và Private. Đây là một hệ thống Blockchain nơi quyền kiểm soát và quản lý được chia sẻ giữa một nhóm các tổ chức hoặc các thành viên cụ thể. Thay vì chỉ có một tổ chức duy nhất kiểm soát toàn bộ hệ thống, các bên tham gia trong mạng lưới Blockchain Consortium chia sẻ quyền kiểm soát và quản lý. Điều này thường được sử dụng trong các ngành công nghiệp hoặc liên minh nơi nhiều tổ chức cần làm việc cùng nhau và chia sẻ dữ liệu mà không tin tưởng một bên duy nhất.

–Ví dụ: Các ngân hàng hay tổ chức tài chính liên doanh sẽ sử dụng Blockchain cho riêng mình.

Giữa các loại blockchain có những đặc điểm và sự khác nhau rõ rệt:

	Loại blockchain		
	Công khai	Riêng tư	Consortium
Có cần được cấp quyền để sửa đổi dữ liệu?	Có	Không	Không
Ai có thể đọc dữ liệu trên blockchain?	Bất kỳ ai	Chỉ những người dùng được mời	Tùy thuộc
Ai có thể ghi dữ liệu?	Bất kỳ ai	Những người tham gia được chấp thuận	Những người tham gia được chấp thuận
Quyền sở hữu	Không ai	Một tổ chức duy nhất	Nhiều tổ chức
Người tham gia có bị tiết lộ danh tính	Không	Có	Có
Tốc độ giao dịch	Chậm	Nhanh	Nhanh

*Hình 2.3. Sự khác nhau về đặc điểm của từng loại Blockchain*

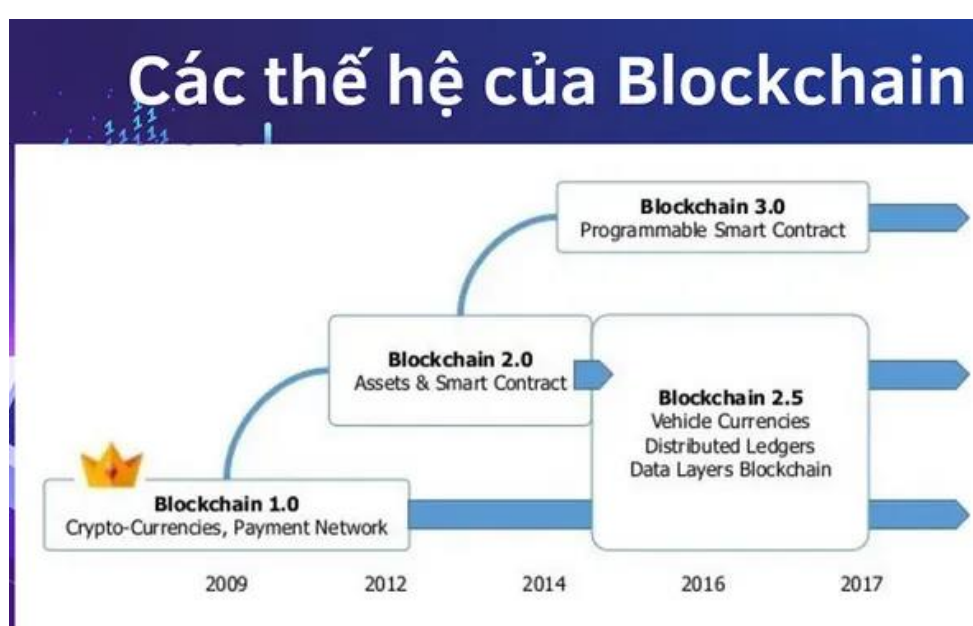
Sự khác biệt này có ý nghĩa quan trọng về nơi thông tin (có khả năng bí mật) di chuyển qua mạng được lưu trữ và ai có quyền truy cập vào nó. Chỉ từ đó, bạn có thể thấy một blockchain công khai có thể không phù hợp với doanh nghiệp như thế nào. Một sự khác biệt quan trọng và liên quan khác là các blockchain công khai thường được thiết kế xung quanh nguyên tắc ẩn danh, trong khi các blockchain riêng sử dụng danh tính để xác nhận tư cách thành viên và đặc quyền truy cập, và vì vậy những người tham gia trong mạng biết chính xác họ đang giao dịch với ai.

Một cách chính khác mà các blockchain công khai và riêng tư khác nhau là cách các giao dịch được xác minh. Về cơ bản, để một giao dịch được thêm vào blockchain, những người tham gia mạng phải đồng ý rằng đó là phiên bản duy nhất và được xác thực. Điều đó được thực hiện thông qua sự đồng thuận, có nghĩa là thỏa thuận. Bitcoin có lẽ là ví dụ nổi tiếng nhất về blockchain công khai và nó đạt được sự đồng thuận thông qua “mining”. Trong khai thác Bitcoin, các máy tính trên mạng (hoặc thợ đào) cố gắng giải quyết một vấn đề mật mã phức tạp để tạo ra bằng chứng công việc. Hạn

chế là điều này đòi hỏi một lượng lớn sức mạnh tính toán, đặc biệt là đối với các blockchain công cộng quy mô lớn.

Ngoài ra, một blockchain riêng bao gồm một mạng lưới được phép, trong đó sự đồng thuận có thể đạt được thông qua một quá trình gọi là “selective endorsement,” (chứng thực chọn lọc) nơi người dùng đã biết xác minh các giao dịch. Ưu điểm của việc này đối với các doanh nghiệp là chỉ những người tham gia có quyền truy cập và quyền thích hợp mới có thể duy trì sổ cái giao dịch. Vẫn còn một vài vấn đề với phương pháp này, bao gồm các mối đe dọa từ người trong cuộc, nhưng nhiều vấn đề trong số đó có thể được giải quyết bằng cơ sở hạ tầng bảo mật cao.

### 2.3.2 Các thể hệ blockchain



Hình 2.4 Biểu đồ sự hình thành và phát triển của nền tảng Blockchain

**-Công nghệ Blockchain 1.0 – Tiền tệ và Thanh toán:** Ứng dụng chính của phiên bản này là tiền mã hoá: bao gồm việc chuyển đổi tiền tệ và tạo lập hệ thống thanh toán kỹ thuật số. Được xây dựng và phát triển từ 2008. Đây cũng là lĩnh vực quen thuộc với chúng ta nhất mà đôi khi khá nhiều người lầm tưởng Bitcoin và Blockchain là một.

**- Công nghệ Blockchain 2.0 – Tài chính và Thị trường:** Ứng dụng xử lý tài chính và ngân hàng: mở rộng quy mô của Blockchain, đưa vào các ứng dụng tài chính và thị trường. Sử dụng hợp đồng thông minh (Smart contract) nhằm giảm thiểu khả năng gian lận trong quá trình vận hành, tăng tính minh bạch cho nền tảng.



Ví dụ điển hình là Ethereum. Được xây dựng và phát triển từ 2012-2014. Blockchain 2.0 được ứng dụng sâu hơn vào trong đời sống cụ thể: Ứng dụng blockchain vào kinh tế, tài chính, chứng khoán, trái phiếu, ...

- **Công nghệ Blockchain 3.0 – Thiết kế và Giám sát hoạt động:** Đưa Blockchain vượt khỏi biên giới tài chính, và đi vào các lĩnh vực như giáo dục, chính phủ, y tế và nghệ thuật. Được xây dựng và phát triển từ 2016-2017.

## 2.4 Ứng dụng thực tiễn của blockchain

### 2.4.1. Tiền mã hóa - tiền điện tử

– Tiền mã hóa được gọi là tiền điện tử hay tiền kỹ thuật số. Là phương tiện trao đổi tiền tệ mạnh mẽ mà không bị hư hỏng theo thời gian và cũng không cần đến người gác cổng cũng như người trung gian để kiểm duyệt các giao dịch.

– Người dùng có thể chuyển và nhận tiền cho tất cả các người dùng khác trên toàn thế giới. Bên cạnh đó, chi phí giao dịch tương đối nhỏ và thời gian giao dịch lại rất nhanh chóng. Các đồng tiền sẽ không thể bị thu hồi hoặc các giao dịch không thể bị đảo ngược hoặc đóng băng.



Hình 2.5. Hai loại tiền mã hóa đầu tiên là Bitcoin (BTC) và Ether (ETH)

### 2.4.2. Ứng dụng chuyển tiền

– Chuyển tiền trong nước tương đối dễ dàng, tuy nhiên việc gửi tiền quốc tế đòi hỏi rất nhiều thủ tục ở các ngân hàng truyền thống. Phí chuyển tiền và thời gian chuyển tương đối chậm, không phù hợp với các giao dịch khẩn cấp vì có mạng lưới trung gian phức tạp. Hệ thống tiền mã hóa trong blockchain đã loại bỏ được yếu tố trung gian này giúp quá trình chuyển tiền diễn ra nhanh chóng, phí giao dịch rẻ.



Hình 2.6 Hệ thống tiền mã hóa blockchain giúp việc chuyển tiền tương đối dễ dàng, nhanh chóng

### 2.4.3. Chuỗi cung ứng

Blockchain chuỗi khối góp phần tạo nên một hệ sinh thái giúp quản lý cơ sở dữ liệu một cách minh bạch và đem lại nhiều cải tiến cho vô số ngành công nghiệp. Sau đây là một số ứng dụng trong quy trình của một chuỗi cung ứng:

- Theo dõi quy trình và lịch trình sản xuất
- Kiểm soát số lượng hàng hóa mua vào, bán ra
- Quản lý hàng tồn trong kho, bãi sản xuất
- Kiểm tra và truy xuất thông tin sản phẩm được sản xuất qua các khâu
- Theo dõi, quản lý nguồn cung nguyên vật liệu trong sản xuất công nghiệp



Hình 2.7 Blockchain là công nghệ trọng tâm giúp quản lý chuỗi cung ứng trong tương lai

### 2.4.4 Chăm sóc sức khỏe

– Với tính minh bạch và tuyệt đối bảo mật của công nghệ blockchain đã giúp nó trở thành nền tảng lý tưởng để lưu giữ hồ sơ trong lĩnh vực y tế (gồm bệnh viện, phòng

khám hoặc các nhà cung cấp dịch vụ thiết bị y tế). Bằng cách mã hóa các dữ liệu hồ sơ, bệnh nhân có thể bảo mật quyền riêng tư của họ mà không tổ chức nào có quyền truy cập vào cơ sở dữ liệu trên toàn cầu.

#### **2.4.5 Nhận dạng kỹ thuật số**

–Thế giới rất cần một giải pháp để nhận dạng danh tính từng người dùng. Danh tính vật lý như thẻ chứng minh nhân dân thường rất dễ bị làm giả và không có sẵn cho nhiều cá nhân. Từ đó nhờ vào ứng dụng nhận dạng kỹ thuật số của blockchain, người dùng có thể kiểm soát tốt hơn và thời điểm sử dụng các thông tin cá nhân.

–Ngoài ra, chuỗi blockchain có thể bảo mật và riêng tư hơn thông qua việc sử dụng mật mã cho các hệ thống (mật mã số, vân tay hoặc face ID).

#### **2.4.6 Sử dụng vân tay để thực hiện các giao dịch trong nền tảng blockchain**

–Hệ thống nhận dạng kỹ thuật số đáng tin cậy hơn các hệ thống truyền thống. Việc sử dụng chữ ký kỹ thuật số giúp nhận diện người dùng và xác minh giao dịch một cách dễ dàng hơn. Điều này sẽ khiến người khác khó làm sai lệch thông tin và bảo vệ hiệu quả hệ thống dữ liệu của người dùng.

#### **2.4.7 Ứng dụng bán lẻ**

–Ứng dụng blockchain trong việc bán lẻ là hết sức cần thiết. Sử dụng blockchain giúp bảo mật dữ liệu của khách hàng, việc thanh toán nhanh gọn và vô cùng tiện lợi, khách hàng có thể truy xuất nguồn gốc của sản phẩm tại cửa hàng, tích lũy điểm mua hàng cho người dùng, ... Các nhãn hàng nổi tiếng đã sử dụng công nghệ này trong hoạt động kinh doanh là: Amazon, Unilever hay Nestle.

#### **2.4.8 Bỏ phiếu**

–Blockchain có thể tạo điều kiện cho một hệ thống bỏ phiếu hiện đại. Bỏ phiếu bằng blockchain mang tiềm năng loại bỏ gian lận bầu cử và tăng tỷ lệ cử tri đi bầu, như đã được thử nghiệm trong cuộc bầu cử giữa kỳ tháng 11 năm 2018 ở Tây Virginia.

–Sử dụng blockchain theo cách này sẽ làm cho phiếu bầu gần như không thể giả mạo. Giao thức blockchain cũng sẽ duy trì tính minh bạch trong quá trình bầu cử, giảm nhân sự cần thiết để tiến hành bầu cử và cung cấp cho các quan chức kết quả gần như ngay lập tức. Điều này sẽ loại bỏ sự cần thiết phải kiểm phiếu lại hoặc bất kỳ mối quan tâm thực sự nào rằng gian lận có thể đe dọa cuộc bầu cử.

#### **2.4.9 Hồ sơ tài sản**

Nếu bạn đã từng dành thời gian trong Văn phòng Ghi âm địa phương của mình, bạn sẽ biết rằng việc ghi lại quyền sở hữu vừa nặng nề vừa không hiệu quả. Ngày nay, một chứng thư vật lý phải được gửi đến một nhân viên chính phủ tại văn phòng ghi âm địa phương, nơi nó được nhập thủ công vào cơ sở dữ liệu trung tâm và chỉ mục công khai của quận. Trong trường hợp tranh chấp tài sản, yêu cầu đối với tài sản phải được hòa giải với chỉ số công khai.

Quá trình này không chỉ tốn kém và tốn thời gian, nó cũng dễ bị lỗi của con người, trong đó mỗi sự không chính xác làm cho việc theo dõi quyền sở hữu tài sản kém hiệu quả hơn. Blockchain có khả năng loại bỏ nhu cầu quét tài liệu và theo dõi các tệp vật lý trong phòng hành chính ở địa phương. Nếu quyền sở hữu tài sản được lưu trữ và xác minh trên blockchain, chủ sở hữu có thể tin tưởng rằng chứng thư của họ là chính xác và được ghi lại vĩnh viễn.

Ở các quốc gia bị chiến tranh tàn phá hoặc các khu vực có ít hoặc không có chính phủ hoặc cơ sở hạ tầng tài chính và không có Văn phòng luật, việc chứng minh quyền sở hữu tài sản có thể gần như không thể. Nếu một nhóm người sống trong một khu vực như vậy có thể tận dụng blockchain, thì các mốc thời gian minh bạch và rõ ràng về quyền sở hữu tài sản có thể được thiết lập.

#### **2.4.10 Tài chính ngân hàng**

Có lẽ không có ngành công nghiệp nào được hưởng lợi từ việc tích hợp blockchain vào hoạt động kinh doanh của mình nhiều hơn ngân hàng. Các tổ chức tài chính chỉ hoạt động trong giờ làm việc, thường là năm ngày một tuần. Điều đó có nghĩa là nếu bạn cố gắng gửi tiền vào thứ Sáu lúc 6 giờ chiều, bạn có thể sẽ phải đợi đến sáng thứ Hai để thấy tiền đó vào tài khoản của bạn.

Ngay cả khi bạn gửi tiền trong giờ làm việc, giao dịch vẫn có thể mất từ một đến ba ngày để xác minh do khối lượng giao dịch tuyệt đối mà các ngân hàng cần giải quyết. Nhưng với blockchain thì lại khác bởi nó không bao giờ ngủ.

Bằng cách tích hợp blockchain vào ngân hàng, người tiêu dùng có thể thấy các giao dịch của họ được xử lý trong vài phút hoặc vài giây – thời gian cần thiết để thêm một khối vào blockchain, bất kể ngày lễ hay thời gian trong ngày hoặc tuần. Với blockchain, các ngân hàng cũng có cơ hội trao đổi tiền giữa các tổ chức nhanh chóng và an toàn hơn. Với quy mô của các khoản tiền liên quan, ngay cả vài ngày tiền được vận chuyển cũng có thể mang lại chi phí và rủi ro đáng kể cho các ngân hàng.

Quá trình thanh toán và thanh toán bù trừ cho các nhà giao dịch chứng khoán có thể mất đến ba ngày (hoặc lâu hơn nếu giao dịch quốc tế), có nghĩa là tiền và cổ phiếu bị đóng băng trong khoảng thời gian đó. Blockchain có thể giảm đáng kể thời gian đó.

## **2.5 Ưu điểm và nhược điểm của công nghệ blockchain**

### **2.5.1 Ưu điểm của blockchain**

–Độ chính xác cao hơn của các giao dịch: Bởi vì một giao dịch blockchain phải được xác minh bởi nhiều nút. Điều này có thể giảm thiểu lỗi.

–Không cần trung gian: Khi sử dụng blockchain, hai bên trong một giao dịch có thể xác nhận và hoàn thành điều gì đó mà không cần làm việc thông qua bên thứ ba. Điều này giúp tiết kiệm thời gian cũng như chi phí thanh toán cho một đơn vị trung gian như ngân hàng.

–Bảo mật bổ sung: Về mặt lý thuyết, một mạng lưới phi tập trung, như blockchain khiến ai đó gần như không thể thực hiện các giao dịch gian lận. Để tham gia vào các giao dịch giả mạo, họ sẽ cần phải hack mọi nút và thay đổi mọi dữ liệu của sổ cái.

–Chuyển tiền hiệu quả hơn: Vì các blockchain hoạt động 24/7 nên mọi người có thể thực hiện chuyển tiền tài chính và tài sản hiệu quả hơn, đặc biệt là trên phạm vi quốc tế. Họ không cần phải đợi nhiều ngày để ngân hàng hoặc cơ quan chính phủ xác nhận mọi thứ theo cách thủ công.

### **2.5.2 Nhược điểm của blockchain**

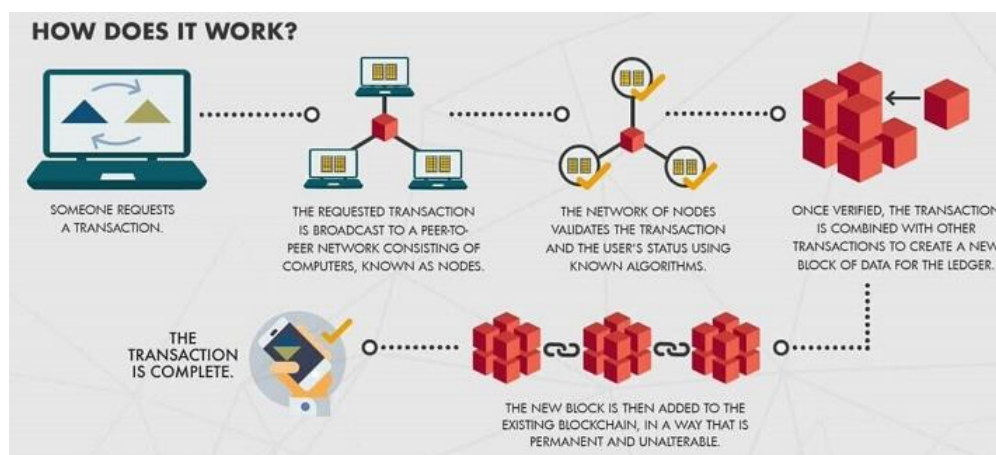
–Giới hạn giao dịch mỗi giây: Blockchain phụ thuộc vào một mạng lưới lớn hơn để phê duyệt các giao dịch nên có một giới hạn về tốc độ di chuyển của nó. Chẳng hạn, Bitcoin chỉ có thể xử lý 4,6 giao dịch mỗi giây.

–Chi phí năng lượng cao: Việc để tất cả các nút hoạt động để xác minh giao dịch tốn nhiều điện hơn đáng kể so với một cơ sở dữ liệu hoặc bảng tính đơn lẻ. Điều này không chỉ làm cho các giao dịch dựa trên blockchain trở nên đắt hơn mà còn tạo ra gánh nặng hơn cho môi trường.

–Rủi ro mất mát tài sản: Một số tài sản kỹ thuật số được đảm bảo sử dụng một khóa mật mã như cryptocurrency trong một chiếc ví blockchain. Bạn cần bảo vệ cẩn thận chìa khóa này. Nếu chủ sở hữu tài sản kỹ thuật số đánh mất khóa mật mã riêng tư cho phép họ truy cập vào tài sản của mình thì hiện tại không có cách nào để khôi phục nó và tài sản đó sẽ biến mất vĩnh viễn.

## **2.6. Cách thức hoạt động của blockchain**

–Ưu điểm lớn nhất của nền tảng blockchain là cho phép người dùng có thể tương tác với nhau bởi một nguồn được chia sẻ mà không cần có sự tin tưởng. Với cấu trúc là mạng phân tán thông tin thì không bên nào có thể tấn công vào một hệ thống blockchain được xây dựng chặt chẽ.



*Hình 2.8 Cách thức hoạt động của nền tảng blockchain*

–Để chạy và thực hiện một giao dịch trên nền tảng blockchain, người dùng phải tải xuống một phần mềm. Sau khi phần mềm được cài đặt, người dùng bắt đầu thực hiện giao dịch. Từ đó các khối chứa giao dịch sẽ được tạo ra.

–Sau đó các khối sẽ được gửi đến cái máy trong mạng và được xác minh giao dịch. Các khối này được thêm vào chuỗi blockchain và giao dịch được xác nhận là thành công. Một giao dịch thông thường chỉ mất khoảng 05 - 15 phút, rất nhanh và đơn giản.

–Những gì chúng ta có là một hệ sinh thái được hình thành từ hàng trăm, hàng nghìn giao dịch được đồng bộ hóa thành cơ sở dữ liệu và được lưu trữ trong các khối giao dịch. Tất cả thông tin giao dịch vừa được tạo ra sẽ được lưu trữ vào khối chứa giao dịch, người dùng đều có thể truy xuất và xem thông tin chi tiết của giao dịch đó.

## **2.7 Mục tiêu của an toàn và quyền riêng tư trong blockchain**

An toàn và quyền riêng tư là hai mục tiêu quan trọng trong thiết kế và triển khai các hệ thống Blockchain.

–Bảo mật: Mục tiêu chính của an toàn trong Blockchain là đảm bảo rằng dữ liệu và giao dịch trên hệ thống không bị sửa đổi, làm giả hoặc thay đổi một cách trái phép. Các biện pháp bảo mật, chẳng hạn như mã hóa và chữ ký điện tử, được sử dụng để bảo vệ tính toàn vẹn của dữ liệu và đảm bảo rằng chỉ những người có quyền truy cập mới có thể thay đổi dữ liệu.

–Tính toàn vẹn: Blockchain đảm bảo tính toàn vẹn bằng cách sử dụng mã băm (hash) để liên kết các khối với nhau. Mỗi khối chứa mã băm của khối trước đó, khiến cho việc thay đổi nội dung của một khối sẽ làm thay đổi mã băm của khối đó và tất cả các khối tiếp theo. Điều này làm cho việc tấn công và thay đổi dữ liệu trở nên khó khăn và dễ bị phát hiện.

–Quyền riêng tư: Trong một số trường hợp, Blockchain cũng đặt mục tiêu bảo vệ quyền riêng tư của người dùng. Mặc dù Blockchain công khai (Public Blockchain) có thể hiển thị các giao dịch công khai và minh bạch, nhưng các biện pháp bảo mật như chữ ký điện tử và mã hóa đảm bảo rằng chỉ người dùng có quyền truy cập mới có thể xem và xác minh thông tin chi tiết về giao dịch.

–Quản lý quyền truy cập: Blockchain cũng có thể ứng dụng các cơ chế quản lý quyền truy cập để kiểm soát việc xem, xác minh và thực hiện giao dịch trên hệ thống. Các quy tắc và quyền hạn được thiết lập để xác định ai có quyền tham gia vào mạng lưới, xem thông tin và thực hiện các tác vụ cụ thể. Điều này đảm bảo rằng chỉ những bên được ủy quyền mới có thể thực hiện các hoạt động trên hệ thống.

## **CHƯƠNG 3: AN TOÀN VÀ QUYỀN RIÊNG TƯ TRONG BLOCKCHAIN**

### **3.1 Thế nào là an toàn và quyền riêng tư trong blockchain?**

–An toàn và quyền riêng tư trong blockchain là những khái niệm liên quan đến việc bảo vệ dữ liệu, tài sản và danh tính của người dùng trên một mạng blockchain. Blockchain là một loại cơ sở dữ liệu phân tán, được duy trì bởi nhiều máy tính trên toàn thế giới, ghi lại các giao dịch kỹ thuật số một cách an toàn và bất biến. Blockchain có thể được sử dụng cho nhiều mục đích khác nhau, như tiền mã hóa, hợp đồng thông minh, token không thể thay thế (NFT) và nhiều ứng dụng khác

#### **3.1.1 An toàn trong blockchain**

–An toàn trong blockchain đề cập đến việc đảm bảo rằng mạng blockchain không bị tấn công, thao túng hoặc làm sai lệch bởi các bên xấu. Để đạt được điều này, blockchain sử dụng nhiều kỹ thuật mã hóa, đồng thuận và phân quyền để bảo vệ dữ liệu và giao dịch trên mạng. Một số ví dụ về các kỹ thuật an toàn trong blockchain như:

- + Mã hóa: Mã hóa là quá trình biến đổi dữ liệu thành một định dạng không thể đọc được bởi bất kỳ ai không có khóa bí mật. Mã hóa được sử dụng để bảo vệ dữ liệu trên blockchain khỏi bị đánh cắp hoặc thay đổi bởi những người không được phép. Một số loại mã hóa phổ biến trong blockchain là mã hóa đối xứng, mã hóa bất đối xứng và mã hóa đa chữ ký

- + Đồng thuận: Đồng thuận là quá trình đạt được sự thống nhất về trạng thái của mạng blockchain giữa các nút tham gia. Đồng thuận giúp đảm bảo tính nhất quán và toàn vẹn của dữ liệu trên blockchain, cũng như ngăn chặn các giao dịch giả mạo hoặc trùng lặp. Một số thuật toán đồng thuận phổ biến trong blockchain là chứng minh công việc (Proof of Work), chứng minh cổ phần (Proof of Stake) và chứng minh ủy quyền (Proof of Authority).

- + Phân quyền: Phân quyền là quá trình phân phối quyền kiểm soát và ra quyết định của mạng blockchain giữa nhiều bên tham gia, thay vì tập trung vào một bên duy nhất. Phân quyền giúp tăng cường tính minh bạch, bảo mật và niềm tin trong mạng blockchain, cũng như khuyến khích sự hợp tác và đổi mới. Một số loại phân quyền trong blockchain là phân quyền theo chiều ngang (horizontal decentralization), phân quyền theo chiều dọc (vertical decentralization) và phân quyền theo lớp (layered decentralization)

#### **3.1.2 Quyền riêng tư trong blockchain**



–Quyền riêng tư trong blockchain đề cập đến việc bảo vệ danh tính và thông tin nhạy cảm của người dùng trên mạng blockchain khỏi bị tiết lộ hoặc lạm dụng bởi các bên không mong muốn. Để đạt được điều này, blockchain sử dụng nhiều kỹ thuật ẩn danh, khử nhận dạng và mã hóa để bảo vệ quyền riêng tư của người dùng. Một số ví dụ về các kỹ thuật quyền riêng tư trong blockchain là:

- + Ẩn danh: Ẩn danh là quá trình che giấu danh tính thực của người dùng trên mạng blockchain bằng cách sử dụng các định danh ngẫu nhiên hoặc mã hóa. Ẩn danh giúp người dùng tránh bị theo dõi, phân tích hoặc xâm phạm bởi các bên có hại. Một số loại tiền mã hóa ẩn danh phổ biến trong blockchain là Monero, Zcash và Dash.

- + Khử nhận dạng: Khử nhận dạng là quá trình biến đổi dữ liệu nhạy cảm của người dùng trên mạng blockchain bằng cách sử dụng các kỹ thuật như làm mờ, thay thế hoặc tổng hợp. Khử nhận dạng giúp người dùng bảo vệ quyền riêng tư của họ khi chia sẻ dữ liệu với các bên khác, cũng như tuân thủ các quy định về bảo mật dữ liệu. Một số phương pháp khử nhận dạng phổ biến trong blockchain là khử nhận dạng k (k-anonymity), khử nhận dạng l (l-diversity) và khử nhận dạng t (t-closeness).

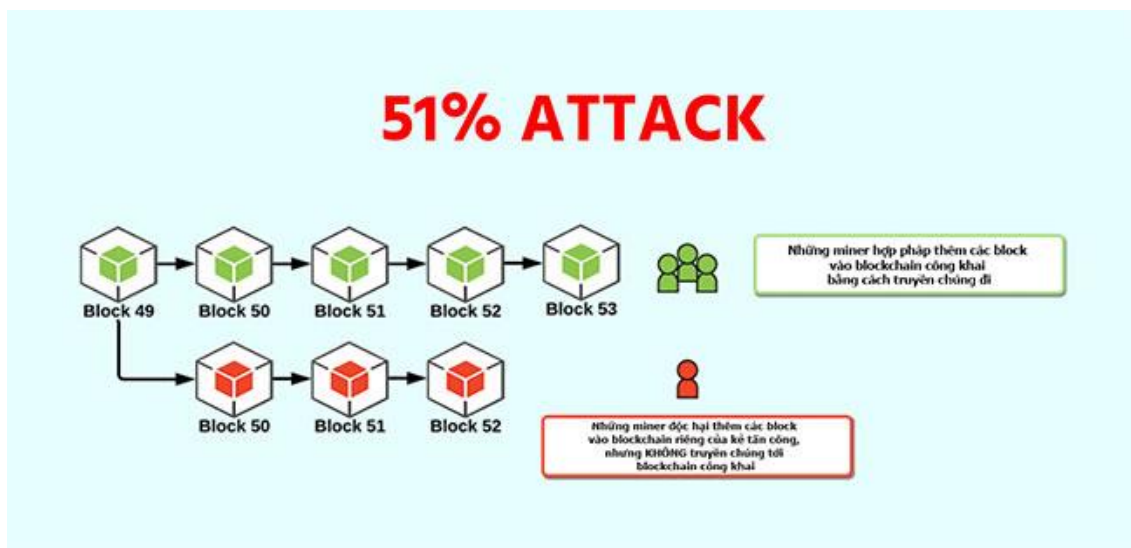
- + Mã hóa: Mã hóa cũng là một kỹ thuật quan trọng để bảo vệ quyền riêng tư của người dùng trên mạng blockchain, bằng cách mã hóa dữ liệu trước khi gửi hoặc lưu trữ trên blockchain. Mã hóa giúp người dùng bảo vệ dữ liệu của họ khỏi bị đọc hoặc thay đổi bởi những người không có khóa bí mật. Một số loại mã hóa quyền riêng tư phổ biến trong blockchain là mã hóa đồng thuận (homomorphic encryption), mã hóa đa bên (multi-party encryption) và mã hóa không đối xứng (asymmetric encryption).

### **3.1.3 Các mối đe dọa liên quan đến an toàn và quyền riêng tư trong blockchain**

Blockchain là một công nghệ cho phép lưu trữ và truyền tải dữ liệu một cách an toàn, minh bạch và hiệu quả. Tuy nhiên, blockchain vẫn có thể gặp phải các mối đe dọa an ninh mạng. Dưới đây là một số mối đe dọa an ninh mạng trong blockchain:

#### **3.1.3.1 Tấn công 51%:**

Cuộc tấn công 51% là khi một người khai thác tiền điện tử hoặc một nhóm người khai thác giành quyền kiểm soát hơn 50% blockchain của mạng. Các cuộc tấn công như vậy là một trong những mối đe dọa đáng kể nhất đối với những người sử dụng và mua tiền điện tử. Lo ngại hơn là các giao dịch có thể bị đảo ngược khi nhóm đối tượng này cố gắng kiểm soát toàn bộ mạng lưới.



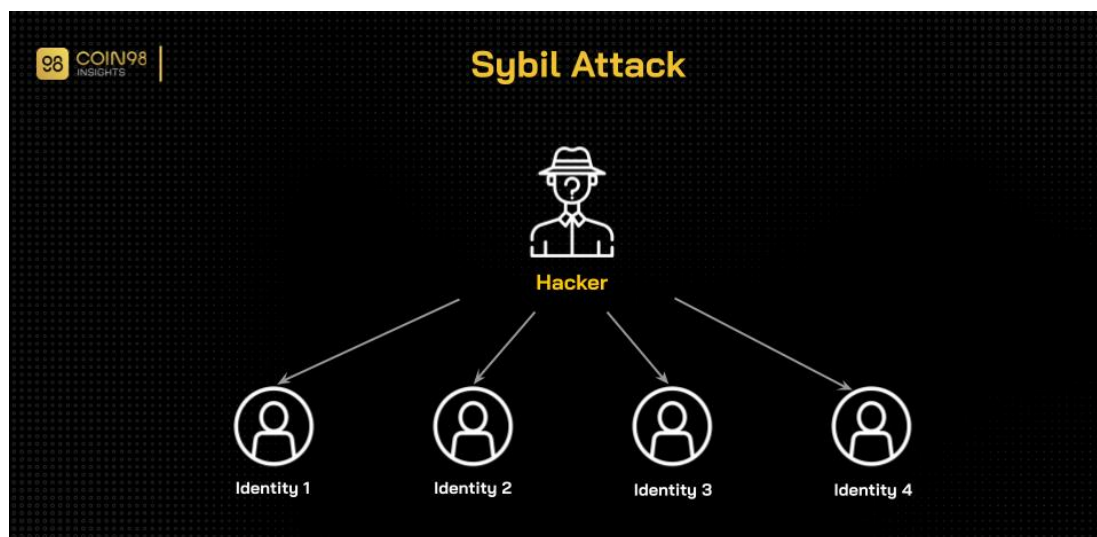
Hình 3.1 Hình ảnh minh họa tấn công 51%

Để ngăn chặn tấn công 51%, cần tăng cường sức mạnh tính toán của mạng blockchain. Điều này có thể được thực hiện bằng cách thu hút nhiều người tham gia vào mạng lưới hoặc sử dụng các cơ chế đồng thuận mới, chẳng hạn như proof-of-stake.

### 3.1.3.2 Tấn công Sybil:

Sybil Attack (hay còn gọi là tấn công mạo nhận) là hình thức tấn công vào các mạng lưới ngang hàng (peer network) được thực hiện bằng cách tạo nhiều thực thể ảo (tài khoản, node hoặc máy tính) để chiếm quyền kiểm soát mạng lưới.

Sybil Attack là một trong những hình thức tấn công mạng lưới phổ biến, có thể được thực hiện bởi bất kỳ ai. Đây đã trở thành một trong những vấn đề bức bối trong lĩnh vực khoa học máy tính, đến nay vẫn chưa có biện pháp bảo vệ tuyệt đối trước hình thức tấn công này.



Hình 3.2 Hình ảnh minh họa tấn công Sybil Attack

Một trong những cách để các mạng blockchain ngăn ngừa tấn công mạo nhận là sử dụng cơ chế đồng thuận như Proof of Stake. Cơ chế này yêu cầu node/validator stake một khoản token để tham gia vận hành mạng lưới. Nếu validator đó có hành vi gian lận, số token đó sẽ bị tịch thu. Do đó, tổng chi phí để thực hiện tấn công sẽ vượt xa phần thưởng nếu thành công.

### **3.1.3.3 Tấn công Eclipse:**

Là một loại tấn công trong đó một bên tấn công kiểm soát lưu lượng truy cập đến một node blockchain. Điều này cho phép bên tấn công chặn các giao dịch hợp pháp và chỉ cho phép các giao dịch của mình được thực hiện.

Để ngăn chặn tấn công eclipse, cần sử dụng các giao thức truyền thông an toàn. Các giao thức này có thể giúp đảm bảo rằng các node blockchain chỉ nhận được lưu lượng truy cập từ các nguồn đáng tin cậy.

### **3.1.3.4 Tấn công Replay:**

Đây là loại tấn công mà một kẻ tấn công sao chép một giao dịch đã được xác nhận trên một blockchain và gửi lại nó trên một blockchain khác có cùng định dạng. Điều này có thể gây ra sự trùng lặp hoặc mâu thuẫn của các giao dịch và làm mất cân bằng của các tài khoản.

### **3.1.3.5 Tấn công Phishing:**

Đây là loại tấn công mà một kẻ tấn công lừa đảo người dùng blockchain bằng cách gửi cho họ các email, tin nhắn hoặc trang web giả mạo để đánh cắp thông tin cá nhân hoặc tài sản của họ. Điều này có thể làm mất quyền truy cập hoặc tiền của người dùng trên blockchain.

Blockchain là một mạng lưới phi tập trung, vì vậy tất cả các giao dịch đều được công khai trên mạng lưới. Điều này có thể gây ra vấn đề về quyền riêng tư cho người dùng, chẳng hạn như: Tấn công theo dõi giao dịch, cụ thể kẻ tấn công có thể theo dõi các giao dịch của một người dùng để thu thập thông tin về hoạt động tài chính của họ. Hay tấn công xác định danh tính: Kẻ tấn công có thể sử dụng các kỹ thuật phân tích dữ liệu để xác định danh tính của một người dùng dựa trên các giao dịch của họ...

## **3.2 Một số vụ tấn công blockchain trong thực tế**

### **3.2.1 Một số vụ tấn công vào hệ thống blockchain ở nước ngoài**

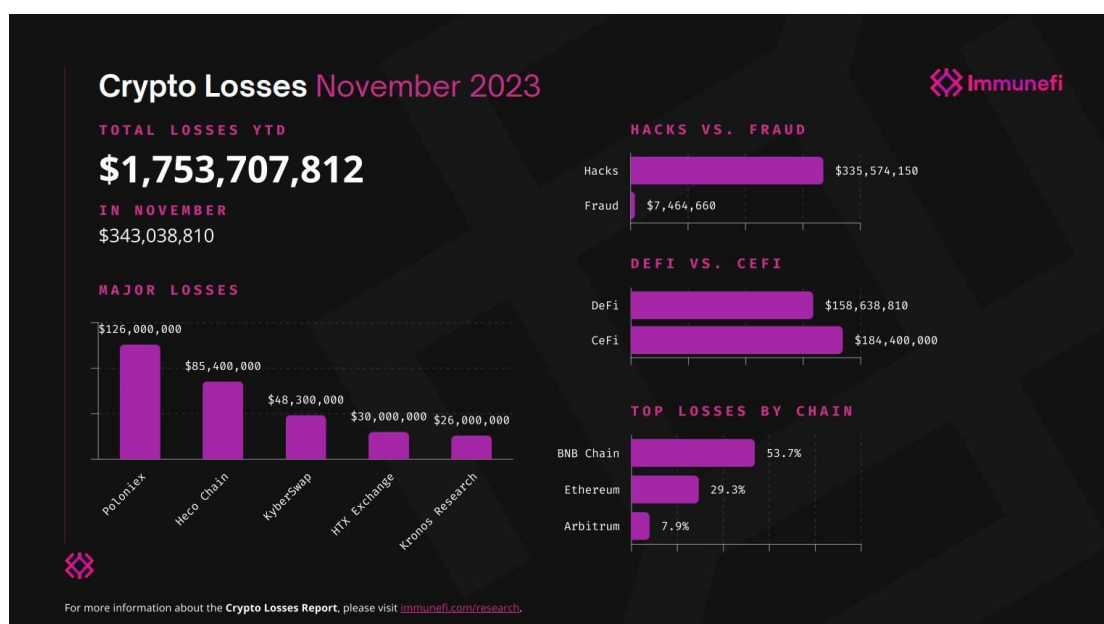
Tháng 11 năm 2023 đã trở thành thời điểm mất mát nhất của ngành tiền mã hóa trong năm qua, với con số thiệt hại lên đến hơn 340 triệu USD.

Từ đầu năm đến nay đã có tổng cộng trên 295 vụ tấn công và rug pull, bòn rút hơn 1,75 tỷ USD của thị trường crypto. Đáng chú ý, số thất thoát trong tháng qua tăng đột biến gấp 15 lần so với con số 22 triệu USD của tháng trước.



Hình 3.3 Thống kê thiệt hại tấn công từ đầu năm đến nay. Nguồn: Immunefi

Theo thống kê của Immunefi, các vụ tấn công trong tháng 11/2023 đã lấy đi của ngành tiền mã hóa hơn 340 triệu USD.



Hình 3.4 Thống kê thiệt hại từ các vụ hack crypto trong tháng 10/2023. Nguồn: Immunefi

Trong tháng 10/2023, các nền tảng tài chính tập trung (CeFi) là “con mồi” ưa thích nhất của giới hacker, chiếm hơn 53% tổng thiệt hại (khoảng 184 triệu USD) chỉ với 4 vụ tấn công. Dẫn đầu danh sách này là Poloniex (125 triệu USD), HTX (86 triệu USD) và Kronos Research (25 triệu USD).

Bên cạnh đó còn các vụ tấn công lớn nhỏ khác, bao gồm:

- + 01/11/2023: Frax Finance bị tấn công DNS;
- + 05/11/2023: Bitfinex bị tấn công "quy mô nhỏ", tài sản người dùng không bị ảnh hưởng;
- + 11/11/2023: Raft bị hack mất 3,3 triệu USD, stablecoin R depeg nghiêm trọng;
- + 17/11/2023: Stars Arena bị hack lần 2;
- + 18/11/2023: Sàn DEX Trader Joe và SpookySwap bị tấn công front-end;
- + 29/11/2023: Velodrome và Aerodrome bị tấn công front-end.
- + BNB Chain và Ethereum là nơi “đón tiếp” hacker nhiều nhất trong tháng 11, chịu 83% thiệt hại.

### **3.2.2 Một số vụ tấn công vào hệ thống blockchain ở Việt Nam**

Trích từ VietNamPlus bài đăng vào ngày 29/11/2023 16:43 cũng như một số trang báo và diễn đàn uy tín khác cũng đã đưa tin về các vụ tấn công blockchain ở Việt Nam:

- + Cuối tháng 3/2020, một mạng blockchain của Việt Nam là Sky Mavis đã bị tấn công, thiệt hại 600 triệu USD. Cointelegraph đánh giá đây là vụ hack lớn nhất lịch sử DeFi lúc bấy giờ. Sau đó, đội ngũ phát triển Sky Mavis đã huy động vốn và cam kết hoàn trả cho những người dùng bị mất tiền sau vụ tấn công.

- + Vụ tấn công Kyber Elastic diễn ra hôm 23/11/2023 của hacker đã lấy đi số tài sản mã hóa (Ethereum, Arbitrum, Optimism, Polygon và Base) trị giá hơn 47 triệu USD (khoảng 1.140 tỉ đồng) và tất cả được gửi vào địa chỉ ví duy nhất.

Được biết, KyberSwap Elastic là một trong những nền tảng tài chính phi tập trung dựa trên công nghệ Blockchain của Việt Nam, từng nhận được sự chú ý lớn trên cộng đồng quốc tế. Nền tảng này được phát triển bởi Kyber Network, start-up thành công nhất Việt Nam năm 2017 khi từng gọi vốn được 52 triệu USD dưới hình thức ICO. Trong nhiều năm qua, Kyber Network được biết đến như là start-up đi đầu về mảng Blockchain tại Việt Nam. Hai nhà sáng lập Lưu Thế Lợi và Trần Huy Vũ của startup này cũng từng lọt top Forbes 30 Under 30 châu Á năm 2018.

Kể thực hiện vụ tấn công đã có nhiều email nặc danh gửi đến đội ngũ phát triển Kyber Network khiến quá trình thu hồi tiền càng trở nên khó khăn hơn. Đại diện Kyber cho biết sẽ phối hợp với cơ quan an ninh mạng sau khi thương lượng bất thành với hacker để lấy lại 47 triệu USD bị đánh cắp.

Chia sẻ với sự cố nghiêm trọng của Kyber Elastic, ông Nguyễn Duy Lâm, chuyên gia an ninh mạng VBA, Đồng sáng lập Công ty bảo mật Veramine (Mỹ) cho biết “Vụ tấn công lần này cho thấy ngay cả khi dự án dù được audit (kiểm toán) cũng vẫn cần có những chính sách quản lý chặt chẽ hơn đối với các vùng code quan trọng hoặc phản biện mang tính quản lý tài chính truyền thống”.

Đồng quan điểm, ông Nguyễn Thanh Sơn - Phó Chủ tịch Công ty ABN châu Âu, chuyên gia công nghệ VBA, cho rằng, sự việc của Kyber Elastic nên được coi như một lời cảnh báo cho các dự án tương tự trong thế giới tài chính phi tập trung DeFi.

“Các dự án khác cần xem xét kỹ lưỡng vấn đề bảo mật và phương án bảo hiểm nhằm bảo vệ tài sản của người tham gia đầu tư, cung cấp thanh khoản và giao dịch trên các nền tảng web3. Không nên nghĩ DeFi chỉ là thế giới công nghệ khi nó chịu trách nhiệm như một hệ thống tài chính.”

### **3.2.3 Đánh giá**

Từ những vụ tấn công trên ta thấy được mức độ nguy hiểm cũng như thiệt hại mà những vụ tấn công đem lại là vô cùng lớn. Điều này càng cho thấy việc đảm bảo an toàn trên các giao dịch blockchain là cực kỳ quan trọng. Bởi lẽ đây là một nền tảng với những ưu điểm đáng kể và đang thu hút nhiều người tham gia, do đó cần có những giải pháp tốt nhất để đảm bảo an toàn cho cả hệ thống nói chung và người tham gia nói riêng.

## **CHƯƠNG 4. NGHIÊN CỨU CÁC GIẢI PHÁP ĐỂ ĐẢM BẢO AN TOÀN VÀ QUYỀN RIÊNG TƯ TRONG CÁC GIAO DỊCH BLOCKCHAIN**

### **4.1 Các giải pháp đảm bảo an toàn và quyền riêng tư trong các giao dịch blockchain**

Blockchain là một công nghệ phân tán, không cần có trung gian, có thể được sử dụng để lưu trữ và bảo mật dữ liệu một cách an toàn và đáng tin cậy. Tuy nhiên, blockchain cũng có một số hạn chế về mặt bảo mật và quyền riêng tư, chẳng hạn như:

– Tính minh bạch: Mọi giao dịch trên blockchain đều được công khai, vì vậy tất cả mọi người đều có thể truy cập và xem thông tin về các giao dịch đó. Điều này có thể dẫn đến việc lộ thông tin cá nhân hoặc nhạy cảm.

– Tính dễ bị tấn công: Các blockchain có thể bị tấn công bởi các hacker, dẫn đến việc thay đổi hoặc xóa thông tin trên blockchain. Để đảm bảo an toàn và quyền riêng tư trong các giao dịch blockchain, cần có các giải pháp phù hợp.

#### **4.1.1 Mã hóa dữ liệu**

Sử dụng mã hóa là một giải pháp quan trọng để bảo vệ dữ liệu trong các giao dịch blockchain. Mã hóa dữ liệu giúp bảo vệ dữ liệu khỏi những kẻ tấn công bằng cách biến dữ liệu thành một chuỗi ký tự không thể đọc được. Trong các giao dịch blockchain, dữ liệu giao dịch được mã hóa trước khi được lưu trữ trên blockchain. Điều này giúp ngăn chặn tin tặc truy cập và đọc dữ liệu.

#### **4.1.2 Hashing**

Blockchains phụ thuộc rất nhiều vào mã hóa để đạt được bảo mật dữ liệu. Một chức năng mã hóa cực kỳ quan trọng trong bối cảnh này chính là hashing (băm). Hashing là một quá trình trong đó một thuật toán được gọi là hàm hash nhận đầu vào dữ liệu (có kích thước bất kỳ) và trả về một đầu ra xác định có giá trị độ dài cố định.

Bất kể kích thước đầu vào, độ dài đầu ra sẽ luôn luôn cố định. Các đầu vào khác nhau sẽ dẫn đến các đầu ra khác nhau. Nếu đầu vào không thay đổi, kết quả hash sẽ luôn giống nhau - bất kể bạn chạy hàm hash bao nhiêu lần.

Trong blockchain, các giá trị đầu ra này, được gọi là các hash, được sử dụng làm định danh duy nhất cho các khối dữ liệu. Hash của mỗi khối được tạo ra liên quan đến hash của khối trước đó, và đó là thứ giúp liên kết các khối lại với nhau, tạo thành một chuỗi các khối. Hơn nữa, hàm hash khối phụ thuộc vào dữ liệu chứa trong khối đó, có

nghĩa là bất kỳ thay đổi nào đối với dữ liệu sẽ yêu cầu sự thay đổi đối với hàm hash khối.

Do đó, hash của mỗi khối được tạo ra dựa trên cả dữ liệu chứa trong khối đó và hash của khối trước đó. Các định danh hash này đóng vai trò chính trong việc đảm bảo tính bảo mật và tính bất biến của blockchain.

Hashing cũng được tận dụng trong các thuật toán đồng thuận để xác nhận các giao dịch. Ví dụ, trên blockchain Bitcoin, thuật toán Proof of Work (PoW) được sử dụng để đạt được sự đồng thuận và để đào các coin mới sử dụng hàm hash có tên là SHA-256. Đúng như tên gọi, SHA-256 nhận dữ liệu đầu vào và trả về một hash dài 256 bit hoặc 64 ký tự.



Hình 4.1 Hashing là hình thức mã hoá một chiều

### 4.1.3 Cryptography (mật mã học)

#### 4.1.3.1 Giới thiệu về Cryptography

Cryptography (mật mã học) là giải pháp bảo mật dữ liệu và thông tin giao dịch của người gửi, thông qua việc biến đổi chúng thành những đoạn mật mã, mà chỉ những người được uỷ quyền (gồm người nhận và người gửi) mới có khả năng xử lý và tiếp cận thông tin.

Đối với blockchain, cryptography bảo vệ dữ liệu, thông tin của tất cả giao dịch trong mạng lưới, bao gồm: giao dịch giữa người dùng, node hay thậm chí giữa các block với nhau. Nhằm mục đích duy trì tính minh bạch và độ tin cậy của dữ liệu trên mạng lưới, và ngăn ngừa vấn đề liên quan tới double spending.



Thông thường, quá trình cryptography có hai giai đoạn đó là:

–**Mã hoá (encrypt):** Quá trình chuyển đổi thông tin và dữ liệu thành những đoạn mật mã không có ý nghĩa.

–**Giải mã (decrypt):** Quá trình chuyển đổi những đoạn mật mã thành thông tin và dữ liệu dễ hiểu và dễ đọc cho người được uỷ quyền.

#### 4.1.3.2 Nguồn gốc của Cryptography

Mặc dù vẫn từ “crypto” xuất hiện trong cryptography, phương pháp bảo mật này đã tồn tại hàng ngàn năm về trước. Cryptography lần đầu xuất hiện vào năm 1900 trước Công Nguyên dưới dạng chữ tượng hình trên một ngôi mộ tại Ai Cập. Và thuật ngữ cryptography bắt đầu từ tiếng Hy Lạp cổ, khi được ghép bởi hai từ là “kryptos” (ẩn giấu) và “graphein” (viết/vẽ).

Vào năm 40 trước Công Nguyên, Julius Caesar - hoàng đế La Mã, đã sử dụng một mật mã riêng để thay đổi các ký tự trên bức thư của ông, để phòng các nội dung của bức thư rơi vào tay kẻ thù. Cách giải mã hiển nhiên chỉ có Julius và những cận thần xung quanh ông biết.

Và cho đến thời đại công nghệ lên ngôi, mục đích của cryptography cũng tương tự như cách của Julius Caesar. Đó là khiến nội dung, thông tin nội bộ trở thành những đoạn mã không thể đọc được bởi người ngoài.

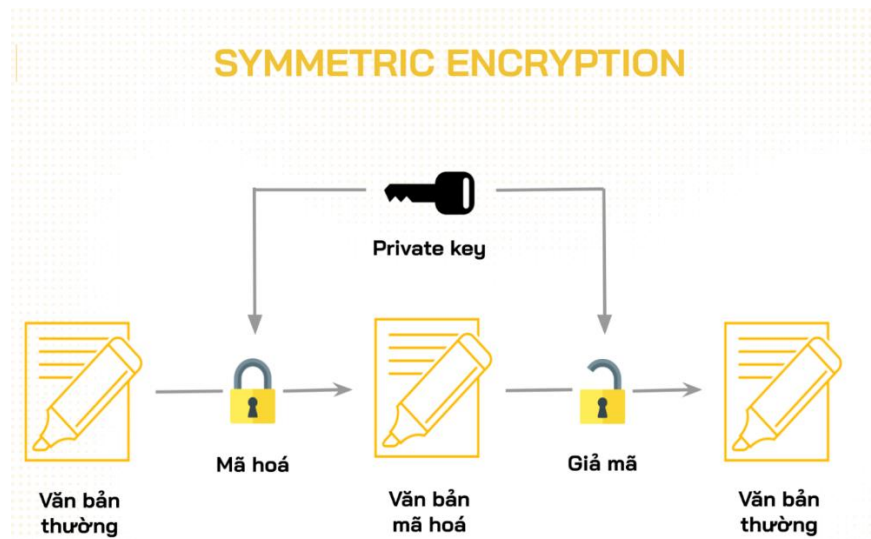
#### 4.1.3.3 Các loại Cryptography trong Blockchain

–Cryptography trong blockchain được chia làm hai loại chính: Symmetric encryption (mã hoá đối xứng), Asymmetric encryption (mã hoá bất đối xứng)

##### –Symmetric encryption

Symmetric encryption (mã hoá đối xứng) là loại bảo mật mà người dùng có thể sử dụng một chìa khoá (key) giống nhau, để mã hoá và giải mã. Vì vậy, với tính chất sử dụng cùng một chìa cho hai việc, nên symmetric là phương thức bảo mật được sử dụng ở những tình huống thuộc nội bộ hoặc cần sự riêng tư.

Trong thị trường crypto, chìa khoá để giải mã và mã hoá cùng lúc là private key. Thông thường, người dùng sử dụng private key để lưu trữ những thông tin bảo mật, mã hoá mật khẩu... Và nếu muốn giải mã, họ sẽ sử dụng lại private key đó.



Hình 4.2 Symmetric encryption là loại hình vừa mã hoá và giải mã chỉ bằng 1 key.

#### –Asymmetric encryption (mã hoá bất đối xứng)

Asymmetric encryption (mã hoá bất đối xứng) là loại bảo mật sử dụng hai chìa khoá cho việc mã hoá và giải mã, trái ngược với symmetric encryption. Vì sử dụng hai loại chìa khoá khác nhau, nên độ bảo mật của asymmetric cao hơn so với symmetric.

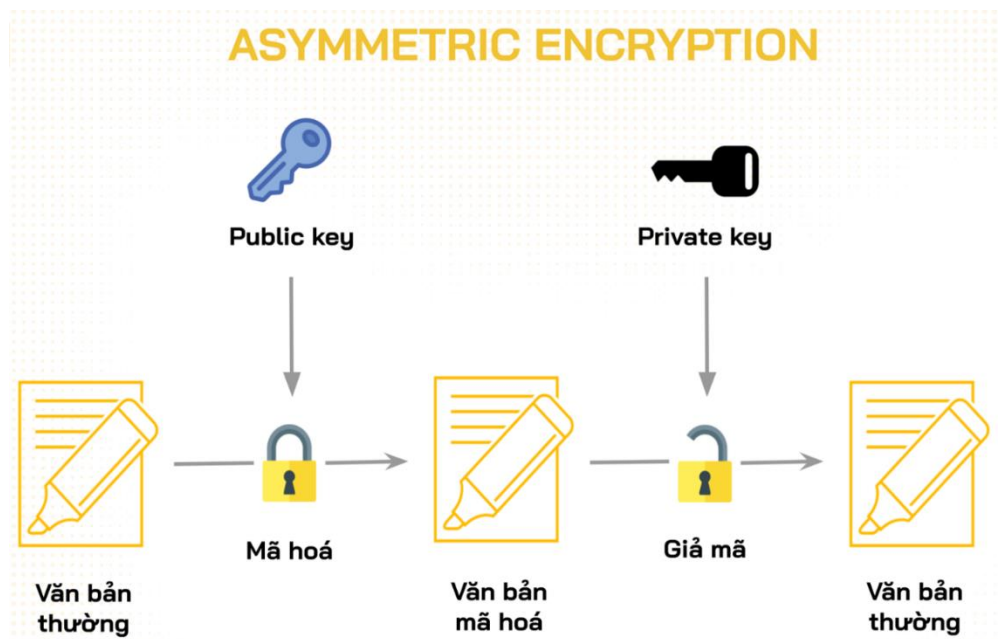
Tại thị trường crypto, hai chìa khoá ở đây là public key và private key, trong đó:

–Public key: Loại chìa khoá được sử dụng để mã hoá tin nhắn, và tất cả mọi người đều có quyền tiếp cận public key.

–Private key: Loại chìa khoá được sử dụng để giải mã tin nhắn, và chỉ những cá nhân được uỷ quyền mới có thể tiếp cận.

Có thể hiểu điều trên qua ví dụ sau:

A gửi một thông điệp đến B và đảm bảo rằng chỉ có B mới có thể hiểu được thông điệp đó, A có thể mã hóa thông điệp bằng khóa public key sao cho chỉ B mới có thể giải mã thông điệp bằng private key của B. Tưởng tượng rằng hòm thư của B, nơi mà tất cả mọi người (bao gồm A) có thể bỏ thư vào hòm. Và B là người duy nhất có quyền mở hòm thư và đọc.



Hình 4.3 Asymmetric encryption là loại hình sử dụng hai loại chìa khoá cho việc mã hoá và giải mã

#### 4.1.3.4 Ứng dụng của cryptography trong blockchain

##### – Ví blockchain

Ví blockchain (wallet) là phần mềm hoặc phần cứng có khả năng lưu trữ thông tin giao dịch và thông tin cá nhân của người dùng. Nhiều người lầm tưởng wallet chứa đựng tài sản của bạn, thực tế wallet chỉ chứa private key để người dùng giải mã và truy cập vào tài sản mà họ sở hữu trên blockchain.

Ngoài ra, wallet còn đóng vai trò là công cụ giao tiếp giữa người dùng với nhau và hỗ trợ họ thực hiện các giao dịch.

Đầu tiên, wallet A tạo một public key để mã hoá các thông tin của giao dịch như tài sản crypto, tin nhắn... và gửi đoạn mã hoá đến wallet B. Sau đó, wallet B sẽ sử dụng private key để có quyền tiếp cận, giải mã những thông tin về tài sản, tin nhắn... mà wallet A gửi đến.

##### – Chữ ký số (digital signature)

Chữ ký số (digital signature) là bằng chứng mà người gửi sử dụng để xác minh tính đúng đắn trong giao dịch của họ. Để dễ hình dung, người dùng khi thực hiện một giao dịch trên ngân hàng, họ phải có mật khẩu và mã OTP, đây được cho là bằng chứng cho việc bạn đang xác thực giao dịch này là của mình.

Digital signature dựa vào cơ chế symmetric encryption, khi người dùng tạo digital signature bằng việc sử dụng private key để mã hoá chữ ký của bản thân.

Đối với những giao dịch được xác thực và mã hoá bởi digital signature, thì chỉ có public key được uỷ quyền hoặc private key của người gửi mới có thể giải mã.

#### **4.1.3.5 Ưu nhược điểm của cryptography**

##### **Ưu điểm**

–Độ bảo mật cao: Cryptography cho phép mã hoá mọi giao dịch trên blockchain, từ đó nâng cao tính bảo mật của mạng lưới, đồng thời bảo toàn tính trọn vẹn của các dữ liệu.

–Khả năng mở rộng: Cryptography đảm bảo dữ liệu của mọi giao dịch không thể bị tiếp cận bởi những bên thứ ba. Từ đó, khiến mạng lưới có khả năng chạy nhiều giao dịch hơn mà không sợ việc dữ liệu bị thay đổi.

–Không thể thay đổi: Chữ ký số khiến các bên thứ ba không có quyền can thiệp hoặc sửa đổi. Nếu như xảy ra trường hợp bị can thiệp, chữ ký số sẽ không thể hợp lệ. Vì vậy, cryptography có thể bảo vệ dữ liệu khỏi sự can thiệp, và khiến tốc độ giao dịch diễn ra mượt mà hơn.

##### **Nhược điểm**

–Không thể hỗ trợ độ bảo mật cho cơ sở hạ tầng: Nếu như có những cuộc tấn công do lỗi nằm trong thiết kế cấu trúc hay lỗi đến từ cơ sở hạ tầng, cryptography gần như không có khả năng bảo vệ. Ví dụ, nếu một blockchain bị tấn công 51%, kẻ tấn công có khả năng thay đổi lịch sử giao dịch và mạng lưới sẽ bị double spending. Trong khi mục đích của cryptography là bảo vệ tính toàn vẹn của dữ liệu giao dịch.

–Cần nhiều tài nguyên: Cơ sở hạ tầng và tài nguyên để xây dựng cryptography cho mạng lưới cần nhiều sự đầu tư, từ tiền bạc cho tới con người (cryptography yêu cầu trình độ kỹ thuật cao). Ngoài ra, việc mã hoá và giải mã có thể tiêu tốn nhiều thời gian của mạng lưới, nếu dữ liệu và thông tin giao dịch lớn.

#### **4.1.4 Cơ chế đồng thuận:**

##### **4.1.4.1 Tổng quan về cơ chế đồng thuận trong blockchain**

–Cơ chế đồng thuận trong blockchain là một quy tắc hoặc cơ chế để các node tuân theo, nhằm đảm bảo các giao dịch được thực hiện trên blockchain là chính xác, minh bạch và không thể thay đổi.

–Trong một hệ thống blockchain, tất cả các node đều được kết nối với nhau thông qua mạng lưới ngang hàng. Các node này liên tục trao đổi dữ liệu mới nhất để tất cả các node luôn được cập nhật về trạng thái của blockchain.

–Để thêm một giao dịch mới vào blockchain, một node cần phải chứng minh rằng giao dịch đó là hợp lệ. Cơ chế đồng thuận là cách mà các node xác định xem một giao dịch có hợp lệ hay không. Cơ chế đồng thuận là một thành phần quan trọng của blockchain. Nó giúp đảm bảo rằng blockchain hoạt động một cách an toàn và hiệu quả.

Khi nhắc đến cơ chế đồng thuận (consensus mechanism) trong các hệ thống phân tán và mạng blockchain, có một số thuật ngữ quan trọng cần biết, bao gồm:

- + Khối (Block): Một đơn vị cơ bản của dữ liệu trong blockchain. Mỗi khối bao gồm một số lượng giao dịch và một mã hash đại diện cho khối đó.

- + Mã hash (Hash): Một chuỗi ký tự duy nhất, được tạo ra bằng cách sử dụng một thuật toán mã hóa. Mã hash được sử dụng để đại diện cho một khối hoặc một giao dịch cụ thể trong blockchain.

- + Node: Một thực thể trong mạng blockchain, có nhiệm vụ xác nhận các giao dịch và thêm các khối mới vào blockchain.

- + Proof of Work (PoW): Một cơ chế đồng thuận trong blockchain, nơi các nodes trong mạng cạnh tranh để giải quyết các bài toán tính toán phức tạp để thêm khối mới vào blockchain.

- + Proof of Stake (PoS): Một cơ chế đồng thuận khác trong blockchain, nơi sự đồng thuận được đạt được bằng cách các nodes sở hữu token hoặc đồng tiền ảo để cạnh tranh giải quyết các nhiệm vụ trong mạng.

- + Delegated Proof of Stake (DPoS): Một biến thể của PoS, trong đó sự đồng thuận được đạt được thông qua một nhóm các nodes được bầu chọn để giải quyết các nhiệm vụ và đóng vai trò quản lý blockchain.

- + Practical Byzantine Fault Tolerance (PBFT): Một cơ chế đồng thuận khác trong blockchain, nhằm đảm bảo tính toàn vẹn và độ tin cậy của các thông tin trao đổi giữa các nodes.

- + Fork: Sự tách khỏi của blockchain, khi một số nodes trong mạng không đồng ý với một số quyết định của blockchain và tạo ra một phiên bản khác của blockchain.

- + Consensus Algorithm: Một thuật toán được sử dụng trong cơ chế đồng thuận để giải quyết các vấn đề liên quan đến việc đạt được sự đồng thuận trong hệ thống phân tán và blockchain.

#### **4.1.4.2 Tầm quan trọng của thuật toán đồng thuận đối với Blockchain**

–Các blockchain cần thuật toán đồng thuận bởi vì đây chính là cơ chế tạo dựng và duy trì sự phi tập trung ngang hàng của mạng lưới. Thay vì một vài cá nhân hay tổ chức kiểm soát toàn bộ hệ thống, blockchain cho phép ai cũng có thể tham gia mạng lưới bằng cách trở thành một node.

–Cơ chế đồng thuận cũng là lớp bảo vệ vững chắc của blockchain khỏi việc thay đổi dữ liệu cũng như chống lại các giao dịch gian lận của hacker, nhờ có cơ chế đồng thuận, một giao dịch sẽ luôn được xác thực bởi các node trong mạng lưới một cách ngang hàng.

–Nếu các cơ chế đồng thuận luôn ổn định, vững chắc và an toàn, sẽ không có một bên nào có thể khai thác hay tấn công vào blockchain. Càng có nhiều node/validator, blockchain đó càng trở nên bảo mật và phi tập trung. Điều này đồng nghĩa với việc Bitcoin và Ethereum là 2 blockchain an toàn nhất cho tới hiện tại.

Bên cạnh đó cơ chế đồng thuận còn giải quyết các vấn đề như:

–Tính toàn vẹn dữ liệu: Các nodes trong mạng cần đồng ý với các giao dịch và khối được thêm vào blockchain, và không có giao dịch nào bị thay đổi hoặc xóa bỏ. Cơ chế đồng thuận giúp đảm bảo tính toàn vẹn dữ liệu trên blockchain.

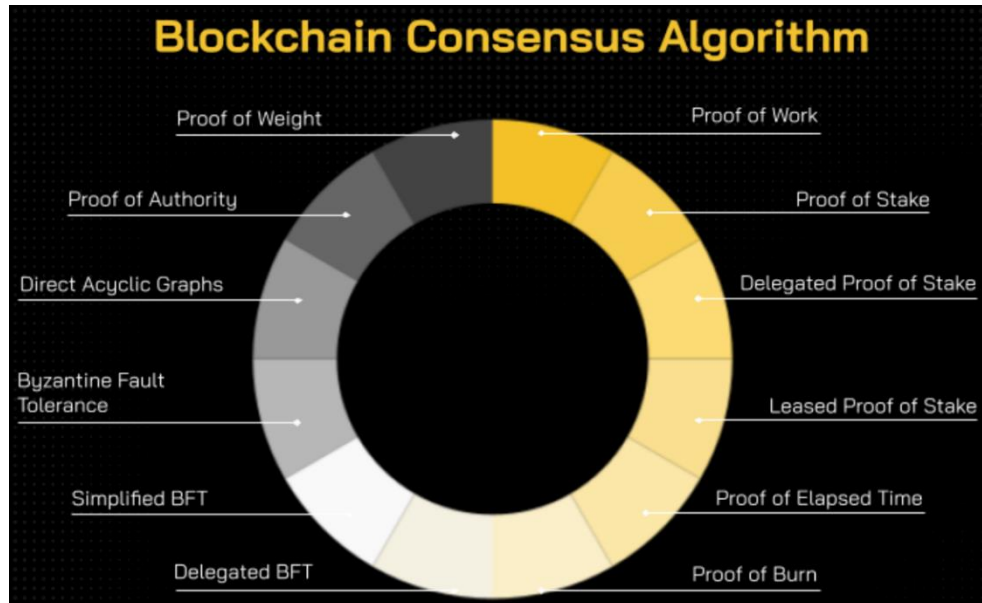
–Tránh gian lận và tấn công: Các kẻ tấn công có thể cố gắng thay đổi hoặc xóa các giao dịch trên blockchain để lợi dụng hệ thống. Cơ chế đồng thuận giúp đảm bảo rằng các giao dịch chỉ được thêm vào blockchain sau khi được xác thực bởi nhiều nodes khác nhau, từ đó giảm thiểu nguy cơ tấn công.

–Đảm bảo sự đồng bộ giữa các nodes trong mạng: Các nodes trong mạng blockchain có thể hoạt động không đồng bộ và chậm chạp. Cơ chế đồng thuận giúp đảm bảo rằng tất cả các nodes trong mạng đồng bộ với nhau về các khối mới nhất được thêm vào blockchain.

–Giải quyết các xung đột trong dữ liệu: Khi hai nodes cùng thêm một khối mới vào blockchain, xảy ra xung đột dữ liệu. Cơ chế đồng thuận giúp giải quyết các xung đột này bằng cách xác định khối nào sẽ được chấp nhận và khối nào sẽ bị loại bỏ.

Vì vậy, consensus mechanism đóng một vai trò quan trọng trong việc đảm bảo tính toàn vẹn và độ tin cậy của các dữ liệu trong hệ thống phân tán và blockchain.

#### **4.1.4.3 Các cơ chế đồng thuận phổ biến**

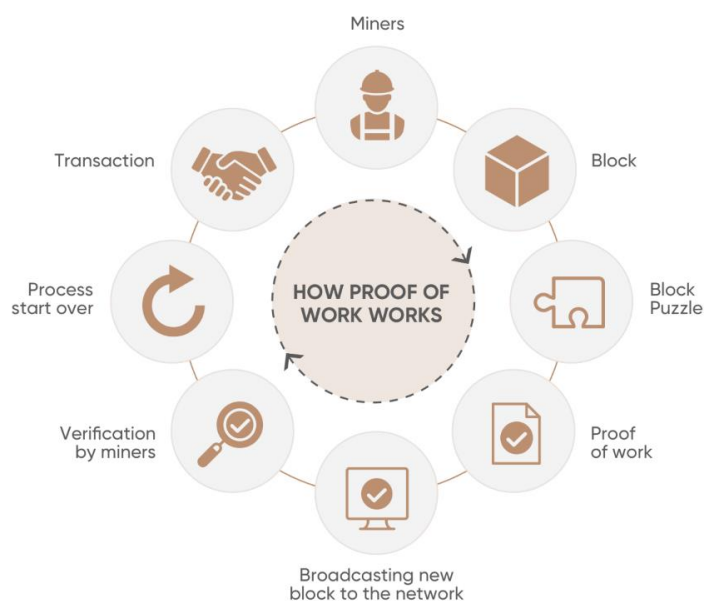


Hình 4.4 Hình ảnh tổng hợp các loại thuật toán blockchain

#### 4.1.4.3.1 Proof of Work (PoW)

Proof of Work (PoW) hay bằng chứng công việc là thuật toán đồng thuận blockchain ra đời đầu tiên, thuật toán này được sử dụng bởi Bitcoin - đồng tiền mã hoá đầu tiên trên thế giới.

PoW yêu cầu các node sử dụng sức mạnh máy tính để giải các bài toán tạo ra mã hash. Node đầu tiên giải bài toán, giành quyền xác thực giao dịch, sau đó sẽ được nhận phần thưởng là BTC. Quá trình này được gọi là “mining” (đào coin), trong đó các node đóng vai trò là các miners (thợ đào).



Hình 4.5 Cách hoạt động của Proof of Work

Khi một node giải bài toán và xác nhận giao dịch, giao dịch đó cũng sẽ được kiểm tra và xác nhận bởi tất cả các node khác trong mạng lưới. Nếu câu trả lời được thông qua, tất cả các node sẽ thêm giao dịch này vào blockchain, làm cho blockchain có thể dễ dàng xác minh và đồng bộ hoá.

Đây là cơ chế đồng thuận gắn liền với Bitcoin (BTC), Litecoin (LTC)...

**Ưu điểm:** Là giao thức đầu tiên, Proof-of-work (PoW) đã chứng minh khả năng phục hồi của nó trước các cuộc tấn công nội bộ và bên ngoài.

**Nhược điểm:**

–PoW sử dụng sức mạnh máy tính để bảo mật cho blockchain, do đó yêu cầu điện năng tiêu thụ lớn và chi phí đắt đỏ cho các phần cứng bắt buộc.

–Một block trên blockchain PoW cần nhiều thời gian hơn để được tạo ra và xác thực, khiến cho thuật toán này kém hiệu quả và tốn tài nguyên (thậm chí là không thân thiện với môi trường) hơn các thuật toán đồng thuận khác.

#### 4.1.4.3.2 Proof of Stake (PoS)

–Proof of Stake (PoS), hay còn gọi là bằng chứng cổ phần, là cơ chế thuật toán đồng thuận phổ biến nhất hiện nay, được giới thiệu đầu tiên bởi Peercoin vào năm 2013, được sử dụng đầu tiên bởi Ethereum. Thay vì sử dụng sức mạnh máy tính, Proof of Stake yêu cầu các node tham gia xác thực giao dịch phải đặt cược (stake) một số lượng nhất định native token của blockchain để giành quyền tham gia xác thực và tạo khối.

–Thường các blockchain sử dụng Proof of Stake sẽ yêu cầu một số lượng token tối thiểu để được tham gia làm validator.



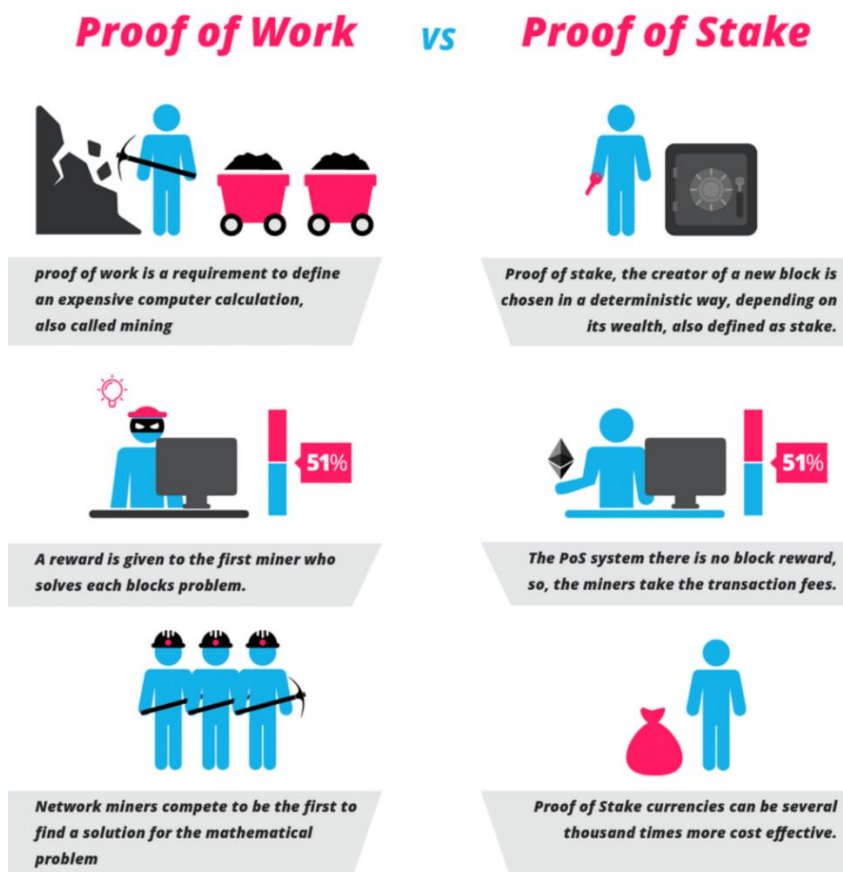
Hình 4.6 Người dùng stake coin để trở thành validator trong mạng lưới Proof of Stake



–Ví dụ, để trở thành validator của Ethereum, người dùng sẽ phải stake ít nhất 32 ETH (khoảng 33 nghìn USD tại thời điểm viết bài). Số token này được đặt cọc để đảm bảo các node hoạt động tốt, tức là nếu node đó offline quá lâu hoặc có những hành vi gian lận, số token đã stake có thể bị thu một phần hoặc mất toàn bộ tùy thuộc vào mức độ.

–Validator node trong mạng lưới Proof of Stake sẽ nhận được phí giao dịch làm phần thưởng. Khi một giao dịch giao dịch diễn ra, các validator sẽ được chọn ngẫu nhiên để xác thực giao dịch, số lượng token stake càng nhiều tỉ lệ được chọn cũng sẽ tăng tương ứng.

–Với các hoạt động trên, Proof of Stake là thuật toán tiết kiệm chi phí, thân thiện với môi trường hơn Proof of Work. Để trở thành một validator node cũng đơn giản hơn và không phải sử dụng các thiết bị phần cứng quá “khủng”.



Hình 4.7 So sánh giữa Proof of Stake và Proof of Work

### Proof of Stake

–Bằng chứng công việc là một yêu cầu để xác định một phép tính máy tính đắt tiền, còn được gọi là khai thác

–Phần thưởng sẽ được trao cho người khai thác đầu tiên giải quyết được từng vấn đề của khối.

–Những người khai thác mạng cạnh tranh để trở thành người đầu tiên tìm ra giải pháp cho vấn đề toán học

### **Proof of Work**

–Bằng chứng về cổ phần, người tạo ra khối mới được chọn theo cách xác định, tùy thuộc vào mức độ giàu có của nó, cũng được định nghĩa là cổ phần.

–Hệ thống PoS không có phần thưởng khối nên thợ đào sẽ phải chịu phí giao dịch.

–Tiền tệ bằng chứng cổ phần có thể hiệu quả hơn về mặt chi phí hàng nghìn lần.

–So sánh giữa Proof of Stake và Proof of Work

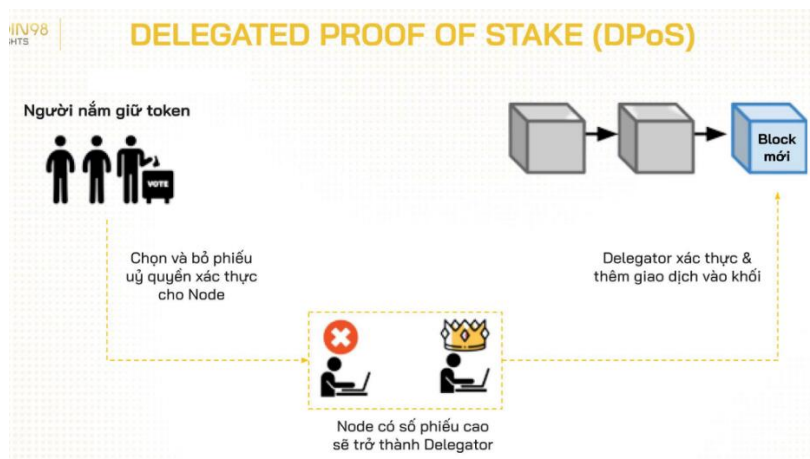
**Đánh giá:** Proof of Stake được đánh giá là ưu việt hơn Proof Of Work và đang rất thịnh hành với rất nhiều blockchain sử dụng như Cosmos (ATOM), Binance Coin (BNB), Ontology (ONT),...

#### **4.1.4.3.3 Delegated Proof of Stake (DPoS)**

Delegated Proof of Stake (DPoS) hay bằng chứng uỷ quyền cổ phần, là thuật toán đồng thuận được phát triển từ Proof of Stake.

Thay vì trở thành validator, DPoS cho phép người nắm giữ token (holder) stake token và chọn một người đại diện (delegator) để uỷ quyền xác thực giao dịch, duy trì bảo mật cho blockchain. Đổi lại, holder sẽ được chia sẻ phần thưởng từ việc gián tiếp vận hành mạng lưới.

Thông thường, delegator sẽ được chọn dựa trên danh tiếng (chứ không phải tài sản) của họ và có số lượng giới hạn khoảng 20-100 delegator trên mỗi block.



Hình 4.8 Cơ chế đồng thuận DPoS cho phép người dùng uỷ quyền cho delegator

#### **4.1.4.3.4 Proof of Authority (PoA)**

Proof of Authority (PoA) hay bằng chứng uỷ quyền là thuật toán đồng thuận dựa trên danh tiếng, phát triển dựa trên Proof of Stake.

Thay vì stake coin, validator stake “uy tín” của mình để được tham gia vào mạng lưới node xác thực giao dịch và khối của blockchain, đồng thời đóng vai trò như là những người vận hành của hệ thống.

PoA đề cao giá trị danh tính, tức là những người được chọn để trở thành validator phải thật sự đáng tin cậy. Điều này khiến cho các blockchain PoA phải đối mặt với sự đánh đổi giữa tính phi tập trung và khả năng mở rộng:

Vì tính chất chỉ lựa chọn những người uy tín và có danh tiếng, blockchain PoA thường có ít validator node, dẫn đến việc ít phi tập trung hơn so với những thuật toán đồng thuận khác.

PoA có số lượng validator giới hạn, giúp giảm thời gian xác nhận giao dịch, tăng thông lượng và khả năng mở rộng cho mạng lưới.

Nói cách khác, thuật toán đồng thuận PoA sẽ phù hợp hơn với các hệ thống tập trung.

Một số blockchain sử dụng cơ chế PoA: Vechain (VET), HECO Chain (HECO)...

#### **4.1.4.3.5 Proof of Contribution (PoC)**

Proof of Contribution (tạm dịch là bằng chứng công hiến) giám sát hành động của tất cả validator trong mạng lưới và xếp hạng các validator đó dựa theo đóng góp của họ - một cơ chế khá tương đồng với hệ thống tín dụng xã hội. Sự uy tín của một người dùng được đánh giá dựa trên số lượng token đã stake và các giao dịch trong lịch sử.

Trước khi tham gia vào mạng lưới, người dùng sẽ phải stake một khoản tiền gọi là security deposit. Sau khi hoàn thành các công việc tính toán, các node có các kết quả được xác thực sẽ được thưởng phí giao dịch và staked token từ các node không có kết quả chính xác.

Ngoài ra, còn có rất nhiều thuật toán đồng thuận khác có thể kể đến như Proof of Weight (PoWeight), Proof of Burn (PoB), Direct Acyclic Graph Tangle (DAG)... Các thuật toán blockchain này khá khó để thay đổi, do đó người ta thường nghĩ tới việc tạo ra một cơ chế mới. Những blockchain mới hơn với những cơ chế đồng thuận mới hơn sẽ đem đến sự phát triển không ngừng của blockchain trong tương lai.

#### 4.1.5 Xác thực Blockchain

##### 4.1.5.1 Xác thực Blockchain là gì?

–Blockchain là một sổ cái công khai phi tập trung kỹ thuật số được thiết kế để ghi lại mọi trao đổi dữ liệu trên mạng của nó. Do đó, để bảo mật trao đổi dữ liệu trên mạng, luồng blockchain là một quá trình xác minh người dùng bằng sổ cái phân tán và đồng thời xác minh danh tính kỹ thuật số của người dùng để bảo vệ mật khẩu và dữ liệu của người dùng, quá trình này được gọi là xác thực Blockchain.

–Xác thực blockchain đề cập đến hệ thống được phát triển để tăng tính bảo mật của người dùng và xác minh danh tính người dùng và cho phép người dùng kết nối với các tài nguyên được tìm thấy trên các công nghệ tiền kỹ thuật số, giao dịch, tiền điện tử...

–Nó sử dụng công nghệ sổ cái phân tán của blockchain và các phương pháp xác thực để tăng cường quyền riêng tư và bảo mật của các hệ thống xác thực.

–Toàn bộ mạng dựa trên blockchain có khả năng có tính toàn vẹn dữ liệu riêng.

–Thông tin cá nhân được sử dụng để xác minh danh tính của người dùng được lưu trữ trên hàm băm của khối như tên người dùng hoặc mật khẩu. Điều này sẽ giúp đạt được một bản sắc tự chủ.

##### 4.1.5.2 Ví dụ về xác thực Blockchain

Dưới đây là năm lĩnh vực mà xác thực blockchain được sử dụng:

–**Giao dịch tài chính:** Công nghệ Blockchain có thể được áp dụng cho tất cả các giao dịch tài chính. Nhờ blockchain, an ninh tài chính đã được cải thiện rất nhiều. Về cơ bản, công nghệ blockchain được phát triển để xử lý và ghi lại tất cả các giao dịch trên mạng của nó. Ngày nay, nhiều ngân hàng đang bắt đầu sử dụng công nghệ blockchain để cải thiện tính bảo mật của thanh toán và giao dịch.

–**Chuỗi cung ứng:** Chuỗi cung ứng blockchain có thể giúp người tham gia ghi lại thông tin liên quan như giá cả, ngày, địa điểm, chất lượng, chứng nhận..., để quản lý chuỗi cung ứng hiệu quả hơn. Sự sẵn có của thông tin này trong blockchain có thể cải thiện khả năng truy xuất nguồn gốc của chuỗi cung ứng nguyên liệu. Giảm tổn thất từ hàng giả và thị trường xám, tăng khả năng hiển thị và tuân thủ sản xuất hợp đồng thuê ngoài và có khả năng củng cố vị trí của công ty như một nhà lãnh đạo trong sản xuất có trách nhiệm.

–**Y tế:** Việc truy xuất nguồn gốc thuốc rất quan trọng trong chăm sóc sức khỏe vì ngành dược phẩm là một trong những ngành bị ảnh hưởng nhiều nhất bởi hàng giả trên thế giới. Công nghệ Blockchain đang giúp ngành công nghiệp dược phẩm theo dõi an toàn các lô hàng thuốc để chống hàng giả, đây là mối quan tâm lớn đối với ngành chăm sóc sức khỏe.

–**An ninh mạng:** An ninh mạng là bảo vệ hệ thống máy tính và mạng khỏi các cuộc tấn công kỹ thuật số và bảo vệ dữ liệu nhạy cảm trong máy tính hoặc cơ sở dữ liệu. Trong an ninh mạng, Blockchain có thể cung cấp các biện pháp kiểm soát bảo mật nâng cao bằng cách sử dụng cơ sở hạ tầng khóa công khai để xác minh danh tính của các bên và mã hóa thông tin liên lạc của họ. Mã hóa khóa công khai trong mạng blockchain giúp duy trì tính bảo mật của người dùng.

–**Danh tính cá nhân:** Vì danh tính được phân cấp trên sổ cái blockchain, blockchain cung cấp cho người dùng cuối nhiều quyền kiểm soát hơn đối với danh tính kỹ thuật số của họ. Blockchain cung cấp các hồ sơ bất biến cho mục đích quản lý danh tính và pháp y. Do tính chất phi tập trung của công nghệ blockchain, dữ liệu không thể bị giả mạo. Do đó, danh tính cá nhân được bảo mật trên blockchain.

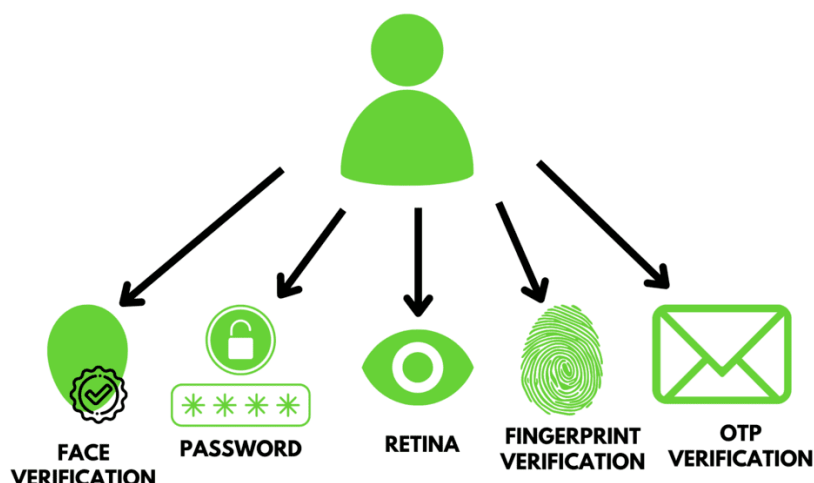
#### 4.1.5.3 Xác thực 2 yếu tố là gì?

Xác thực 2 yếu tố cung cấp thêm một lớp bảo mật bằng cách thêm một lớp bảo mật nữa vào lớp bảo mật hiện có. Xác thực 2 yếu tố liên quan đến việc người dùng nhập kết hợp tên người dùng và mật khẩu và thay vì truy cập thẳng vào tài khoản, người dùng sẽ được nhắc nhập một trong các thông tin sau:

**Những thứ bạn có:** Điều này liên quan đến việc xác thực dựa trên chi tiết thẻ (thẻ tín dụng / thẻ ghi nợ), mã thông báo phần cứng, mã thông báo phần mềm hoặc điện thoại thông minh.

**Những thứ đã biết:** Điều này liên quan đến việc người dùng trả lời một số thông tin bổ sung như câu trả lời cho câu hỏi bí mật hoặc mã PIN (Số nhận dạng cá nhân).

**Xác thực danh tính:** Điều này liên quan đến việc xác thực bằng sinh trắc học như hành vi gõ phím, vân tay, võng mạc, dấu tay...



Hình 4.9 Hình ảnh minh họa xác thực hai yếu tố

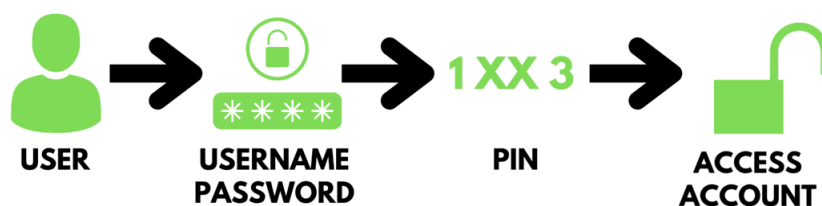
### . Cách thức hoạt động của xác thực hai yếu tố

–**Nhập tên người dùng và mật khẩu:** Trong bước này, người dùng được nhắc nhập tên người dùng và mật khẩu

–**Xác thực tên người dùng và mật khẩu:** Tên người dùng và mật khẩu được xác thực bởi máy chủ xác thực và nếu thông tin đăng nhập chính xác thì người dùng đủ điều kiện để xác thực yếu tố thứ hai.

–**Xác thực yếu tố thứ hai:** Trong bước này, người dùng sẽ nhập thông tin chi tiết theo cơ chế xác thực thứ hai được chọn. Máy chủ xác thực sẽ xác thực thông tin xác thực bổ sung do thiết bị yếu tố thứ hai cung cấp và sẽ xác nhận danh tính người dùng.

Có thể hiểu quy trình trên qua một ví dụ đơn giản trong đó người dùng cố gắng đăng nhập vào tài khoản mạng xã hội.



Hình 4.10 Tại đây người dùng truy cập tài khoản bằng mã PIN và mật khẩu

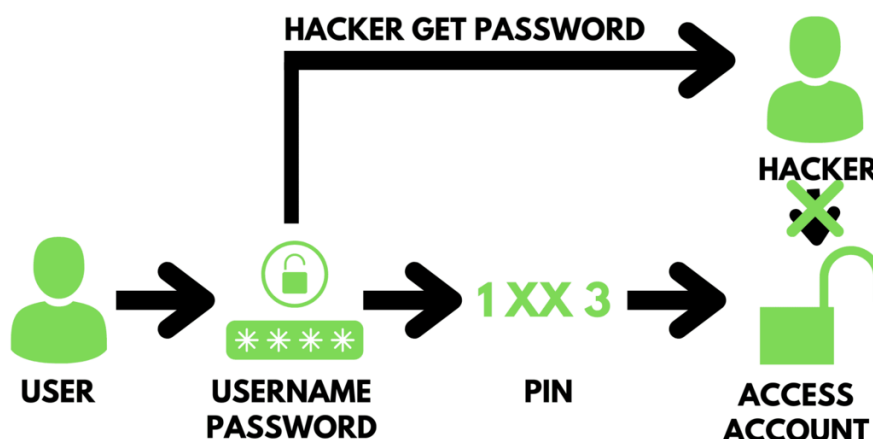
–**Bước 1:** Nhập tên đăng nhập và mật khẩu: Người dùng sẽ nhập tên người dùng và mật khẩu.

–**Bước 2:** Xác thực tên đăng nhập và mật khẩu: Máy chủ xác thực đã xác thực tên người dùng và mật khẩu và thông tin đăng nhập là chính xác. Người dùng đủ điều kiện để xác thực yếu tố thứ hai mà mã PIN trong trường hợp này.

–**Bước 3:** Mã PIN xác thực yếu tố thứ hai: Người dùng sẽ nhập mã PIN gồm 4 chữ số.

–**Bước 4:** Xác thực yếu tố thứ hai: Máy chủ xác thực sẽ kiểm tra mã PIN đã nhập và nếu chính xác, người dùng sẽ có quyền truy cập vào tài khoản.

#### 4.1.5.4 Tầm quan trọng của xác thực hai yếu tố



Hình 4.11 Tin tặc không thể truy cập tài khoản

–**Tăng cường bảo mật:** Xác thực 2 yếu tố bổ sung thêm một lớp bảo mật cho thực tiễn bảo mật hiện có. Ngay cả khi tin tặc có quyền truy cập vào tên người dùng và mật khẩu, tin tặc sẽ không dễ dàng truy cập vào phần thông tin thứ hai như OTP hoặc bất kỳ sinh trắc học nào để truy cập vào tài khoản. Do đó giảm nguy cơ bị tấn công vào tài khoản.

–**Tăng năng suất:** Xác thực 2 yếu tố cho phép nhân viên truy cập tài liệu của công ty và hệ thống của bên thứ ba từ bất kỳ thiết bị nào mà không cần chia sẻ bất kỳ thông tin bí mật nào.

–**Giảm gian lận:** Hầu hết nạn nhân lừa đảo tránh truy cập các trang web từ nơi họ đã trải qua gian lận mặc dù nhà bán lẻ không biết về gian lận hoặc chúng tôi có thể nói không chịu trách nhiệm về gian lận. Việc sử dụng xác thực 2 yếu tố trên các trang đăng nhập và thanh toán của website giúp giảm thiểu các gian lận đó và khiến khách hàng cảm thấy an toàn, tin tưởng.

–**Tăng độ tin cậy:** Xác thực 2 yếu tố giúp nhân viên truy cập dữ liệu công ty từ mọi nơi và giúp người dùng mua hàng hóa từ các trang web Thương mại điện tử một cách an toàn, do đó xây dựng niềm tin giữa người dùng rằng tài khoản của họ được bảo vệ và chống hack. Xây dựng niềm tin là quan trọng nhất để xây dựng mạng lưới khách hàng lâu dài.

#### 4.1.5.5 Blockchain cho xác thực 2 yếu tố

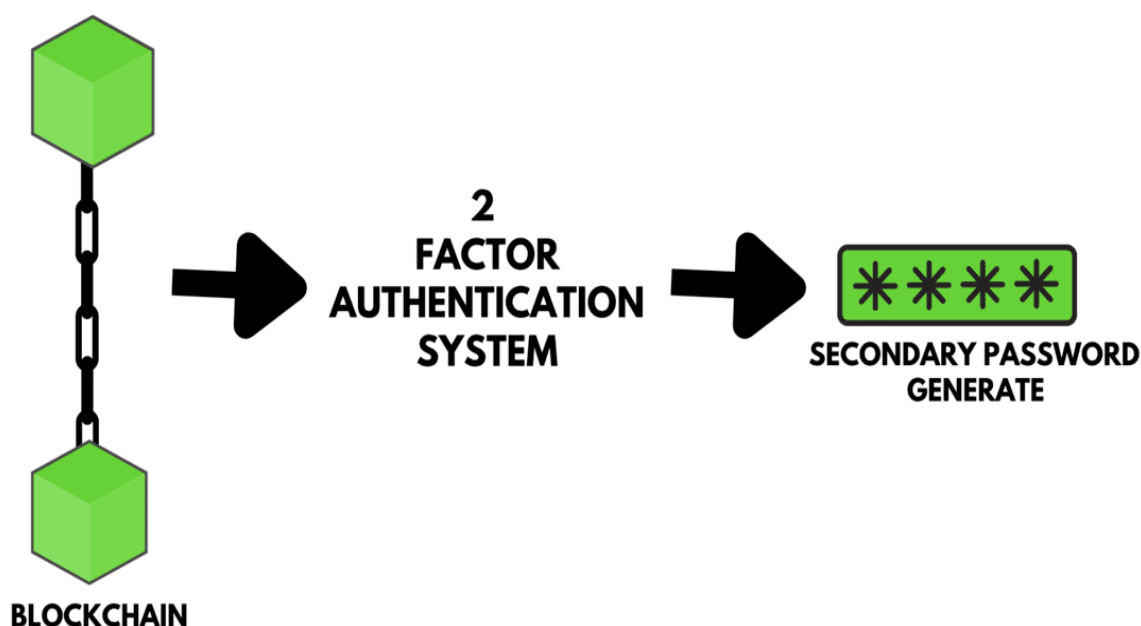
Những điểm sau đây cho chúng ta biết làm thế nào blockchain có thể tăng cường quyền riêng tư và bảo mật của các hệ thống xác thực.

–Bảo mật và toàn vẹn dữ liệu: Blockchain cung cấp tính bảo mật và toàn vẹn dữ liệu tuyệt vời do kiến trúc phi tập trung của nó. Blockchain sử dụng công nghệ băm để lưu trữ thông tin trên sổ cái của nó một cách an toàn. Không có điểm tấn công quan trọng nào để hack và xâm nhập vào hệ thống, điều này có nghĩa là vi phạm cơ sở dữ liệu không còn là mối đe dọa lớn đối với các hệ thống nhận dạng.

–Kiểm soát danh tính kỹ thuật số: Vì danh tính được phân cấp trên sổ cái blockchain, blockchain cung cấp cho người dùng cuối nhiều quyền kiểm soát hơn đối với danh tính kỹ thuật số của họ.

–Bản ghi bất biến: Blockchain cung cấp các hồ sơ bất biến cho mục đích quản lý danh tính và pháp y. Do tính chất phi tập trung của công nghệ blockchain, dữ liệu không thể bị giả mạo, vì vậy mọi thay đổi đều được phản ánh trên tất cả các nút trên mạng blockchain, do đó blockchain trở nên an toàn hơn vì không ai phạm tội gian lận trên mạng blockchain.

–Phân cấp đồn bầy: Blockchain là một công nghệ phi tập trung cho phép giao dịch giữa nhiều bên mà không cần sự tham gia của bất kỳ bên thứ ba nào. Sử dụng blockchain, thông tin nhạy cảm có thể được lưu giữ trên nhiều nút trên mạng blockchain thay vì được lưu giữ trong một cơ sở dữ liệu.



Hình 4.12 Hình ảnh mô tả một hệ thống xác thực hai yếu tố (2FA) sử dụng công nghệ blockchain.



Hệ thống này bao gồm hai thành phần chính:

–Máy chủ xác thực: Máy chủ này lưu trữ thông tin đăng nhập của người dùng, bao gồm tên người dùng, mật khẩu và mã xác minh 2FA.

–Thiết bị khách xác thực: Thiết bị này có thể là điện thoại thông minh, máy tính bảng hoặc khóa bảo mật vật lý. Thiết bị này tạo mã xác minh 2FA.

Hệ thống hoạt động như sau:

–Người dùng muốn đăng nhập vào một ứng dụng hoặc trang web.

–Người dùng nhập tên người dùng và mật khẩu của họ.

–Máy chủ xác thực gửi mã xác minh 2FA đến thiết bị khách xác thực của người dùng.

–Người dùng nhập mã xác minh 2FA vào ứng dụng hoặc trang web.

–Nếu mã xác minh 2FA chính xác, người dùng sẽ được đăng nhập. Nếu mã xác minh 2FA không chính xác, người dùng sẽ không được đăng nhập.

Hệ thống 2FA sử dụng blockchain để tăng cường bảo mật. Blockchain là một hệ thống sổ cái phân tán, có nghĩa là thông tin được lưu trữ trên nhiều máy tính khác nhau. Điều này làm cho việc truy cập trái phép vào thông tin đăng nhập của người dùng trở nên khó khăn hơn.

Ngoài ra, hệ thống 2FA còn sử dụng mã xác minh 2FA, là một mã dùng một lần (OTP) được tạo ra bởi thiết bị khách xác thực. Mã xác minh 2FA chỉ có giá trị trong một khoảng thời gian ngắn, điều này giúp ngăn chặn việc đánh cắp mã xác minh.

**Đánh giá:** Về tổng thể, hệ thống 2FA sử dụng công nghệ blockchain là một cách hiệu quả để tăng cường bảo mật cho tài khoản trực tuyến của bạn.

#### **4.1.6 Tích hợp AI và Blockchain để bảo vệ quyền riêng tư**

##### **4.1.6.1 Khái quát**

Blockchain là một công nghệ lưu trữ dữ liệu phân tán, có nghĩa là dữ liệu được lưu trữ trên nhiều máy tính khác nhau. Điều này làm cho blockchain trở nên rất an toàn và bảo mật, vì dữ liệu không thể bị kiểm soát bởi bất kỳ cá nhân hoặc tổ chức nào.

AI là một lĩnh vực khoa học máy tính liên quan đến việc tạo ra các hệ thống có thể suy nghĩ và hành động như con người. AI có thể được sử dụng để thực hiện nhiều nhiệm vụ khác nhau, bao gồm phân tích dữ liệu, học máy và tự động hóa. Các ứng dụng

nhằm mục đích tích hợp blockchain và trí tuệ nhân tạo thể hiện sự tích hợp ở các khía cạnh sau.

- Sử dụng công nghệ blockchain để ghi lại và lưu trữ dữ liệu đào tạo, đầu vào và đầu ra của mô hình cũng như các tham số, đảm bảo trách nhiệm giải trình và tính minh bạch trong kiểm tra mô hình.

- Sử dụng các khung blockchain để triển khai các mô hình AI nhằm đạt được các dịch vụ phân cấp giữa các mô hình, đồng thời nâng cao khả năng mở rộng và tính ổn định của hệ thống.

- Cung cấp quyền truy cập an toàn vào dữ liệu và mô hình AI bên ngoài bằng cách sử dụng các hệ thống phi tập trung và cho phép các mạng blockchain thu được thông tin bên ngoài đáng tin cậy.

- Sử dụng các thiết kế mã thông báo dựa trên blockchain và cơ chế khuyến khích để thiết lập kết nối và tương tác đáng tin cậy giữa người dùng và nhà phát triển mô hình AI.

#### **4.1.6.2 Bảo vệ quyền riêng tư thông qua việc tích hợp công nghệ Blockchain và AI**

Trong kịch bản hiện tại, hệ thống tin cậy dữ liệu có những hạn chế nhất định làm ảnh hưởng đến độ tin cậy của việc truyền dữ liệu. Để thách thức những hạn chế này, các công nghệ blockchain có thể được triển khai để thiết lập một giải pháp lưu trữ và chia sẻ dữ liệu an toàn và đáng tin cậy nhằm bảo vệ quyền riêng tư và tăng cường bảo mật dữ liệu. Một số ứng dụng của chuỗi khối trong AI bảo vệ quyền riêng tư được đề cập trong bảng sau.

Blockchain Technology	AI Technology	Security Mechanism
Consensus Protocol, Digital Signature	Machine Learning	Decentralization
Permissioned Blockchain, Cryptographic Signature	Machine Learning	De-identification
Anonymity, Multi-Signature	Deep Learning	Privacy Protection Algorithm
Tamper-Resistance, Smart Contract	Machine Learning	Smart contract
Consortium Blockchain, Incentive Mechanism	Federated Learning	De-identification
Consortium Blockchain, Smart Contract, Cryptocurrency	Edge AI	Smart Contract
Privacy Protection, Encryption key	Federated Learning	Encryption Protection
Decentralization, Heterogeneous Encryption, Digital Signature	AI	Encryption Protection
Trustworthiness, Homomorphic Encryption, Differential Privacy	Machine Learning	Privacy Protection Algorithm

*Hình 4.13 Hình ảnh cho thấy cách blockchain và AI có thể được kết hợp để tạo ra các giải pháp mới cho nhiều vấn đề khác nhau.*

Blockchain có thể được sử dụng để lưu trữ dữ liệu AI một cách an toàn và bảo mật. Điều này có thể giúp cải thiện chất lượng của các hệ thống AI, vì dữ liệu sẽ không bị truy cập trái phép hoặc bị thay đổi.

Ngoài ra, blockchain có thể được sử dụng để tạo ra các thị trường AI. Thị trường AI là nơi các nhà phát triển AI có thể chia sẻ và bán tài nguyên AI của họ. Điều này có thể giúp thúc đẩy sự phát triển của AI, vì các nhà phát triển sẽ có thể dễ dàng truy cập vào các tài nguyên họ cần.

AI cũng có thể được sử dụng để cải thiện hiệu quả của blockchain. Ví dụ, AI có thể được sử dụng để tối ưu hóa giao thức đồng thuận blockchain, giúp blockchain hoạt động nhanh hơn và hiệu quả hơn.

Ngoài ra, AI có thể được sử dụng để phát triển các ứng dụng blockchain mới. Ví dụ, AI có thể được sử dụng để phát triển các ứng dụng blockchain cho các lĩnh vực như tài chính, chăm sóc sức khỏe và chính phủ.

Ứng dụng Trí tuệ nhân tạo (AI) trong bảo vệ an toàn và quyền riêng tư cho các giao dịch blockchain có thể mang lại nhiều lợi ích. Dưới đây là một số cách mà AI có thể được tích hợp để cải thiện an toàn và quyền riêng tư trong môi trường blockchain:

–**Phát hiện giao dịch đáng ngờ:** AI có thể được sử dụng để phân tích hành vi giao dịch và xác định các mô hình đáng ngờ hoặc không bình thường. Hệ thống có thể tự động cảnh báo hoặc tạm dừng các giao dịch có thể đe dọa đến an toàn của mạng blockchain.

–**Xác thực hai yếu tố (2FA) dựa Trên AI:** AI có thể được tích hợp để cải thiện các phương tiện xác thực, chẳng hạn như xác thực bằng giọng nói hoặc nhận diện khuôn mặt, để đảm bảo rằng người thực hiện giao dịch là người chính xác.

–**Phân tích tâm trạng và ngôn ngữ:** AI có thể phân tích các thông điệp, bình luận hoặc thông tin từ các giao dịch để đánh giá tâm trạng và ngôn ngữ có thể điều hướng đến môi đe dọa hoặc lừa đảo.

–**Học mô hình tự động cho bảo mật:** Học máy và học sâu có thể được sử dụng để xây dựng mô hình dự đoán và phát hiện mẫu lạ, giúp nâng cao khả năng phát hiện lừa đảo trong các giao dịch.

–**Mạng lưới nơ-ron đồng thuận:** Mạng lưới nơ-ron có thể được sử dụng để cải thiện đồng thuận blockchain bằng cách tối ưu hóa quy trình xác minh và xác nhận giao dịch.

–**Quản lý quyền riêng tư:** AI có thể giúp quản lý quyền riêng tư bằng cách tự động hóa quy trình ẩn danh hóa và bảo vệ thông tin cá nhân.

–**Dự báo và phòng ngừa:** Sử dụng AI để dự báo các mô hình tấn công tiềm ẩn và triển khai các biện pháp phòng ngừa trước khi xảy ra vấn đề.

–**Hệ thống bảo mật dựa trên sự kiện:** Tích hợp AI vào hệ thống bảo mật dựa trên sự kiện để phản ứng nhanh chóng đối với các sự kiện đáng ngờ hoặc lừa đảo.

–**Quản lý rủi ro dựa trên dữ liệu lớn:** Sử dụng khả năng xử lý dữ liệu lớn của AI để phân tích rủi ro và cải thiện khả năng dự báo về các vấn đề bảo mật.

–**Giao thức đồng thuận tự động:** AI có thể giúp tự động hóa và tối ưu hóa giao thức đồng thuận, cải thiện hiệu suất và đảm bảo tính an toàn.

**Đánh giá:** Tích hợp AI vào môi trường blockchain không chỉ giúp tăng cường an toàn mà còn nâng cao khả năng bảo vệ quyền riêng tư của người dùng trong quá trình thực hiện các giao dịch.

#### **4.1.7 Sử dụng các giải pháp riêng tư:**

Một số giải pháp riêng tư cụ thể bao gồm:

–Zero-Knowledge Proof (ZKP): ZKP là một kỹ thuật mã hóa cho phép một bên chứng minh cho bên kia rằng họ biết một số thông tin mà không cần tiết lộ thông tin đó. ZKP có thể được sử dụng để bảo vệ danh tính của người dùng trong các giao dịch blockchain bằng cách cho phép người dùng xác minh tính hợp lệ của một giao dịch mà không cần biết danh tính của người thực hiện giao dịch.

–Ring Signature: Ring Signature là một kỹ thuật mã hóa cho phép một người tạo ra một chữ ký điện tử mà không thể xác định được người ký. Ring Signature có thể được sử dụng để bảo vệ quyền riêng tư của người dùng trong các giao dịch blockchain bằng cách cho phép người dùng thực hiện một giao dịch mà không tiết lộ danh tính của họ.

–Confidential Transactions (CT): CT là một kỹ thuật mã hóa cho phép người dùng ẩn nội dung của các giao dịch. CT có thể được sử dụng để bảo vệ quyền riêng tư của người dùng trong các giao dịch blockchain bằng cách cho phép người dùng thực hiện một giao dịch mà không tiết lộ số tiền hoặc các bên liên quan đến giao dịch.

#### **Ưu điểm của các giải pháp riêng tư**

–Bảo vệ quyền riêng tư của người dùng: Các giải pháp riêng tư giúp bảo vệ quyền riêng tư của người dùng trong các giao dịch blockchain bằng cách ngăn chặn kẻ tấn công theo dõi các giao dịch của họ hoặc xác định danh tính của họ dựa trên các giao dịch của họ.

–Tăng cường tính bảo mật: Các giải pháp riêng tư có thể giúp tăng cường tính bảo mật của blockchain bằng cách ngăn chặn kẻ tấn công sử dụng các thông tin từ các giao dịch để thực hiện các cuộc tấn công.

#### **Nhược điểm của các giải pháp riêng tư**

–Tăng chi phí: Các giải pháp riêng tư thường yêu cầu sử dụng các kỹ thuật mã hóa phức tạp, điều này có thể làm tăng chi phí của các giao dịch blockchain.

–Giảm hiệu suất: Các giải pháp riêng tư có thể làm giảm hiệu suất của các giao dịch blockchain, vì chúng yêu cầu thêm bước mã hóa và giải mã.

## **CHƯƠNG 5: SO SÁNH VÀ PHÂN TÍCH CÁC MÔ HÌNH QUYỀN RIÊNG TƯ KHÁC NHAU TRÊN BLOCKCHAIN**

### **5.1 Tìm hiểu và phân tích các mô hình quyền riêng tư trên blockchain:**

Một mô hình quyền riêng tư là một hệ thống hoặc giao thức được thiết kế để bảo vệ quyền riêng tư của người dùng. Quyền riêng tư là quyền của một người để kiểm soát thông tin của họ.

#### **5.1.1 Mô hình quyền riêng tư Zero-knowledge proof (ZKP)**

##### **5.1.1.1 Tổng quan về ZKP**

Zero-knowledge Proof (ZKP) là một công nghệ mật mã học cho phép một bên (người chứng minh) chứng minh cho bên kia (người xác nhận) rằng họ biết một thông tin cụ thể mà không cần phải tiết lộ thông tin đó.

##### **Một số đặc điểm của Zero-knowledge Proof**

Zero-knowledge Proof có một số đặc điểm cơ bản để phân biệt với các công nghệ khác. Dưới đây là ba đặc điểm cơ bản của công nghệ ZKP:

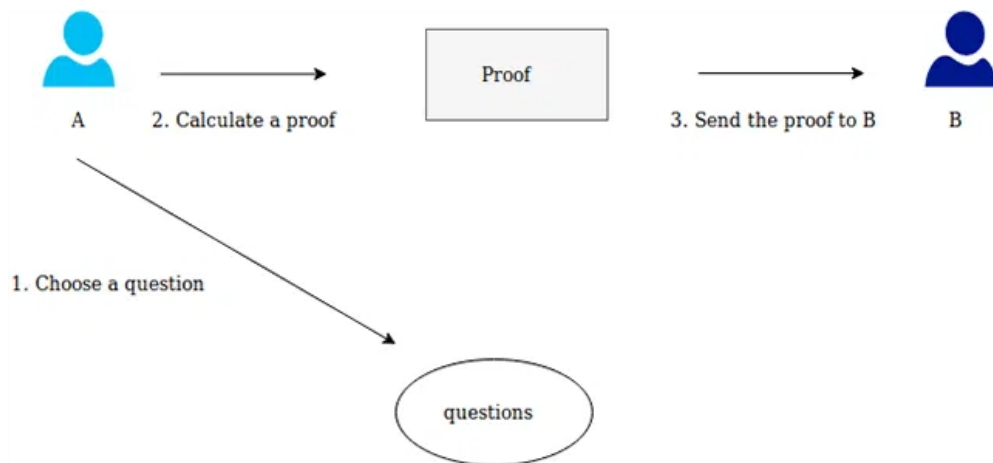
– Tính đầy đủ: Khi cung cấp đầy đủ các thông tin, minh chứng để chứng minh tuyên bố là đúng, người xác minh sẽ bị thuyết phục.

– Tính hợp lý: Nếu các thông tin, minh chứng đưa ra không hợp lý, người xác minh sẽ biết rằng tuyên bố đó là sai. Rất khó để bạn có thể gian lận được, trừ một số xác suất nhỏ.

– Zero-knowledge: Người xác minh sẽ không có thêm bất kỳ thông tin nào ngoài tuyên bố hiện tại và tính xác thực của tuyên bố ấy. Tất cả các thông tin khác sẽ bị ẩn đi.

Ở dạng cơ bản, ZKP được tạo thành từ ba yếu tố: “nhân chứng”, “thách thức” và “phản hồi”.

– Nhân chứng: Với Zero-knowledge Proof, người chứng minh muốn chứng minh kiến thức về một số thông tin ẩn. Thông tin bí mật là “nhân chứng” cho bằng chứng, và giả định của người chứng minh về nhân chứng thiết lập một loạt câu hỏi mà chỉ một bên có kiến thức về thông tin mới có thể trả lời được. Do đó, người chứng minh bắt đầu quá trình chứng minh bằng cách chọn ngẫu nhiên một câu hỏi, tính toán câu trả lời và gửi nó cho người xác minh.



*Hình 5. 1 Hình ảnh mô tả quá trình chứng minh kiến thức về một số thông tin  
ẩn một cách an toàn và bảo mật*

Trong hình ảnh, có hai chủ thể tham gia vào quá trình chứng minh:

+Người chứng minh (Prover): là người có kiến thức về thông tin ẩn mà họ muốn chứng minh.

+Người xác minh (Verifier): là người muốn xác minh kiến thức của người chứng minh.

Quá trình chứng minh bao gồm các bước sau:

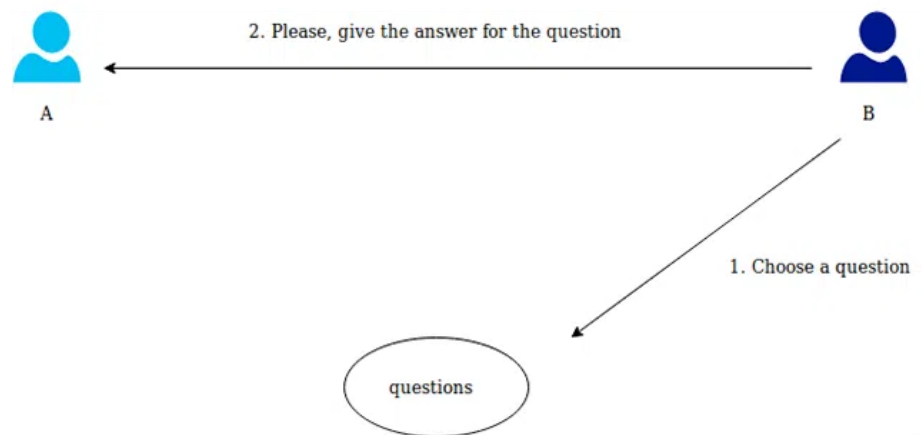
+Chọn câu hỏi: Người chứng minh chọn ngẫu nhiên một câu hỏi từ một tập hợp các câu hỏi mà chỉ một bên có kiến thức về thông tin mới có thể trả lời được.

+Tính toán câu trả lời: Người chứng minh tính toán câu trả lời cho câu hỏi đã chọn.

+Gửi câu trả lời: Người chứng minh gửi câu trả lời cho người xác minh.

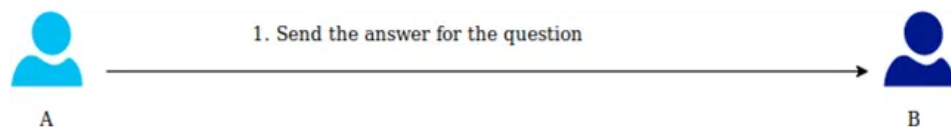
+Xác minh câu trả lời: Người xác minh sử dụng kiến thức của họ về thông tin ẩn để xác minh câu trả lời của người chứng minh.

–Thách thức : Người chứng minh nhận câu hỏi, tính toán câu trả lời và gửi kết quả lại cho người xác minh.



Hình 5. 2 Hình ảnh minh họa “thách thức”

–Phản hồi: Người kẻ tiếp nhận câu hỏi, tính toán câu trả lời và trả lại cho người xác minh. Câu trả lời của người chứng minh cho phép người xác minh kiểm tra xem người trước có thực sự tiếp cận được nhân chứng hay không.



Hình 5. 3 Hình ảnh minh họa “phản hồi”

Để đảm bảo người xác minh không đoán mò quá và tình cờ nhận được câu trả lời đúng, người xác minh chọn thêm câu hỏi để hỏi. Bằng cách lặp lại sự tương tác này nhiều lần, khả năng người chứng minh giả mạo biết về nhân chứng giảm đáng kể cho đến khi người xác minh hài lòng.

#### 5.1.1.2 Phương thức hoạt động của Zero-knowledge Proof

Để có thể hiểu rõ về phương thức hoạt động của Zero-knowledge Proof, hãy theo dõi một ví dụ “Hang động Alibaba”.

Hãy tưởng tượng, Alice và Bob đang đứng trước một hang động có hai lối đi dẫn đến hai con đường riêng biệt (con đường A và con đường B). Trong hang động này sẽ có một cánh cửa nối liền hai lối đi và chỉ có thể mở bằng một mật mã bí mật. Hiện nay, Alice đang sở hữu mật mã đó, Bob đang muốn mua lại mật mã của Alice.



Trước hết Bob cần Alice chứng minh rằng mình đang thực sự sở hữu mật mã đó. Vậy làm cách nào để Alice có thể chứng minh mà không cần tiết lộ nội dung trong mật mã?

Đầu tiên Bob sẽ yêu cầu Alice đi vào hang động bằng một trong hai con đường A và B một cách ngẫu nhiên. Khi đến cánh cửa nối, Bob sẽ yêu cầu Alice phải đi ra bằng lối ra nào. Có hai trường hợp xảy ra:

- Thứ nhất Alice có thể dễ dàng đi qua mà không cần phải mở cánh cửa nối liền hai đường.

- Thứ hai Alice có thể đi qua con đường mà Bob yêu cầu vì Alice biết được mật mã cánh cửa nối hai con đường.

Để đảm bảo rằng không xảy ra trường hợp một, Bob sẽ phải bắt buộc lặp đi lặp lại các kiểm tra của mình đến số lần nhất định để khẳng định rằng Alice chắc chắn có giữ mật mã. Về phần Alice cũng không cần phải chia sẻ nội dung trong mật mã.

Như vậy, cách thức hoạt động của ZKP cũng tương tự như trên. Bên chứng minh sẽ cung cấp cho bên xác nhận các thông tin mình đưa ra là đúng mà không cần phải tiết lộ thêm bất kì các thông tin nào khác ngoài tuyên bố.

### **5.1.1.3 Ưu điểm và hạn chế của Zero-knowledge Proof**

#### **Ưu điểm:**

- Bảo vệ Quyền Riêng Tư: Zero-knowledge proofs cung cấp phương tiện mạnh mẽ để bảo vệ quyền riêng tư, đặc biệt trong các ứng dụng blockchain, nơi thông tin nhạy cảm như người thực hiện giao dịch, số lượng tiền, và người nhận có thể được giữ bí mật.

- Chứng Minh Tính Đúng Đắn Mà Không Tiết Lộ Chi Tiết: Cho phép chứng minh tính đúng đắn của một tuyên bố mà không cần phải tiết lộ thông tin chi tiết, giữ cho sự ẩn danh và bảo mật.

- Giảm Thiểu Tương Tác: Các dạng như zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) cho phép tạo ra các chứng minh không cần tương tác nhiều giữa người chứng minh và người xác nhận, giảm bớt giao tiếp và tài nguyên tính toán.

- Chống Gian Lận: Cung cấp cách hiệu quả để ngăn chặn và phát hiện gian lận trong các ứng dụng như giao dịch tài chính hoặc quản lý quyền truy cập.

–Tính Toàn Vẹn và An Toàn: Đảm bảo tính toàn vẹn và an toàn của dữ liệu, giữ cho thông tin không bị thay đổi hay bị tấn công.

**Nhược điểm:**

–Tính Tính Toán Phức Tạp: Các phương pháp chứng minh không thông tin thường đòi hỏi tài nguyên tính toán lớn, đặc biệt là các dạng như zk-SNARKs, có thể làm tăng chi phí tính toán và tài nguyên hệ thống.

–Khả Năng Triển Khai Khó Khăn: Việc triển khai và tích hợp các giải pháp Zero-knowledge proofs đòi hỏi kiến thức sâu rộng về mật mã và công nghệ, điều này có thể làm tăng ngưỡng khả năng sử dụng cho nhiều ứng dụng.

–Chưa Đạt Đến Quy Mô Lớn: Một số phương pháp Zero-knowledge proofs có thể gặp khó khăn khi áp dụng trên quy mô lớn, đặc biệt là khi cần xử lý một lượng lớn dữ liệu.

#### **5.1.1.4 Phân loại loại Zero-knowledge Proof**

##### **5.1.1.4.1 ZK-SNARK**

ZK-SNARK là viết tắt của Zero-Knowledge Succinct Non-Interactive Argument of Knowledge . Giao thức ZK-SNARK có các đặc điểm sau:

–Không có kiến thức: Người xác minh có thể xác thực tính toàn vẹn của một câu lệnh mà không cần biết bất cứ điều gì khác về câu lệnh đó. Kiến thức duy nhất mà người xác minh có về tuyên bố là liệu nó đúng hay sai.

–Ngắn gọn: Bằng chứng không có kiến thức nhỏ hơn bằng chứng và có thể được xác minh nhanh chóng.

–Không tương tác: Bằng chứng là 'không tương tác' vì người chứng minh và người xác minh chỉ tương tác một lần, không giống như bằng chứng tương tác yêu cầu nhiều vòng giao tiếp.

–Lập luận: Bằng chứng đáp ứng yêu cầu về 'tính hợp lý', vì vậy việc gian lận là cực kỳ khó xảy ra.

–(Of) Knowledge: Không thể xây dựng bằng chứng không có kiến thức nếu không có quyền truy cập vào thông tin bí mật (nhân chứng). Rất khó, nếu không muốn nói là không thể, đối với một người chứng minh không có nhân chứng để tính toán một bằng chứng không có kiến thức hợp lệ.

–Thiết lập đáng tin cậy yêu cầu người dùng tin tưởng những người tham gia tạo tham số. Tuy nhiên, sự phát triển của ZK-STARK đã cho phép chứng minh các giao thức hoạt động với thiết lập không đáng tin cậy.

#### **5.1.1.4.2 ZK-STARK**

–ZK-STARK là từ viết tắt của Đối số tri thức minh bạch có thể mở rộng không kiến thức . ZK-STARK tương tự như ZK-SNARK, ngoại trừ:

–Có thể mở rộng: ZK-STARK nhanh hơn ZK-SNARK trong việc tạo và xác minh bằng chứng khi quy mô của nhân chứng lớn hơn. Với bằng chứng STARK, thời gian của người chứng minh và người xác minh chỉ tăng nhẹ khi nhân chứng tăng lên (thời gian người chứng minh và người xác minh SNARK tăng tuyến tính với quy mô nhân chứng).

–Minh bạch: ZK-STARK dựa vào tính ngẫu nhiên có thể kiểm chứng công khai để tạo các tham số công khai nhằm chứng minh và xác minh thay vì thiết lập đáng tin cậy. Do đó, chúng minh bạch hơn so với ZK-SNARK.

–ZK-STARK tạo ra bằng chứng lớn hơn ZK-SNARK, nghĩa là chúng thường có chi phí xác minh cao hơn. Tuy nhiên, có những trường hợp (chẳng hạn như chứng minh tập dữ liệu lớn) trong đó ZK-STARK có thể tiết kiệm chi phí hơn ZK-SNARK.

#### **5.1.1.5 Ứng dụng phổ biến của Zero-knowledge Proof**

Công nghệ Zero-knowledge Proof tạo ra mang đến nhiều tiện ích cho người dùng, đảm bảo quyền riêng tư và tính bảo mật. Vì thế Zero-knowledge Proof được ứng dụng vào nhiều vấn đề khác nhau. Dưới đây là một số ứng dụng tiêu biểu của ZKP

–Ứng dụng nhắn tin bảo mật: So với các ứng dụng truyền thống, khi nhắn tin bạn phải cần sự xác nhận danh tính thì đối với ZKP bạn không cần phải thực hiện điều này. ZKP sử dụng công nghệ để mã hóa dữ liệu end-to-end cho phép tin nhắn gửi đi một cách riêng tư.

–Ứng dụng trong Blockchain: Công nghệ ZKP hứa hẹn sẽ là một trong các công nghệ hàng đầu trong giải pháp giúp mở rộng Blockchain. Các giải pháp Zk Rollup giúp quá trình xác minh - xác nhận các giao dịch một cách nhanh chóng. Điều này có ích cho việc Ethereum và layer 1 mở rộng một cách mạnh mẽ.

–Ứng dụng trong xác minh: ZKP sẽ hạn chế bất kỳ sự truy cập nào nếu đó không phải là tác giả.

–Ứng dụng trong tài liệu: Công nghệ giúp truyền tải thông tin một cách bảo mật cao. Đảm bảo quyền riêng tư và tính bảo mật cho người dùng.

–Ứng dụng trong chia sẻ dữ liệu: Zero-knowledge Proof cho phép truyền tải dữ liệu trên chuỗi mà không cần phải thông qua bên thứ ba.

–Ứng dụng trong bảo mật thông tin nhạy cảm: ZKP tăng cường khả năng bảo mật các thông tin nhạy cảm như các sao kê ngân hàng hoặc Credit Card,...

–Ứng dụng trong bảo vệ lưu trữ: Đây là một trong các công nghệ đáng lựa chọn trong việc bảo vệ lưu trữ khỏi các Hacker.

–Ứng dụng trong file điều khiển hệ thống: ZKP có thể thực hiện bảo vệ các file hệ thống. Với mỗi file, người dùng và người đăng nhập tạo ra các lớp bảo vệ cho các file.

### **Những Blockchain ứng dụng công nghệ Zero-knowledge Proof:**

#### **StarkWare**

–StarkWare được thành lập vào năm 2018 bởi nhà khoa học đi đầu trong lĩnh vực tính toán Zk. Công nghệ này được xây dựng dựa trên Zk-STARKs. Các sản phẩm của StarkWare sử dụng nền tảng Turing và ngôn ngữ lập trình để tạo ra bản thử nghiệm có tên là Cairo.

–StarkWare mang đến giải pháp Validium với khách hàng (StarkEx). Đây là một trong những giải pháp quy mô đầu tiên của Zero-knowledge Proof cho thấy sự phù hợp của thị trường sản phẩm với các giao thức khác. Dapp DeFi và NFT đều đã tận dụng giải pháp này để mang đến trải nghiệm tiện ích hơn cho người dùng.

–Điểm mạnh rõ nhất của StarkWare là chứng minh được giải pháp mở rộng quy mô của mình Chính vì thế mà số vốn đầu tư tăng dần qua các năm.

#### **Matters Labs**

–Matters Labs được thành lập năm 2019 bởi Alex Gluchowski và Alex Vlasov là những người đều có chuyên môn sâu về nghiên cứu và phát triển Ethereum và ZK.

#### **Secret Network**

–Secret Network thực hiện các tính toán trong TEE (Trusted Execution Environments) để nâng cấp tính bảo mật và riêng tư. Đây là Smart Contract ẩn danh đầu tiên khởi chạy Mainnet.

–TEE thực chất là một phần cơ bản của máy tính có thể chạy tính toán và lưu trữ dữ liệu mà ngay cả chủ sở hữu cũng không thể truy cập được. Điều này đảm bảo Node

vẫn truy cập các phép tính trong khi cả đầu vào và đầu ra đang trong trạng thái được mã hóa hoàn toàn.

–Hiện nay, Secret NetWork đang sở hữu nhiều sector khác nhau như: Lending Protocol, NFT Marketplace, Liquid Staking Protocol,...

### **Immutable X**

–Immutable X là một Validium cho NFT trên Ethereum, được xây dựng trên StarkEx. Thực hiện các giao dịch NFT và các hoạt động liên quan đến NFT là ứng dụng chủ yếu của Immutable X.

–Mặc dù đây là NFT Protocol nổi bật của công nghệ Zk Rollup nhưng vẫn cần cải thiện rất nhiều chỗ vì khối lượng giao dịch còn tương đối thấp

### **dYdX**

–Đây là một Trading Platform được xây dựng trên StarkEx. Nền tảng hỗ trợ nhiều loại sản phẩm như: Spot Trading, Margin, Perpetuals.

–dYdX hiện đang chiếm giữ TVL \$960M và lượng giao dịch hàng ngày quanh mức \$500M. Đây chính là một trong các sàn giao dịch phái sinh hàng đầu hiện nay.

### **Polygon**

–Polygon cũng là một nhân tố quan trọng khác của Rollup. Hiện nay Polygon đã ra mắt Nightfall, một Rollup tập trung vào quyền riêng tư hợp tác với EY. Polygon về cơ bản đã triển khai ba Rollup để phục vụ cho các mục đích sau:

–Polygon Hermez (Zk Rollup)

–Polygon Nightfall (Zk Rollup vào quyền riêng tư)

–Polygon Miden (dựa trên STARK, EVM Rollup)

–Mina Protocol

–Mina Protocol (trước đây được biết đến là Coda Protocol). Evan Shapiro và Isaac Meckler là hai nhà khoa học đã thành lập nên Mina Protocol. Vào tháng 3 năm 2021, Mina Protocol chính thức Mainnet sau gần ba năm phát triển.

–Đây cũng là dự án nhận được nhiều đầu tư như: Multicooin Capital, Polychain Capital,.... Mina Protocol được thiết kế hướng đến kích thước không đổi là 22kb để trở thành Blockchain nhẹ nhất thế giới.

### **Dusk Network**

–Đây là một Privacy Blockchain dành cho ứng dụng tài chính. ZKP là công nghệ được sử dụng để làm cơ sở cho các Smart Contract.

–Mục tiêu hướng đến của Dusk Network là trở thành layer 1 đầu tiên hỗ trợ Smart Contract ZKP. Các nhà đầu tư tài chính có thể an tâm bởi tính bảo mật cao thông qua việc sử dụng công nghệ ZKP PLONK Proof để xác nhận và xác minh giao dịch.

### **5.1.2 Mô hình quyền riêng tư Ring Signatures (chữ ký dạng vòng)**

#### **5.1.2.1 Giới thiệu về Ring Signatures (chữ ký dạng vòng)**

–Chữ ký vòng là một loại chữ ký số cho phép một người ký một tài liệu mà không tiết lộ danh tính của họ. Chữ ký vòng sử dụng thuật toán mật mã để tạo ra một chữ ký mà chỉ có thể được xác minh bởi một nhóm người, được gọi là vòng.

–Theo truyền thống, chữ ký số chỉ sử dụng một khóa mà bất kỳ ai cũng có thể dễ dàng liên kết với một người dùng cụ thể. Điều này có nghĩa là có thể truy tìm lại giao dịch về bên đã thực hiện giao dịch đó.

–Vào năm 2021, một nhóm các nhà nghiên cứu có tên là nhóm Rivest, Shamir và Tauman (RST) đã nhận ra vấn đề này và đưa ra chữ ký vòng để ký các tin nhắn với tư cách một nhóm và giữ ẩn danh danh tính của người ký thực tế.

–Tiền điện tử dựa trên quyền riêng tư Monero sử dụng chữ ký vòng trong cơ sở hạ tầng của nó để bảo vệ danh tính của người dùng trong quá trình giao dịch.

#### **5.1.2.2 Cách thức hoạt động của Ring Signatures**

Chữ ký vòng sử dụng bài toán logarit rời rạc để cho phép các thành viên trong nhóm cùng ký một tin nhắn bằng khóa của họ. Việc tính toán khiến bất kỳ bên thứ ba nào không thể xác định khóa riêng được sử dụng để tạo chữ ký.

Để tạo ra một chữ ký vòng, người ký cần có một cặp khóa riêng và khóa công khai. Khóa riêng chỉ được biết bởi người ký, còn khóa công khai được chia sẻ với tất cả mọi người trong vòng.

Người ký tạo chữ ký bằng cách sử dụng khóa riêng của họ để tạo ra một hàm băm của tài liệu được ký. Sau đó, họ sử dụng hàm băm này để tạo ra một chữ ký vòng. Chữ ký vòng bao gồm một số thông tin, bao gồm:

- Hàm băm của tài liệu được ký
- Một số ngẫu nhiên
- Một số khóa công khai từ vòng
- Cách xác minh chữ ký vòng

Để xác minh một chữ ký vòng, người xác minh cần có khóa công khai của tất cả mọi người trong vòng. Người xác minh sử dụng khóa công khai của mọi người trong vòng để giải mã chữ ký. Nếu chữ ký được giải mã thành hàm băm của tài liệu được ký, thì chữ ký được coi là hợp lệ.

Ví dụ, trong giao dịch Monero (XMR)



Hình 5. 4 Hình ảnh minh họa cách hoạt động của chữ ký vòng trong Monero.

–An output of the person sending Monero: Đây là phần tiền xu mà người gửi Monero muốn ký.

–Non-signers: Đây là những người không ký chữ ký. Họ cung cấp các khóa công khai của họ để giúp bảo vệ quyền riêng tư của người ký.

–Monero Ring Signatures: Đây là chữ ký vòng được tạo ra bởi người gửi.

–Outputs of previous transactions on the Monero blockchain: Đây là các phần tiền xu từ các giao dịch Monero trước đó. Chúng được sử dụng để tạo ra chữ ký vòng.

–Signer: Đây là người ký chữ ký.

Cách hoạt động của chữ ký vòng được giải thích như sau:

–Người gửi Monero tạo ra một chữ ký vòng bằng cách sử dụng khóa riêng của họ. Chữ ký vòng bao gồm một hàm băm của phần tiền xu được ký, một số ngẫu nhiên, và một số khóa công khai từ những người không ký.

–Người gửi Monero gửi chữ ký vòng cùng với phần tiền xu được ký cho người nhận.

–Người nhận sử dụng khóa công khai của những người không ký để xác minh chữ ký vòng. Nếu chữ ký được xác minh thành công, thì người nhận biết rằng người gửi đã ký phần tiền xu.

Chữ ký vòng bảo vệ quyền riêng tư của người gửi bằng cách không tiết lộ danh tính của họ. Chỉ có những người trong vòng mới có thể xác minh chữ ký, vì vậy, kẻ tấn công không thể biết chắc chắn ai là người đã ký chữ ký.

Trong hình ảnh, người gửi Monero là người đứng ở trung tâm vòng. Người gửi sử dụng khóa riêng của họ để tạo ra chữ ký vòng. Họ sau đó gửi chữ ký vòng cùng với phần tiền xu được ký cho người nhận. Người nhận sử dụng khóa công khai của những người không ký để xác minh chữ ký vòng. Nếu chữ ký được xác minh thành công, thì người nhận biết rằng người gửi đã ký phần tiền xu.

Những người không ký trong vòng cung cấp các khóa công khai của họ để giúp bảo vệ quyền riêng tư của người gửi. Khóa công khai của những người không ký được sử dụng để tạo ra chữ ký vòng. Nếu kẻ tấn công muốn xác định được người gửi, họ sẽ cần phải có khóa riêng của tất cả mọi người trong vòng. Điều này là rất khó khăn, vì khóa riêng chỉ được biết bởi những người trong vòng.

### **5.1.2.3 Ưu nhược điểm của chữ ký vòng**

#### **Ưu điểm**

– Quyền riêng tư giao dịch và ẩn danh người dùng: Chữ ký vòng cung cấp quyền riêng tư và ẩn danh giao dịch cho người dùng tiền điện tử.

– Tăng cường bảo mật: Bên thứ ba không thể giả mạo hoặc giả mạo chữ ký vòng.

– Khả năng mở rộng: Khái niệm ký tin nhắn thay mặt cho một nhóm lớn người dùng có tiềm năng cho các ứng dụng ngoài giao dịch. Ví dụ về các ứng dụng như vậy bao gồm giao tiếp ẩn danh, tố cáo, xác thực nhóm và hệ thống bỏ phiếu.

#### **Nhược điểm**

Chữ ký vòng có một số nhược điểm:

– Tốc độ và phí giao dịch: Không giống như chữ ký số truyền thống, chữ ký vòng lớn hơn, do tính năng sử dụng khóa nhóm làm mờ. Do đó, điều này có thể gây tắc nghẽn mạng và làm chậm giao dịch, khiến người dùng phải trả phí cao hơn.

– Tính ẩn danh không phải lúc nào cũng được đảm bảo: Có thể theo dõi các giao dịch trong các nhóm nhỏ, đặc biệt nếu danh tính thực sự của người dùng được biết.

### **5.1.2.4 Ứng dụng của chữ ký dạng vòng**

– Chữ ký số: Chữ ký vòng có thể được sử dụng để tạo chữ ký số cho các tài liệu điện tử. Điều này giúp đảm bảo tính xác thực và toàn vẹn của các tài liệu này.



–Bảo vệ quyền riêng tư: Chữ ký vòng có thể được sử dụng để bảo vệ quyền riêng tư của người dùng khi họ thực hiện các giao dịch trực tuyến. Ví dụ, một người dùng có thể sử dụng chữ ký vòng để mua hàng trực tuyến mà không cần tiết lộ danh tính của họ.

–Tính năng an ninh: Chữ ký vòng có thể được sử dụng để tăng cường tính an ninh của các hệ thống và ứng dụng. Ví dụ, chữ ký vòng có thể được sử dụng để bảo vệ các cuộc bầu cử trực tuyến khỏi gian lận.

### **5.1.3 Mô hình quyền riêng tư Mimblewimble**

Trong lĩnh vực công nghệ blockchain, Mimblewimble là một khái niệm mới thu hút sự chú ý trong những năm gần đây. Đó là một giao thức tập trung vào quyền riêng tư, được giới thiệu lần đầu tiên vào năm 2016 bởi một nhà phát triển ẩn danh, sử dụng biệt danh Tom Elvis Jedusor (tên tiếng Pháp của kẻ thù chính của Harry Potter, Lord Voldemort). Mục tiêu của Mimblewimble là giải quyết một số vấn đề về quyền riêng tư và khả năng mở rộng mà các mạng blockchain truyền thống như Bitcoin đã từng gặp phải.

#### **5.1.3.1 Những điều cơ bản về giao thức Mimblewimble Blockchain**

Mimblewimble blockchain là một giao thức blockchain thông minh, đảm bảo tính riêng tư và khả năng mở rộng giao dịch. Lấy cảm hứng từ bộ truyện Harry Potter, Mimblewimble được ví von như một loại phép thuật giúp ngăn chặn việc tiết lộ thông tin cá nhân, phù hợp với chức năng của giao thức này.

Điểm đặc biệt của Mimblewimble so với các blockchain khác như Bitcoin là nó đảm bảo tính ẩn danh hoàn toàn, không tiết lộ địa chỉ người gửi, số lượng tiền đi và địa chỉ người nhận, thông tin thường được tiết lộ trong các loại tiền mã hóa khác.

Giao thức này kết hợp công nghệ từ các giao thức mật mã như CoinJoin, Confidential Transactions (CTs), Dandelion và Cut-Through nhằm cải thiện tính bảo mật và ẩn danh. Ví dụ, CoinJoin kết hợp các thanh toán từ nhiều người gửi thành một giao dịch duy nhất, làm cho việc theo dõi quỹ tiền trở nên khó khăn.

Mimblewimble có những đặc điểm độc đáo như tính ẩn danh, tính thay thế và khả năng mở rộng, đó là lý do tại sao giao thức này có tiềm năng phát triển trong công nghệ blockchain trong tương lai.

Mimblewimble được sử dụng trong nhiều dự án tiền mã hóa nhờ tính bảo mật, riêng tư và khả năng mở rộng mạnh mẽ. Đồng tiền mã hóa gốc MimbleWimble Coin (MWC) cũng được phát triển dựa trên giao thức này.

Các đồng tiền mã hóa khác như Grin (GRIN) và Beam (BEAM) cũng sử dụng Mimblewimble. Thậm chí một số đồng tiền mã hóa phổ biến khác như Litecoin (LTC) cũng tích hợp Mimblewimble để cải thiện tính riêng tư và tính thay thế trong giao dịch trên blockchain của họ.

### **5.1.3.2 Cách thức hoạt động:**

Mimblewimble sử dụng một dạng mật mã đường cong elip. Trong mạng sử dụng giao thức Mimblewimble, không có địa chỉ nào trên blockchain giúp việc lưu trữ dữ liệu mạng đạt hiệu quả cao.

Mimblewimble chỉ yêu cầu dung lượng lưu trữ nhiều hơn khoảng 10% so với mạng Bitcoin, khiến nó có khả năng mở rộng cao và nhanh hơn. Ngược lại với Bitcoin, khi người dùng gửi giao dịch BTC, ba thông tin sẽ được công khai:

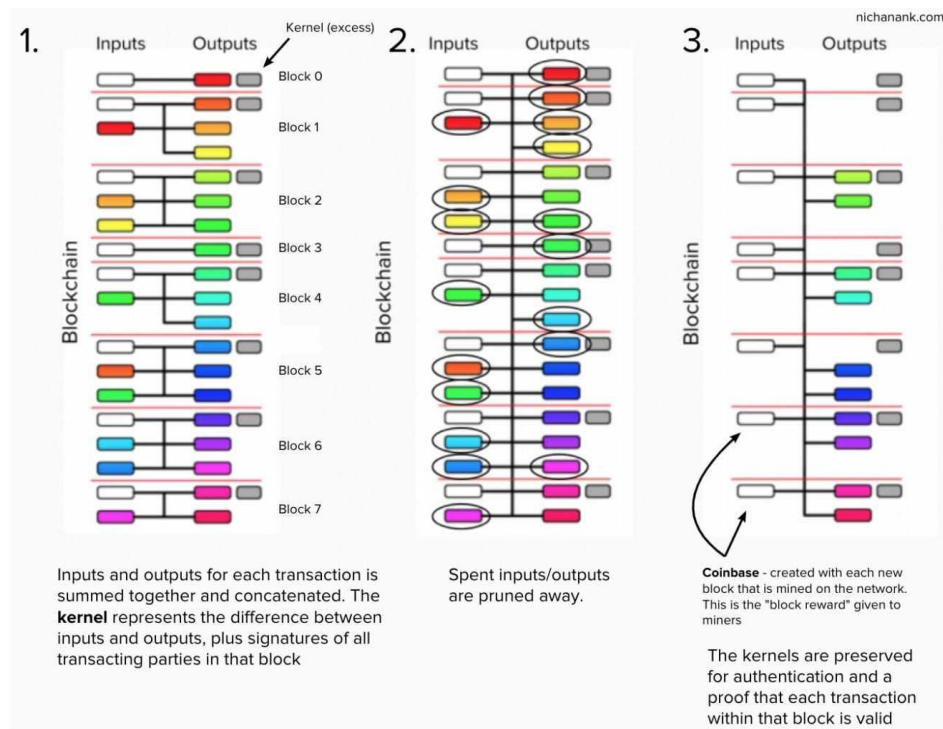
- Địa chỉ của người gửi
- Địa chỉ của người nhận
- Số tiền

Với Mimblewimble, ba thông tin này có thể được ẩn khỏi sổ cái blockchain công khai.

Giao thức không sử dụng cùng mô hình UTXO đầu vào/đầu ra được Bitcoin sử dụng. Thay vào đó, Mimblewimble sử dụng mô hình đa chữ ký cho tất cả đầu vào và đầu ra.

Các giao dịch sử dụng mô hình này được gọi là Giao dịch bí mật (CT) và chúng sử dụng Chương trình cam kết Pedersen, có nghĩa là không cần có địa chỉ. Thay vào đó, các giao dịch sử dụng “yếu tố mù” để mã hóa đầu vào và đầu ra của giao dịch, cùng với cả khóa công khai và khóa riêng của người gửi và người nhận. Yếu tố gây mù này được chia sẻ bí mật giữa hai bên tham gia giao dịch, giữ tính riêng tư của mạng rất cao.

Thay vì công khai đầu vào và đầu ra của mỗi giao dịch, Mimblewimble tổng hợp tất cả các bên giao dịch và xác minh toàn bộ tổng số tiền của mỗi chữ ký. Điều này dẫn đến việc không cần phải lưu trữ địa chỉ và số tiền riêng lẻ.



Hình 5.5 Hình ảnh minh họa cho một sơ đồ của mạng blockchain

### Mimblewimble

Hình ảnh mô tả các yếu tố sau của sơ đồ Mimblewimble:

–Các khối: Các khối là đơn vị cơ bản của dữ liệu trong blockchain Mimblewimble. Mỗi khối chứa một tập hợp các giao dịch.

–Inputs và outputs: Inputs và outputs là các tham số trong một giao dịch. Inputs là các khối trước đó được sử dụng để tạo ra giao dịch. Outputs là các khối mới được tạo ra bởi giao dịch.

–Kernel: Kernel là một giá trị đại diện cho sự khác biệt giữa inputs và outputs. Kernel được sử dụng để xác minh tính hợp lệ của giao dịch.

–Coinbase-created: Coinbase-created là một khối đặc biệt được tạo ra bởi các thợ đào. Coinbase-created chứa phần thưởng khai thác, được trả cho các thợ đào đã tạo ra khối đó.

### Cách thức hoạt động của sơ đồ

Sơ đồ Mimblewimble hoạt động như sau:

–Các thợ đào tạo ra các khối mới. Các khối mới được tạo ra bằng cách kết hợp các inputs và outputs từ các giao dịch.

–Các thợ đào tính toán kernel cho mỗi khối. Kernel được tính toán bằng cách trừ inputs từ outputs.

–Các thợ đào ký tên cho các khối của họ. Ký tên cho phép xác minh tính hợp lệ của các khối.

–Các thợ đào thêm các khối mới vào blockchain. Các khối mới được thêm vào blockchain theo thứ tự thời gian.

### **5.1.3.3 Mật mã của Mimblewimble**

Phương pháp mã hóa được đặt tên là Mật mã đường cong Elliptic (ECC) và đó là điều cho phép Mimblewimble đạt được các yêu cầu giao dịch blockchain trong việc xác minh số tiền giao dịch chính xác, cùng với bên gửi và nhận mà không tiết lộ công khai thông tin.

ECC dựa trên logarit rời rạc, thuật ngữ rời rạc dùng để chỉ một nhánh toán học xoay quanh một tập hợp các giá trị toán học rời rạc và sử dụng các chủ đề như xác suất và lý thuyết tập hợp.

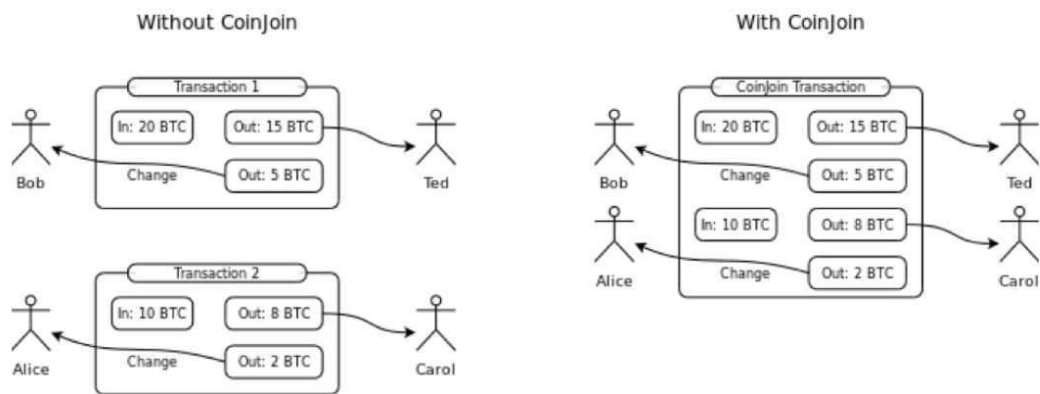
Điều này cũng tăng cường bảo mật giao thức nhưng không dừng lại ở đó. Mimblewimble cũng kết hợp các giao thức mã hóa sau:

Giao dịch bí mật (CT) - Đây là giao thức cũng được Monero sử dụng và che giấu giá trị của giao dịch.

Dandelion-Giao thức Dandelion ẩn danh tính của cả người gửi và người nhận.

CoinJoin- Giao thức CoinJoin khiến việc theo dõi dấu vết giao dịch trở nên rất khó khăn, nếu không muốn nói là không thể. Giao thức này cho phép các địa chỉ công khai của giao dịch được ẩn bằng cách kết hợp các khoản thanh toán từ nhiều người gửi khác nhau trong một giao dịch. CoinJoin cũng giúp thu gọn dữ liệu blockchain vì nó không còn yêu cầu lưu trữ tất cả dữ liệu giao dịch khác ngoài đầu vào và đầu ra.

Dưới đây là cái nhìn về giao dịch khi có và không có CoinJoin:



This coinjoin implementation is **interactive** as everybody who is transacting has to consent to it as per the protocol. If Alice wanted to make a coinjoin payment, she can find someone else who also wants to make a payment (e.g. Bob) and they can make a joint payment together. Externally, it is unclear who paid Ted and who paid Carol.

*Hình 5.6 Hình ảnh minh họa cho một giao dịch coinjoin trên mạng Monero.*

Các yếu tố chính của giao dịch:

- Các vòng: Các vòng là các nhóm người tham gia vào giao dịch coinjoin. Mỗi vòng có ít nhất 12 người tham gia, nhưng có thể có nhiều hơn.
- Các địa chỉ ẩn: Mỗi người tham gia trong một vòng có một địa chỉ ẩn. Địa chỉ ẩn là một địa chỉ duy nhất chỉ sử dụng một lần cho mỗi giao dịch.
- Các giao dịch: Mỗi người tham gia trong một vòng thực hiện một giao dịch. Các giao dịch này đều có cùng số tiền.

#### **Cách thức hoạt động của giao dịch:**

- Những người tham gia trong một vòng đồng ý tạo một giao dịch coinjoin.
- Mỗi người tham gia trong vòng tạo một địa chỉ ẩn.
- Mỗi người tham gia trong vòng gửi số tiền bằng nhau đến địa chỉ ẩn của một người tham gia khác trong vòng.
- Các giao dịch này được thêm vào blockchain Monero.

Tất cả đều hoạt động cùng nhau trong giao thức Mimblewimble để che giấu thông tin giao dịch đồng thời hỗ trợ khả năng mở rộng và bảo mật.

#### **Kết quả của giao dịch:**

- Người gửi và người nhận thực tế của mỗi giao dịch không thể được xác định từ blockchain.
- Số lượng tiền trong mỗi giao dịch không thể được xác định từ blockchain.

#### **5.1.3.4 Các tính năng cốt lõi của Mimbalewimble:**

**Ẩn danh:** Phần lớn các mạng blockchain có địa chỉ công cộng có thể theo dõi, công bố thông tin người gửi và người nhận cho bất kỳ bản dịch nào.

**Tính linh hoạt:** Thực tế là các tài sản khó theo dõi khiến các giao thức hỗ trợ Mimbalewimble và tài sản của chúng có tính linh hoạt hơn so với các chuỗi khối khác.

Vì người dùng có thể trao đổi bất kỳ loại tiền điện tử nào trên nền tảng mà không có nguy cơ mất mát hoặc khả năng tài sản tiền điện tử bị “làm bẩn” thông qua lịch sử hoạt động bất hợp pháp, điều này có thể dẫn đến các đồng tiền bị ràng buộc tội phạm có giá trị thấp hơn, nên tài sản được giao dịch trên Mimbalewimble được coi là dễ thay thế hơn.

#### **5.1.3.5 Ứng dụng thực tế:**

Mimbalewimble là một công nghệ tương đối mới, vì vậy nó vẫn đang được phát triển và chấp nhận. Tuy nhiên, có một số dự án đang sử dụng Mimbalewimble, bao gồm:

–Grin: Grin là một loại tiền điện tử tập trung vào quyền riêng tư sử dụng giao thức Mimbalewimble. Nó được phát hành lần đầu tiên vào năm 2016 và là dự án đầu tiên triển khai Mimbalewimble.

–Beam: Beam là một loại tiền điện tử tập trung vào quyền riêng tư khác sử dụng giao thức Mimbalewimble. Nó được phát hành lần đầu tiên vào năm 2019.

–Litecoin Mimbalewimble: Litecoin là một loại tiền điện tử phổ biến đã triển khai Mimbalewimble vào năm 2022.

Nhìn chung, Mimbalewimble là một công nghệ có tiềm năng được sử dụng trong nhiều ứng dụng khác nhau. Nó có thể thu hút được sự quan tâm của nhiều người dùng, bao gồm những người tìm kiếm quyền riêng tư, tính linh hoạt và tính có thể hoán đổi trong các giao dịch của họ.

#### **5.1.3.6 Ưu, nhược điểm của Mimbalewimble**

##### **Ưu điểm**

–Tính riêng tư: Mimbalewimble sử dụng một số kỹ thuật để cải thiện tính riêng tư của các giao dịch, bao gồm:

–Sự bí mật của địa chỉ: Địa chỉ của người gửi và người nhận giao dịch không được hiển thị công khai.

–Sự bí mật của số dư: Số dư của một người dùng không thể được xác định từ blockchain.

–Sự bí mật của lịch sử giao dịch: Lịch sử giao dịch của một người dùng không thể được xác định từ blockchain.

–Khả năng mở rộng: Mimblewimble được thiết kế để cải thiện khả năng mở rộng của blockchain, bằng cách giảm kích thước của các khối. Điều này làm cho việc xác minh các giao dịch nhanh hơn và hiệu quả hơn.

–Bảo mật: Mimblewimble sử dụng một số kỹ thuật bảo mật để cải thiện tính bảo mật của blockchain, bao gồm:

–Hàm băm mật mã: Các giao dịch được ký bằng chữ ký số, được tạo ra bằng cách sử dụng hàm băm mật mã.

–Khóa riêng tư: Mimblewimble sử dụng khóa riêng tư để tạo ra các giao dịch. Khóa riêng tư là bí mật và không được chia sẻ với bất kỳ ai.

### **Nhược điểm**

–Thông lượng giao dịch dài hơn- Các hệ thống hỗ trợ Giao dịch bí mật thường có tốc độ giao dịch thấp hơn so với tốc độ giao dịch có sẵn từ các mạng như Ripple (XRP) và mạng PoS như Solana và Cardano do kích thước dữ liệu của Giao dịch bí mật.

–Sự phụ thuộc vào chữ ký số- Vì Mimblewimble phụ thuộc vào chữ ký số, điều này làm cho giao thức dễ bị tấn công hơn trước các cuộc tấn công máy tính lượng tử theo lý thuyết.

## **5.2. So sánh các mô hình quyền riêng tư:**

### **5.2.1 Mimblewimble vs Monero**

Mimblewimble và Monero là hai giao thức blockchain được thiết kế để cải thiện tính riêng tư và khả năng mở rộng. Tuy nhiên, giữa hai giao thức này có một số điểm khác biệt đáng chú ý.

#### **Tính riêng tư**

–Mimblewimble và Monero đều sử dụng giao dịch bí mật để bảo vệ quyền riêng tư của người dùng. Giao dịch bí mật che giấu số tiền được chuyển, người gửi và người nhận khỏi công chúng.

–Tuy nhiên, Mimblewimble có một số lợi thế về tính riêng tư so với Monero. Thứ nhất, Mimblewimble không yêu cầu người dùng thêm các đồng xu “chim mồi” vào mỗi giao dịch. Điều này giúp giảm kích thước của các giao dịch và blockchain, đồng thời cải thiện khả năng mở rộng. Thứ hai, Mimblewimble sử dụng một thuật toán

giao dịch bí mật khác với Monero. Thuật toán này được thiết kế để chống lại các cuộc tấn công từ máy tính lượng tử.

### **Khả năng mở rộng**

Mimblewimble và Monero đều được thiết kế để cải thiện khả năng mở rộng của blockchain. Mimblewimble đạt được điều này bằng cách sử dụng một số kỹ thuật, bao gồm:

- Giao dịch bí mật: Giao dịch bí mật giúp giảm kích thước của các giao dịch và blockchain.

- Kết hợp giao dịch: Mimblewimble kết hợp các giao dịch lại với nhau, giúp giảm kích thước của blockchain.

- Tổng hợp chữ ký một chiều (OWAS): OWAS cho phép xác minh các giao dịch mà không cần lưu trữ tất cả các giao dịch trước đó trong blockchain.

Monero cũng sử dụng một số kỹ thuật để cải thiện khả năng mở rộng, bao gồm:

- Tăng kích thước khối: Monero đã tăng kích thước khối của mình từ 128 kilobyte lên 1.750 kilobyte. Điều này giúp tăng tốc độ xử lý giao dịch.

- RingCT: RingCT là một công nghệ được sử dụng trong Monero để bảo vệ quyền riêng tư của người dùng khi họ thực hiện các giao dịch. RingCT cũng giúp giảm kích thước của các giao dịch.\*\*

Nhìn chung, Mimblewimble có lợi thế về khả năng mở rộng so với Monero. Mimblewimble sử dụng các kỹ thuật tiên tiến hơn để giảm kích thước của các giao dịch và blockchain.

Dưới đây là bảng so sánh tóm tắt các tính năng chính của Mimblewimble và Monero:

Tính năng	Mimblewimble	Monero
Tính riêng tư	Tốt hơn	Tốt
Khả năng mở rộng	Tốt hơn	Khá tốt
Tính năng khác	Cut-Through, PoW	RingCT, tăng kích thước khối, tính năng Ring Signatures

*Hình 5.7 Bảng so sánh tóm tắt các tính năng chính của Mimblewimble và Monero*



## **Tính năng khác**

### **Mimblewimble có các tính năng sau:**

–Cut-Through: Cut-Through là một cơ chế giúp giảm kích thước của blockchain bằng cách loại bỏ các giao dịch đã được xác minh khỏi blockchain.

–Bằng chứng công việc (PoW): Mimblewimble sử dụng PoW để xác minh các giao dịch.

### **Monero có các tính năng sau:**

–RingCT: RingCT là một công nghệ được sử dụng trong Monero để bảo vệ quyền riêng tư của người dùng khi họ thực hiện các giao dịch.

–Tăng kích thước khối: Monero đã tăng kích thước khối của mình từ 128 kilobyte lên 1.750 kilobyte. Điều này giúp tăng tốc độ xử lý giao dịch.

–Tính năng Ring Signatures: Ring Signatures là một công nghệ được sử dụng trong Monero để bảo vệ quyền riêng tư của người dùng khi họ thực hiện các giao dịch.

## **Kết luận**

Tóm lại, Mimblewimble và Monero đều là các mô hình quyền riêng tư có tiềm năng. Tuy nhiên, Mimblewimble có một số lợi thế so với Monero về tính riêng tư, khả năng mở rộng và khả năng chống lại các cuộc tấn công từ máy tính lượng tử.

### **5.2.2 So sánh Zero-knowledge Proof với Ring Signatures**

Zero-knowledge Proof (ZKP) và Ring Signature là hai kỹ thuật mật mã được sử dụng để tăng cường tính riêng tư và bảo mật trong nhiều ứng dụng, bao gồm các hệ thống dựa trên blockchain. Mặc dù cả hai đều phục vụ những mục đích tương tự, nhưng chúng khác nhau về cơ chế cơ bản, khả năng ứng dụng và những điểm mạnh và điểm yếu tổng thể.

#### **Zero-knowledge Proof (ZKP)**

ZKP cho phép người chứng minh thuyết phục người xác minh về một tuyên bố mà không tiết lộ bất kỳ thông tin bổ sung nào ngoài tính hợp lệ của tuyên bố đó. Người chứng minh chứng minh kiến thức về một bí mật hoặc điều kiện nhất định mà không tiết lộ bí mật đó. Điều này cho phép xác thực và xác minh an toàn mà không làm rò rỉ thông tin nhạy cảm.

Ví dụ: Giả sử bạn muốn chứng minh cho ai đó rằng bạn biết số 23. Bạn có thể làm điều này bằng cách sử dụng ZKP. Bạn sẽ tạo ra một số ngẫu nhiên và sau đó sử

dùng ZKP để chứng minh cho người xác minh rằng bạn biết số 23 mà không cần tiết lộ số đó.

### Ring Signature

Mặt khác, ring signatures tập trung vào tính ẩn danh bằng cách che giấu danh tính của người ký trong một nhóm các người ký tiềm năng. Khi một giao dịch được ký bằng chữ ký vòng, sẽ không thể xác định được thành viên nào trong vòng thực sự đã ký giao dịch. Điều này cung cấp tính ẩn danh mạnh mẽ cho người ký trong khi vẫn duy trì tính toàn vẹn của giao dịch.

Ví dụ:

Giả sử bạn muốn thực hiện một giao dịch trên blockchain. Bạn có thể sử dụng ring signature để che giấu danh tính của mình. Bạn sẽ tạo ra một vòng gồm 10 người ký tiềm năng, bao gồm cả bạn. Bạn sẽ sử dụng chữ ký vòng để ký giao dịch, nhưng chỉ bạn mới biết bạn là người ký thực sự.

### So sánh ZKP và Ring Signature

Dưới đây là bảng so sánh ZKP và ring signatures về các khía cạnh chính của chúng:

Tính năng	Zero-knowledge Proof (ZKP)	Ring Signature
Mục đích	Chứng minh kiến thức mà không tiết lộ bí mật	Ẩn danh người ký trong nhóm
Cơ chế	Các chứng minh toán học	Các kỹ thuật mật mã như cam kết Pedersen
Khả năng ứng dụng	Phạm vi ứng dụng rộng hơn, bao gồm xác minh danh tính, tính toàn vẹn dữ liệu và bỏ phiếu an toàn	Chủ yếu tập trung vào tính riêng tư của giao dịch trong các hệ thống blockchain
Điểm mạnh	Bảo vệ quyền riêng tư mạnh mẽ, xác minh không tương tác, có thể xác minh mà không cần tin tưởng vào người chứng minh	Tính ẩn danh cao cho người ký, tính toàn vẹn giao dịch vẫn được bảo toàn
Điểm yếu	Tính toán tốn kém, có thể cần các thuật toán chuyên biệt	Có khả năng tấn công đồng lõa, tập hợp ẩn danh cần đủ lớn

*Hình 5.8. Bảng so sánh ZKP và Ring Signature*

### Ứng dụng của ZKP và Ring Signature

ZKP đã tìm thấy ứng dụng trong nhiều lĩnh vực, bao gồm:

–Blockchain: ZKP được sử dụng cho chứng minh tính ẩn danh, chứng minh kiến thức và chứng minh ngắn gọn không tương tác về kiến thức (zk-SNARKs) trong các hệ thống blockchain.

–Bỏ phiếu an toàn: ZKP cho phép các hệ thống bỏ phiếu có thể xác minh và an toàn, nơi cử tri có thể chứng minh phiếu bầu của họ mà không tiết lộ lựa chọn của họ.

–Tính toàn vẹn dữ liệu: ZKP có thể được sử dụng để chứng minh tính toàn vẹn dữ liệu mà không tiết lộ dữ liệu đó, đảm bảo tính bảo mật dữ liệu trong khi vẫn duy trì niềm tin.

Ring signatures, chủ yếu được sử dụng trong các hệ thống blockchain, cung cấp tính ẩn danh cho các giao dịch, đặc biệt là trong các loại tiền điện tử tập trung vào quyền riêng tư như Monero và Beam. Chúng giúp che giấu danh tính của người gửi hoặc người nhận tiền, nâng cao tính riêng tư của giao dịch.

### **Kết luận**

ZKP và Ring signatures đều là những kỹ thuật mật mã có giá trị giải quyết các mối quan tâm về quyền riêng tư theo những cách khác nhau. ZKP cung cấp phạm vi ứng dụng rộng hơn và bảo vệ quyền riêng tư mạnh mẽ hơn, trong khi ring signatures tập trung cụ thể vào tính ẩn danh của giao dịch trong các hệ thống blockchain. Sự lựa chọn giữa hai loại phụ

## CHƯƠNG 6: TRIỂN KHAI THỰC NGHIỆM

### 6.1 Thực nghiệm cách hoạt động của blockchain và mã hóa bảo mật bằng hàm băm (hash)

Bảng demo dựa trên nghiên cứu của Mr. Anders Brownworth, giảng viên từng tham gia nhiều khóa giảng dạy và hội nghị về blockchain ở đại học MIT, Yale,...

#### 6.1.1 Hàm băm (SHA256 Hash)

SHA256 Hash



Data:	I'm Trang
Hash:	83bc0579c5b0c14f399d75e4d0f94825d0e08c667abc59dd85fd7ba017b83d54

Hình 6.1 Hình ảnh hàm băm trong bản demo

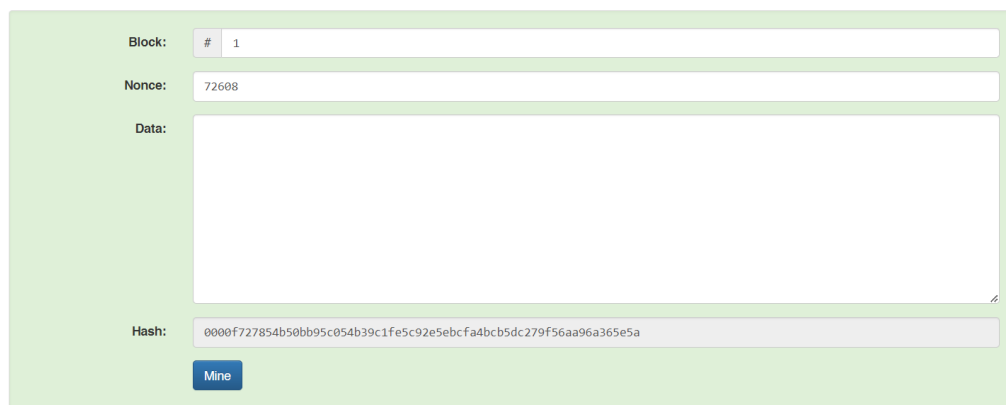
Đây được gọi là hàm băm, nó giống như một chuỗi các kí tự ngẫu nhiên. Về cơ bản nó là dấu vân tay của dữ liệu kỹ thuật số. Khi ta nhập dữ liệu vào Data ta thì hàm băm sẽ thay đổi. Nếu ta nhập một dãy dữ liệu giống nhau sẽ nhận được hàm băm giống nhau của dãy ký tự đó.

#### 6.1.2 Block

Về cơ bản nó cũng giống như hàm băm, nó được chia thành ba phần.

- Phần thứ nhất block nó là một dạng con số và ta đặt là block 1.
- Phần thứ hai None là con số được dùng một lần
- Phần thứ ba Data dữ liệu được nhập

Block



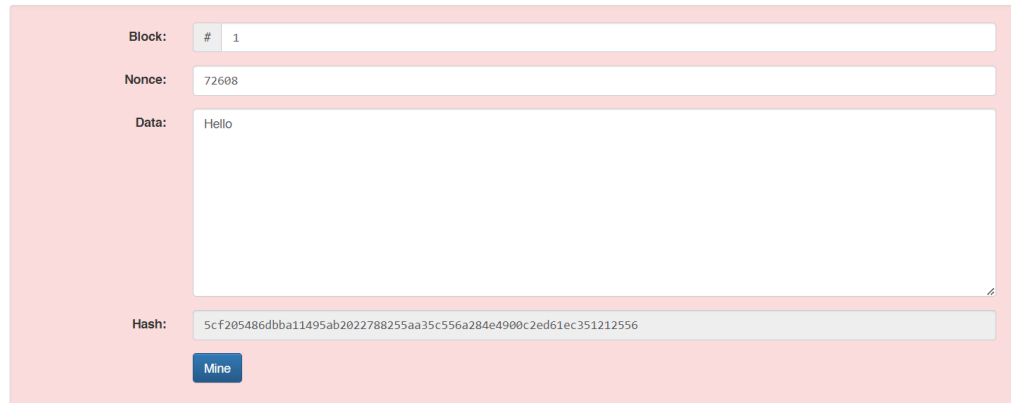
Block:	# 1
Nonce:	72608
Data:	
Hash:	0000f727854b50bb95c054b39c1fe5c92e5ebcf44bcb5dc279f56aa96a365e5a
<button>Mine</button>	

Hình 6.2 Hình ảnh minh họa block trong bản demo

Hàm băm bao gồm tất cả các thông tin ở trên và nó bắt đầu bằng bốn con số 0 (đây là block đã được xác nhận)

Khi nhập Data khác ta thấy giao diện chuyển sang màu đỏ và hàm băm không còn bắt đầu bằng bốn số 0 nữa. Qua đó ta thấy khối block này cùng những thông tin bên trong không hợp lệ và đây là block không được ký dấu

Block



Block: # 1

Nonce: 72608

Data: Hello

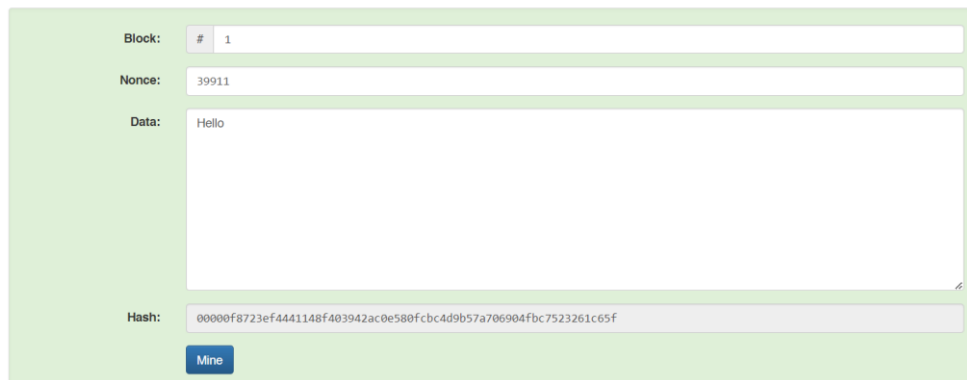
Hash: 5cf205486dbba11495ab2022788255aa35c556a284e4900c2ed61ec351212556

Mine

*Hình 6.3 Hình ảnh demo block*

Số none là số mà ta có thể thiết lập để tìm ra một số phù hợp để hàm băm xuất hiện lại với bắt đầu là bốn số 0. Ta dùng nút Mine( đại diện cho lệnh đào), khi nhấn nút này thì sẽ bắt đầu chạy tất cả các số bắt đầu từ số 1 cũng có nghĩa là quá trình khai thác mỏ bắt đầu.

Block



Block: # 1

Nonce: 39911

Data: Hello

Hash: 00000f8723ef4441148f403942ac0e580fcbcd49b57a706904fbc7523261c65f

Mine

*Hình 6.4 Kết quả đào khi nhấn nút Mine*

Theo đó với giá trị None dừng lại ở số 39911 và hàm băm đã đạt được bốn số 0 ở đầu thì block này đã được xác nhận.

### 6.1.3 Blockchain

Blockchain là một chuỗi của các khối block, ở đây có 5 khối, Prev ở đây là mã của khối trước đó

Block đầu tiên là một dãy số 0 do trước nó không có hàm băm nào.

## Blockchain

Block: #	Nonce	Data	Prev	Hash
1	11316		00	000015783b764259d382017d91a36d206d0600e2cbb3567748f
2	35230		000015783b764259d382017d91a36d206d0600e2cbb3567748f	000012fa9b916eb9078fd98a7864e697ae83ed54f5146bd844
3	12937		000012fa9b916eb9078fd98a7864e697ae83ed54f5146bd844	0000b9015ce2a08b61216ba5a0778545

Hình 6.5 Hình ảnh demo cho một blockchain

Nếu ta thay đổi data của một block bất kỳ trừ block đầu tiên thì khối thay đổi đó sẽ không hợp lệ

Ví dụ khi ta thay đổi giá trị ở block thứ 3 nhưng nó không hợp lệ sẽ kéo theo các block phía sau cũng không hợp lệ.

Block: #	Nonce	Data	Prev	Hash
3	12937	Trang	000012fa9b916eb9078fd98a7864e697ae83ed54f5146bd844	bc3caad68ed2842c7877a95c1d822ccc308bdedc34391f4568e
4	35990		bc3caad68ed2842c7877a95c1d822ccc308bdedc34391f4568e	285977ed43c91da49a5ff7ebc3bb4df2d548425a847d46aa127
5	12937		000012fa9b916eb9078fd98a7864e697ae83ed54f5146bd844	0000b9015ce2a08b61216ba5a0778545

Hình 6.6 Hình ảnh các block không hợp lệ

Nếu muốn thay đổi chuỗi blockchain này thì ta sẽ thay đổi ở khối cuối, sau đó nhấn nút Mine để bắt đầu quá trình đào

<b>Block:</b>	# 5
<b>Nonce:</b>	12537
<b>Data:</b>	Trang
<b>Prev:</b>	0000ae8bbc96cf89c68be6e10a865cc47c6c48a9ebec3c6cad7
<b>Hash:</b>	000003cdcbd1c6c30bb4cb136411a4eb875981e5253da4165a3
<button>Mine</button>	

*Hình 6.7 Hình ảnh block thứ năm đã được xác thực thành công*

## **CHƯƠNG 7: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**

### **7.1. Những điều làm được**

- Đã tìm hiểu và nắm được các kiến thức cơ bản về blockchain
- Nêu được các giải pháp để bảo đảm an toàn và quyền riêng tư trong các giao dịch blockchain
- Đã so sánh đánh giá và phân tích một số mô hình quyền riêng tư trong blockchain
- Có thực nghiệm để hiểu về quy trình hoạt động cũng như công nghệ mã hóa của blockchain

### **7.2 Những điều chưa làm được**

- Chưa tìm hiểu toàn bộ các vấn đề bảo mật và an toàn trong blockchain
- Mới nêu được một vài mô hình về quyền riêng tư phổ biến
- Đề tài còn mang tính lý thuyết nhiều

### **7.3 Hướng phát triển**

- Nghiên cứu sâu hơn nữa các khía cạnh về blockchain
- Xây dựng và ứng dụng công nghệ blockchain vào đời sống thực tế



## TÀI LIỆU THAM KHẢO

- [1] Blockchain là gì? Hoạt động của Blockchain như thế nào? Ứng dụng ra sao?  
<https://vbpo.com.vn/news/blog-40/blockchain-la-gi-hoat-dong-cua-blockchain-nhu-the-nao-ung-dung-ra-sao>
- [2] Blockchain là gì? - Thông tin từ A-Z về nền tảng này- Tác giả: Kim Anh  
“<https://luatvietnam.vn/linh-vuc-khac/blockchain-la-gi-883-91342-article.html>”
- [3] Các vụ tấn công crypto trong tháng 11 đã lấy đi 340 triệu USD.  
“<https://cacvutancongrongthang11>”
- [4] “Vụ tấn công Kyber Elastic lấy đi 47 triệu USD được chuẩn bị rất công phu”,  
tác giả Minh Sơn bài đăng ngày 29/11/2023 16:43 trên trang VietNamPlus.  
<https://www.vietnamplus.vn/vu-tan-cong-kyber-elastic-lay-di-47-trieu-usd-duoc-chuan-bi-rat-cong-phu-post910704.vnp>
- [5] Nền tảng blockchain riêng tư: Lợi ích và lựa chọn hàng đầu - Nguyên tắc cơ bản về Hyperledger.  
<https://vulehuan.com/vi/blog/2023/03/nen-tang-blockchain-rieng-tu-loi-ich-va-lua-chon-hang-dau-nguyen-tac-co-ban-ve-hyperledger-64680f9664ac40ae37cdf48f.html>
- [6] Blockchain Là Gì Và Nó Hoạt Động Như Thế Nào,  
“<https://academy.binance.com/vi/articles/what-is-blockchain-technology-a-comprehensive-guide-for-beginners>”
- [7] Blockchain security: What keeps your transaction data safe? By Curtis Miles, December 12, 2017, “[Blockchain security: What keeps your transaction data safe? - IBM Blog](#)”
- [8] What is Blockchain Authentication?, “[What is Blockchain Authentication? - GeeksforGeeks](#)”
- [9] Thuật toán đồng thuận Blockchain là gì? “<https://coin98.net/thuat-toan-dong-thuan-blockchain-la-gi>”
- [10] Tích hợp AI và Blockchain để bảo vệ quyền riêng tư, “[Tích hợp AI và Blockchain để bảo vệ quyền riêng tư - Unite.AI](#)”
- [11] What is Mimblewimble, What Does it Do, and Why You should Care, By Tayler McCracken, <https://www.coinbureau.com/education/what-is-mimblewimble/>