HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Lê Trọng Quý

NGHIÊN CỨU CHỮ KÝ SỐ NGƯỠNG VÀ KHẢ NĂNG ỨNG DỤNG TRONG CÔNG NGHỆ BLOCKCHAIN

Chuyên ngành: Hệ thống thông tin
Mã số: 8.48.01.04

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI - 2022

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: TS. ĐẶNG MINH TUẤN

Phản biện 1: TS. NGÔ QUỐC DŨNG

Phản biện 2: PGS. TS. ĐỖ TRUNG TUẤN

Luận văn được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính viễn thông

Vào lúc: 10 giờ 00 ngày 02 tháng 7 năm 2022

Có thể tìm hiểu luận văn tại

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

PHẦN MỞ ĐẦU

1. Lý do chọn đề tài

Blockchain hiện đang là xu thế công nghệ của thời đại, đang được áp dụng rất nhiều ngành nghề và lĩnh vực khác nhau. Có những quốc gia hay doanh nghiệp lớn bỏ rất nhiều tiền và thời gian để đầu tư và nghiên cứu công nghệ Blockchain bởi tính ứng dụng cao và độ bảo mật tuyệt vời của nó.

Chữ ký số là một cơ chế mật mã hóa được sử dụng để kiểm tra độ chân thực và tính toàn vẹn của dữ liệu số, có thể xem nó như là một phiên bản kỹ thuật số của các chữ ký bằng tay thông thường, nhưng với mức độ phức tạp và bảo mật cao hơn.

Lược đồ Chữ ký Ngưỡng (Threshold Signature Scheme - TSS) là một thuật toán mã hóa, được sử dụng để tạo khóa phân tán và chữ ký. Sử dụng TSS trên các máy của người dùng (máy khách) Blockchain là một mô hình mới có thể mang đến nhiều lợi ích, đặc biệt là trong lĩnh vực bảo mật. Chữ ký ngưỡng có thể nâng cao khả năng bảo mật của hệ thống trong khi vẫn duy trì tính phân tán của Blockchain.

Vì vậy tôi xin chọn đề tài **"Nghiên cứu chữ ký số ngưỡng và khả năng ứng dụng trong công nghệ Blockchain"** làm luận văn tốt nghiệp trình độ Thạc sĩ của mình.

2. Tổng quan về vấn đề nghiên cứu

Với việc ứng dụng chữ ký số ngưỡng vào, chúng ta sẽ có một tập hợp các bên cùng tham gia vào quá trình tính toán khóa công khai, mỗi bên nắm giữ một phần bí mật của khóa cá nhân (các phần thông tin bí mật được giữ kín với các bên còn lại).

3. Mục đích nghiên cứu

Bản chất của Blockchain là tính phi tập trung và ý tưởng là chia sẻ sự tin tưởng giữa các bên tham gia trong hệ thống.

Lược đồ chữ ký ngưỡng là giải pháp cho vấn đề nói trên. Mục tiêu nghiên cứu cụ thể được trình bày trong luận văn như sau:

- Nghiên cứu về chữ ký số ngưỡng, công nghệ Blockchain.
- Ứng dụng chữ ký số ngưỡng vào công nghệ Blockchain trong các giao dịch tài chính.
- Đánh giá tính khả thi.

4. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu: Chữ ký số ngưỡng và công nghệ Blockchain.

Phạm vi nghiên cứu của luận văn: Cơ sở lý thuyết liên quan tới chữ ký số, chữ ký số ngưỡng, công nghệ Blockchain và ứng dụng chữ ký số ngưỡng trong công nghệ Blockchain.

5. Phương pháp nghiên cứu

Phương pháp nghiên cứu lý thuyết

- Nghiên cứu về chữ ký số, chữ ký số ngưỡng và công nghệ Blockchain.
- Một số thuật toán đồng thuận được ứng dụng trong Blockchain và ưu điểm, nhược điểm của chúng.
- Sử dụng các bài báo, tạp chí khoa học đã công bố và được công nhận bởi hội đồng khoa học.

Phương pháp nghiên cứu thực nghiệm

- Triển khai chữ ký số ngưỡng trong công nghệ Blockchain.

PHẦN NỘI DUNG

CHƯƠNG 1: TỔNG QUAN VỀ CHỮ KÝ SỐ VÀ CÔNG NGHỆ BLOCKCHAIN

1.1. Tổng quan về chữ ký số

1.1.1. Chữ ký số và các loại chữ ký số

Chữ ký số được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng, theo đó người có được thông điệp dữ liệu ban đầu và khoá công khai của người ký có thể xác định được chính xác.

1.1.2. Chữ ký số tập thể

Mô hình chữ ký số tập thể được đề xuất ở đây cơ bản dựa trên cấu trúc của một PKI (Public Key Infrastructure) truyền thống nhằm bảo đảm các chức năng về chứng thực số cho đối tượng áp dụng là các tổ chức có tư cách pháp nhân trong xã hội (đơn vị hành chính, cơ quan nhà nước, doanh nghiệp...).

1.1.3. Chữ ký số ngưỡng

Lược đồ Chữ ký Ngưỡng (Threshold Signature Scheme - TSS) là một thuật toán mã hóa bậc thấp đã có từ lâu, được sử dụng để tạo khóa phân tán và chữ ký. Từ thập niên 70, ngày càng nhiều hệ thống Internet sử dụng công nghệ mã hóa bất đối xứng, hay còn được gọi là Công nghệ mã khóa công khai (Public key cryptography - PKC). PKC sử dụng hai khóa: khóa công khai và khóa cá nhân. Nếu khóa công khai là khóa có thể được công khai và bất kỳ ai cũng có thể sử dụng nó, thì khóa cá nhân là một thông tin bí mật và đại diện cho tính bảo mật của hệ thống mã hóa này.

1.1.4. Đa chữ ký

Về khái niệm, điều này giải thích tại sao ví đa chữ ký trở thành cách tốt nhất để bảo vệ tiền của bạn, đặc biệt là khi bạn đang điều hành hoặc bắt đầu một cộng đồng hoặc dự án khởi động, và bạn lo lắng về việc đặt tất cả quyền lực để kiểm soát tiền trong một người.

Cách thức hoạt động

Để đơn giản, chúng ta có thể hình dung nó như một hộp tiền gửi an toàn có hai khóa và hai chìa khóa. Một chìa khóa được giữ bởi Alice và một chìa khóa khác được giữ bởi Bob. Cách duy nhất có thể mở hộp là phải có cả hai chìa khóa cùng một lúc, vì vậy, một người không thể mở hộp mà không có sự đồng ý của người khác.

Đơn chìa khóa và đa chữ ký

Thông thường, Bitcoin được lưu trữ trong một địa chỉ tiêu chuẩn có một chìa khóa, có nghĩa là bất kỳ ai giữ chìa khóa cá nhân tương ứng đều có thể truy cập vào quỹ. Điều này có nghĩa là chỉ cần một chìa khóa để ký các giao dịch, và bất kỳ ai có chìa khóa cá nhân đều có thể chuyển coin theo ý muốn mà không cần có sự cho phép của bất kỳ ai khác.

Các tính năng cơ bản của ví đa chữ ký

Khi tạo ra một trong những ví này, bạn có thể chọn số chữ ký sẽ được sử dụng hoặc ủy quyền, và số lượng tối thiểu cần thiết để cho phép một giao dịch. 2 trong số 3 ví là ví đa chữ cái phổ biến nhất được tạo. Trong trường hợp này, chiếc ví yêu cầu ba chữ ký, nhưng chỉ cần hai chữ ký để cho phép một giao dịch.

1.2. Công nghệ Blockchain

Blockchain là một loại cơ sở dữ liệu, thông tin được lưu trữ trong các khối và liên kết với nhau. Thông tin trong khối, các liên kết sẽ được mã hóa đồng thời có thể mở rộng theo thời gian. Mỗi khi một thông tin hoặc giao dịch mới xảy ra, thông tin cũ sẽ không bị mất đi mà thay vào đó, thông tin mới sẽ được lưu vào một khối mới và lần lượt được nối vào khối cũ để tạo thành một chuỗi mới.

1.2.1. Những đặc điểm chính của Blockchain

Blockchain ra đời để giải quyết những hạn chế, rủi ro phát sinh của hệ thống giao dịch thông thường. Chính vì vậy mà công nghệ Blockchain có những đặc điểm nổi bật sau:

- Phân quyền: Blockchain hoạt động độc lập theo các thuật toán máy tính và hoàn toàn không chịu sự kiểm soát của bất kỳ tổ chức nào.
- Phân tán**:** Các khối chứa cùng một dữ liệu, nhưng được phân tán ở nhiều nơi khác nhau. Vì vậy, nếu một nơi nào đó bị mất hoặc bị hỏng, dữ liệu vẫn nằm trên Blockchain.
- Bất biến**:** Một khi dữ liệu được ghi vào khối của chuỗi khối, nó không thể bị thay đổi hoặc sửa đổi.
- Bảo mật: Chỉ người nắm giữ khóa riêng tư (private key) mới có thể truy cập vào dữ liệu bên trong Blockchain và truy xuất dữ liệu đó.
- Minh bạch: Các giao dịch trong chuỗi khối được ghi lại và mọi người đều có thể xem các giao dịch này. 1.2.2. Cấu trúc và cơ chế hoạt động

Blockchain bao gồm 2 phần chính:

Khối (Block): các khối này chứa dữ liệu

Chuỗi (Chain): tức là các khối trên liên kết với nhau tạo thành chuỗi

Hoạt động của Blockchain được diễn ra như sau:

Đầu tiên, thông tin giao dịch của bạn sẽ được ghi lại trên hệ thống để tạo bản ghi hồ sơ. Sau đó, các máy tính trong hệ thống (được gọi là Node) xác minh xem bản ghi của bạn có hợp lệ hay không theo thuật toán đồng thuận trên Blockchain.

1.2.3. Ứng dụng của Blockchain trong thương mại điện tử

Ứng dụng Blockchain trong bảo mật & bảo vệ dữ liệu

Quản lý dữ liệu bằng cách sử dụng blockchain có thể giúp tránh rủi ro rò rỉ dữ liệu do sử dụng công nghệ DLT (Sổ cái phân tán) hoặc các cuộc tấn công mạng. Công nghệ blockchain cũng sẽ giúp bảo mật trang web Thương mại điện tử của bạn trước các cuộc tấn công mạng DDoS.

Hệ thống thanh toán tốt hơn

Blockchain trở nên nổi bật với sự xuất hiện của nhiều loại tiền điện tử khác nhau như Bitcoin và Ethereum. Trong vòng nhiều năm, tiền điện tử đang được coi là một giải pháp thay thế cho các loại tiền tệ truyền thống. Nhiều quốc gia trên thế giới ban đầu phản đối việc sử dụng tiền điện tử hiện đang chấp nhận nó.

Quản lý chuỗi cung ứng tốt hơn

Sử dụng blockchain trong chuỗi cung ứng cũng có thể giảm bớt các thủ tục giấy tờ thủ công cần thiết trong một số trường hợp. Nó có thể làm giảm nhu cầu về hóa đơn giấy, thay vào đó, giá trị của lô hàng có thể được xác minh bằng cách sử dụng blockchain.

Quản lý hàng tồn kho tốt hơn

Ứng dụng Blockchain cũng có thể giúp cải thiện quản lý hàng tồn kho bằng cách kết nối các nhà kho, nhà sản xuất, nhà cung cấp, nhà phân phối và nhà bán lẻ trên một nền tảng. Blockchain có thể giúp chia sẻ từng bản ghi của giao dịch trong mạng của người bán Thương mại điện tử. Điều này sẽ mang lại sự minh bạch giữa nhà cung cấp và người bán để hiểu rõ hơn về nhu cầu sản xuất sản phẩm theo nhu cầu.

Cơ hội mới trong thương mại điện tử

Với sự phổ biến của blockchain và tiền điện tử, nhiều cơ hội mới đã xuất hiện. NFT đã tạo ra doanh thu 2,5 tỷ đô la chỉ trong nửa đầu năm 2021. Việc ứng dụng blockchain đã mở ra nhiều cơ hội mới chưa từng được nghĩ đến trong vài năm trở lại đây. Khối lượng do các chợ này tạo ra nhiều hơn nhiều so với các cửa hàng Thương mại điện tử truyền thống.

1.3. Một số thuật toán đồng thuận trong công nghệ Blockchain

1.3.1. Thuật toán đồng thuận là gì

Thuật toán đồng thuận (Consensus) blockchain được hiểu là cơ chế giúp cho các nút phân tán, tất cả đều đạt đến sự đồng thuận trong hệ thống. Bằng cách này, các thuật toán đồng thuận đạt được độ tin cậy trong mạng Blockchain và thiết lập sự tin cậy giữa các đồng nghiệp chưa biết trong môi trường máy tính phân tán. Về cơ bản, giao thức đồng thuận đảm bảo rằng mọi khối mới được thêm vào Blockchain là phiên bản duy nhất của sự thật được tất cả các nút trong Blockchain đồng ý.

Cách thức hoạt động của thuật toán đồng thuận:

Blockchain quy tụ nhiều người tham gia trên cả thế giới và đặc biệt không có sự quản lý của bất kỳ cơ quan trung ương nào cả. Và để thay thế, Blockchain tồn tại những người đóng vai trò xác minh các giao dịch và thợ mỏ tạo ra các khối mới trên mạng lưới. Để việc diễn ra một cách minh bạch, chính xác và thuyết phục. Thuật toán đồng thuận ra đời.

1.3.2. Các loại thuật toán đồng thuận

Bằng chứng công việc PoW – Proof of Work:

Là thuật toán đồng thuận thành công đầu tiên cho công nghệ blockchain. Proof of Work đòi hỏi những người tham gia thực hiện các công việc chuyên sâu về tính toán nhưng lại có thể được xác minh một cách dễ dàng bởi những người khác trong mạng.

Bằng chứng cổ phần PoS – Proof of Stake:

Hiện nay có rất nhiều đồng cryptocurrency được tạo ra và sử dụng thuật toán đồng thuận Proof of Stake (PoS). Proof of Stake yêu cầu người tham gia "đặt cọc" một phần những đồng cryptocurrency mà họ nắm giữ trong mạng lưới để xác minh các giao dịch

Bằng chứng ủy quyền cổ phần DPoS – Delegated Proof of Stake:

Trong DPoS, thay vì phải đặt cọc để xác thực giao dịch, những người nắm giữ token sẽ tiến hàng bỏ phiếu cho một nhóm được chọn để thực hiện vai trò xác nhận các giao dịch.

Cơ chế đồng thuận chống gian lận BFT – Byzantine Fault Tolerance:

BFT là một thuật toán đồng thuận có tính chất kỹ thuật cao. Nói chung, các thuật toán đồng thuận BFT được sử dụng bởi các dự án cryptocurrency mà cho phép những người thực hiện xác minh quản lý mỗi trạng thái của một chuỗi và chia sẻ các thông điệp giữa mỗi chuỗi khác để có được những bản ghi giao dịch chính xác và đảm bảo sự trung thực.

1.4. Ứng dụng chữ ký số ngưỡng vào công nghệ Blockchain trong các giao dịch tài chính

Phương thức tự nhiên để tích hợp TSS trên blockchain là để cho các máy khách (client) trên blockchain tạo các khóa và chữ ký bằng cách sử dụng TSS. Ở đây, tôi sử dụng thuật ngữ máy khách trên blockchain để mô tả một tập hợp các lệnh do một full-node thực hiện. Trên thực tế, công nghệ TSS cho phép chúng ta thay thế tất cả các lệnh liên quan đến khóa cá nhân bằng các phép tính toán phân tán.

1.4.1. Ví ngưỡng

Ví ngưỡng có một quy trình phức tạp hơn. Mặc dù nó có thể tạo một cấu trúc HD, nhưng quy trình tạo này phải được tính toán theo cách phân tán, như một giao thức MPC khác. Các bên phải cùng quyết định khóa được sử dụng tiếp theo. Nói cách khác, mỗi bên sẽ có một cụm từ chứa thông tin khôi phục của riêng mình.

1.4.2. Hợp đồng thông minh

Trong nhiều năm qua, các nhà nghiên cứu đã tìm ra nhiều ứng dụng của chữ ký số, và một số ứng dụng vô cùng quan trọng. Như đã đề cập ở trên, TSS là một thuật toán mã hóa bậc thấp đã có từ lâu, có khả năng tăng cường bảo mật đáng kể. Chúng ta có thể nói rằng nhiều tính năng của blockchain có thể được thay thế bởi các kỹ thuật mã hóa dựa trên TSS.

1.5. Kết luận chương

Trong Chương 1, tôi đã giới thiệu về loại chữ ký số, blockchain và khả năng ứng dụng mạnh mẽ của blockchain vào xã hội nói chung và trong thương mại điện tử nói riêng. Trong chương tiếp theo, chúng ta sẽ đi sâu vào kỹ thuật được sử dụng trong chữ ký ngưỡng và áp dụng vào Blockchain như thế nào.

CHƯƠNG 2: XÂY DỰNG MÔ HÌNH CHỮ KÝ SỐ NGƯỠNG TRÊN CƠ SỞ HỆ MẬT TRÊN ĐƯỜNG CONG EDWARDS

2.1. Hệ mật trên đường cong Edwards

2.1.1. Đường cong Elliptic

Khóa bí mật và khóa công khai

Khóa bí mật:

Một khoá bí mật - private key chỉ đơn thuần là một con số được chọn ra ngẫu nhiên. Đúng như cái tên của nó, private key cần được giữ bí mật, nên việc chọn ra số ngẫu nhiên phải vô cùng an toàn và đảm bảo tính thực sự ngẫu nhiên để tránh các cuộc tấn công vét cạn hay các cuộc tấn công khác nhằm lấy được private key.

Khóa công khai:

Đường cong Elliptic (EC)

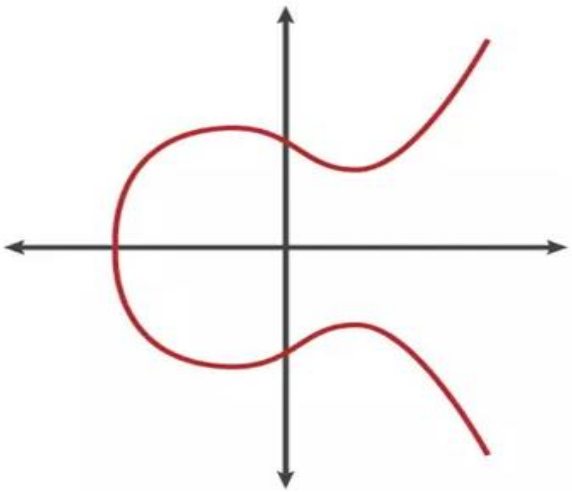
Công thức của đường cong Elliptic là:

$$y2(mod\ p)=x3+ax+b(mod\ p)$$

Đường cong này có công thức như sau:

$$y2(mod\ p)=x3+7(mod\ p)$$

với p là một số nguyên tố rất lớn p=2265−232−29−28−27−26−24−1



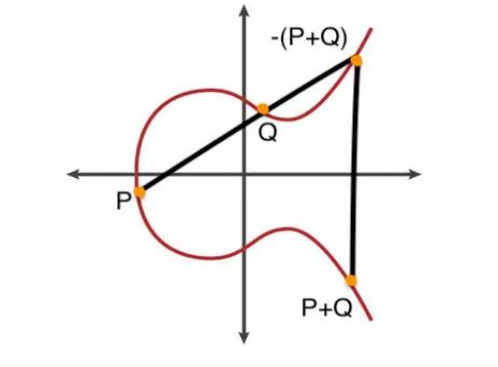
Hình 2.1. Minh họa đường cong Elliptic

Có 2 phép toán quan trọng trên đường cong Elliptic: phép cộng và phép nhân

Phép cộng

Đường cong Elliptic có một tính chất: "Nếu hai điểm P và Q nằm trên đường cong, thì điểm P+Q cũng sẽ nằm trên đường cong". Điểm này được xác định như sau:

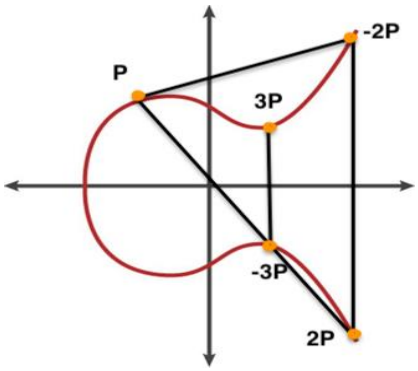
Vẽ đường thẳng nối 2 điểm P và Q, đường thẳng này sẽ cắt đường cong tại một điểm nữa, lấy đối xứng của điểm này qua trục hoành, ta sẽ có được P+Q. Nếu 3 điểm trên đường cong Elliptic là thẳng hàng, thì tổng của chúng bằng 0.



Hình 2.2. Mô tả phép cộng được tiến hành trong đường cong Elliptic

Phép nhân

Trên đường cong Elliptic, việc nhân một điểm với một hằng số không đơn thuần chỉ là lấy từng toạ độ rồi nhân là xong. Thực chất, phép nhân ở đây vẫn là phép cộng, nhưng thực hiện nhiều lần mà thôi.



Hình 2.3. Mô tả phép nhân được tiến hành trong đường cong Elliptic

Do cách tính toán trên, ta có thể dễ dàng tính toán được phép nhân k*P khi biết k và P, nhưng hoàn toàn không thể tính toán được theo chiều ngược lại, tức phép chia. Đó cũng chính là tính chất đặc trưng thú vị của mã hoá bất đối xứng.

Tạo Public key

Ta đã có một private key là một số ngẫu nhiên dA.

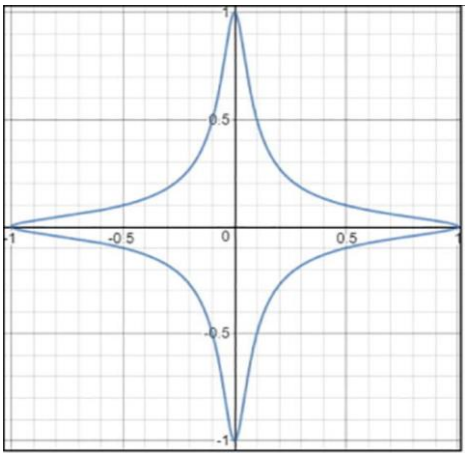
Trên đường cong Elliptic ta chọn một điểm G, gọi là điểm sinh (generator point hay reference point).

Public key QA được sinh ra bằng kết quả của phép nhân:

$$QA=dA\times G$$

Tất nhiên QA cũng sẽ là một điểm trên đường cong Elliptic. Mối quan hệ giữa dA và QA là cố định, và chỉ tính được theo một chiều từ dA đến QA.

2.1.2. Hệ mật trên đường cong Edwards (EdDSA)



Hình 2.4. Đường cong Edwards

Đường cong Edwards thỏa mãn phương trình:

$$x^2 + y^2 = a^2 + a^2x^2y^2 \quad (3)$$

Đây là hình thức mà Harold Edwards đã nghiên cứu trong bài báo gốc. Hơn nữa, Bernstein and Lange cũng đã xây dựng, nghiên cứu và biến đổi các đường cong Edwards tới một dạng đơn giản hơn:

$$x^2 + y^2 = 1 + dx^2y^2 \quad (4)$$

Không giống như các đường cong Elliptic khác sử dụng các hợp âm và tiếp tuyến để xây dựng một điểm, đường cong Edwards sử dụng luật cộng đường tròn đơn vị làm phương pháp của nó.

Điều này chỉ ra rằng nếu có (x_1, y_1) và (x_2, y_2) trong đường cong Edward, trong Phương trình (3) sau đây, (x_3, y_3) được biết là suy ra từ cùng một đường cong:

$$x_3 = \frac{(x_1y_2+x_2y_1)}{(a.(1+x_1y_1x_2y_2))}, y_3 = \frac{(y_1y_2-x_1x_2)}{(a.(1-x_1y_1x_2y_2))} \quad (5)$$

Tương tự, tính chất nhân đôi có thể được áp dụng bằng cách thay thế (x_2, y_2) bằng (x_1, y_1) trong công thức cộng để thu được công thức nhân đôi (x1, y1) + (x1, y1) = (x3, y3) như trong phương trình (6):

$$x_3 = \frac{(x_1y_1+x_1y_1)}{(a.(1+x_1^2y_1^2))}, y_3 = \frac{(y_1^2-x_1^2)}{(a.(1-x_1^2y_1^2))} \quad (6)$$

2.2. Xây dựng mô hình chữ ký số ngưỡng trên đường cong Edwards

EdDSA mạnh và đơn giản hơn ECDSA. EdDSA không phụ thuộc vào bộ tạo số ngẫu nhiên. Chữ ký được biểu diễn trong Phương trình (7) là chữ ký Schnorr của Maxwell et al. (2019), trong đó r là một lựa chọn ngẫu nhiên của người ký và việc xác minh được thực hiện như trong phương trình:

$$(R, s) = (r\,G, r + H\,(X, R, m)\,x) \quad (7)$$

$$s\,G = R + H\,(X, R, m)\,X \quad (8)$$

Dựa trên sự so sánh các tài liệu được khảo sát, một đường cong Edwards và thuật toán chữ ký số dựa trên đường cong Edwards có thể có được mức độ bảo mật cao với kích thước khóa nhỏ. Hình 2.5, 2.6 so sánh số học và hiệu năng của đường cong cơ bản để biện minh cho sự lựa chọn cho đường cong Edwards để đạt được tính toán tối ưu và giảm độ phức tạp tính toán.

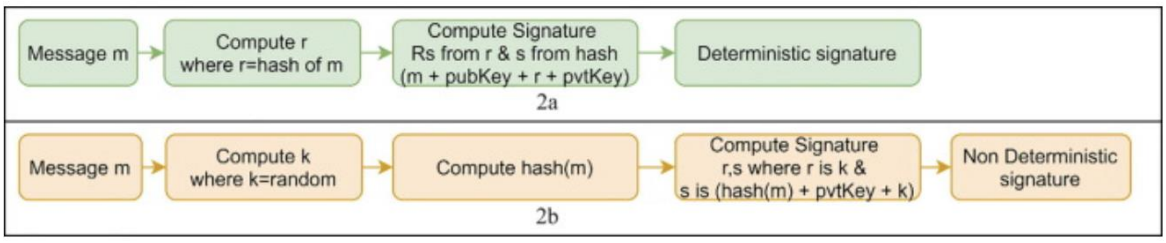
Đường cong	Phương trình	Đồ thị	Khái quát
Edwards	$x^2 + y^2 = 1 + dx^2y^2$	x ^ 2 + y ^ 2 = 1–300 × ^ 2 y^2	nhanh và toàn vẹn
Elliptic	$y^2 = x^3 + ax + b$	y ^ 2 = x ^ 3–0.4 × + 0.7	tin cậy nhưng chậm và không toàn vẹn

Hình 2.5. So sánh đồ thị biểu diễn giữa Edwads và Elliptic

Thông số	ECDSA	EdDSA
Số lượng khoá	384	10
Thời gian tạo mã (giây)	0.799	0.0006
Thời gian ký (giây)	0.0016	0.0002
Thời gian xác thực chữ ký (giây)	0.0082	0.0007

Hình 2.6. So sánh hiệu năng giữa Edwads và Elliptic

Hiệu năng được đo đạc trong hình 2.5 bởi các phép toán số học cơ bản , chẳng hạn như phép nhân, cộng, cộng hỗn hợp, nhân hỗn hợp, cho thấy rằng đường cong Edwards tốt hơn đường cong Elliptic.



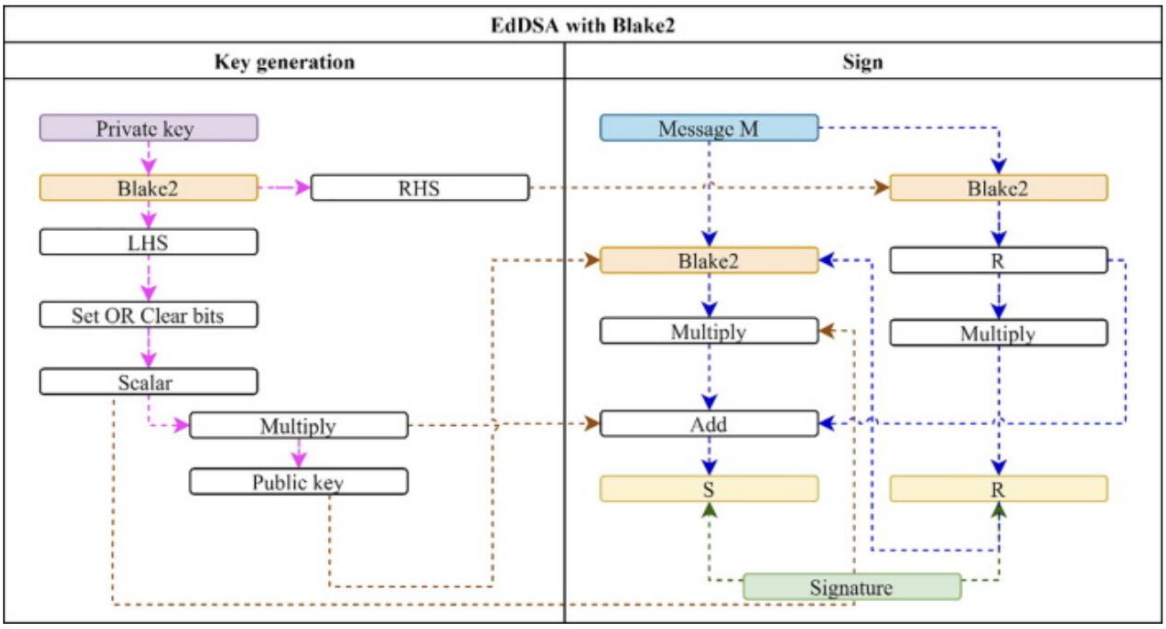
Hình 2.7. a) Luồng EdDSA. b) Luồng ECDSA

Lưu đồ trong Hình 2.6 cho thấy quy trình của EdDSA và ECDSA. EdDSA có lợi thế về hiệu suất, yêu cầu số ngẫu nhiên, khả năng phục hồi đối với các cuộc tấn công kênh bên, va chạm, khóa nhỏ hơn và chữ ký nhỏ hơn, như được trình bày bởi Josefsson và Liusvaara (2017).

Việc HASH (hàm băm) được thực hiện ở nhiều giai đoạn trong DSA và một hàm băm tốt hơn có thể giúp cải thiện công việc hơn nữa. Hình 2.7 cho thấy một nghiên cứu so sánh về các hàm băm , và có thể thấy rằng thuật toán BLAKE2 đứng đầu danh sách có tốc độ băm nhanh nhất. Hơn nữa, so sánh dựa trên kích thước và chiều dài khóa được trình bày trong Hình 2.7 chứng minh sự lựa chọn của tôi về BLAKE2.

Algorithm	Hash speed MiBps	Output sizeBits	Internal state size	Block size	Length size	Word size	Rounds
MD5	632	128	128	512	64	32	64
SHA-0	–	160	160	512	64	32	80
SHA-1	909	160	160	512	64	32	80
SHA3-224	–	224	1600	1152	–	64	24
SHA3-256	367	256	1600	1088	–	64	24
SHA3-384	–	384	1600	832	–	64	24
SHA3-512	198	512	1600	576	–	64	24
BLAKE2b	947	512	512	1024	128	64	12
BLAKE2s	648	256	256	512	64	32	10

Hình 2.8. So sánh tốc độ giữa các thuật toán băm



Hình 2.9. Quy trình của chữ ký số Edwards với BLAKE2

Trong quá trình ký, khóa cá nhân (pvtKey) và khóa công khai (pubKey) được tính toán. Khoá bí mật và message trở thành đầu vào cho chức năng ký. Tôi sử dụng hàm băm BLAKE để đạt được hiệu suất cao trong hàm ký, như sau:

```
Sign(secret, message)
 a = secret
 A = pC(pM(a,G))
r = BLAKE2 mod q(prefix + message)
 R = pM(r,G)
 Rs = pC(R)
h = BLAKE2 mod q(Rs + A + message)
 s = (r + h*a) % q
return signature
```

Hình 2.10. Hàm ký sử dụng thuật toán BLAKE2

Trong đó: pC là nén điểm, pM là phép nhân, G đại diện cho các điểm đường cong và q là nhóm con được tạo ra từ G.

```
Verify(pK, message, signature):
len(pK)!=32: AND len(signature)!=64:
A = decompress(publicKey)
Rs = signature [:32]
s = b' (signature [32:])
h = BLAKE mod q(Rs + pK + message)
sB = pointMultiplication(s,G)
hA = pM(h,A)
pE(sB,pointAdd(R,hA)
return pE === TRUE && verifiedTime >= (threshold + 1)
```

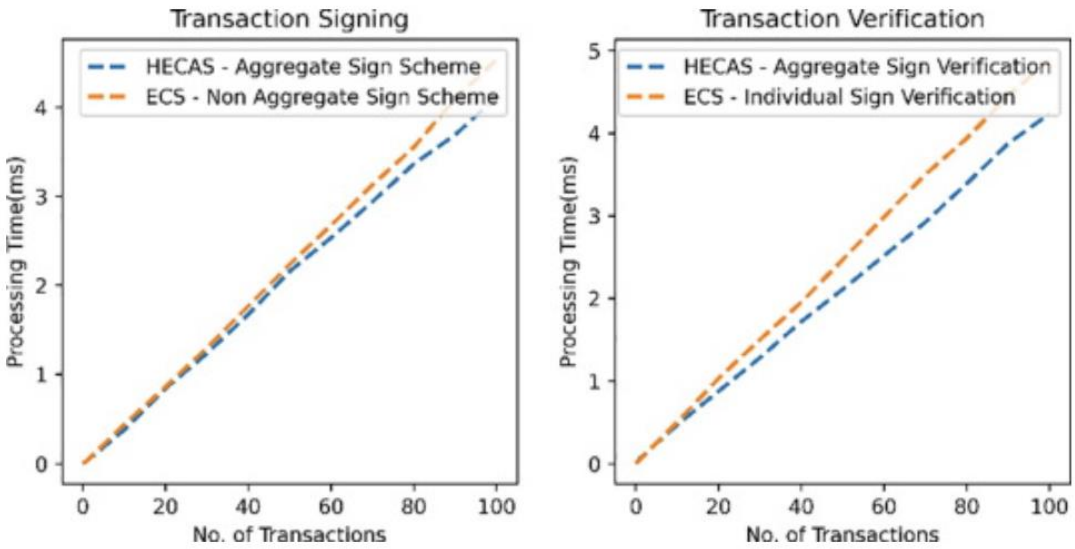
Hình 2.11. Xác minh chữ ký

Trong đó: pK là khóa công khai, pM là phép nhân điểm, pE là điểm bằng nhau, G đại diện cho các điểm đường cong và q là thứ tự nhóm con được tạo ra từ G, verifiedTime là số lần xác minh chữ ký, threshold là ngưỡng xác minh chữ ký.

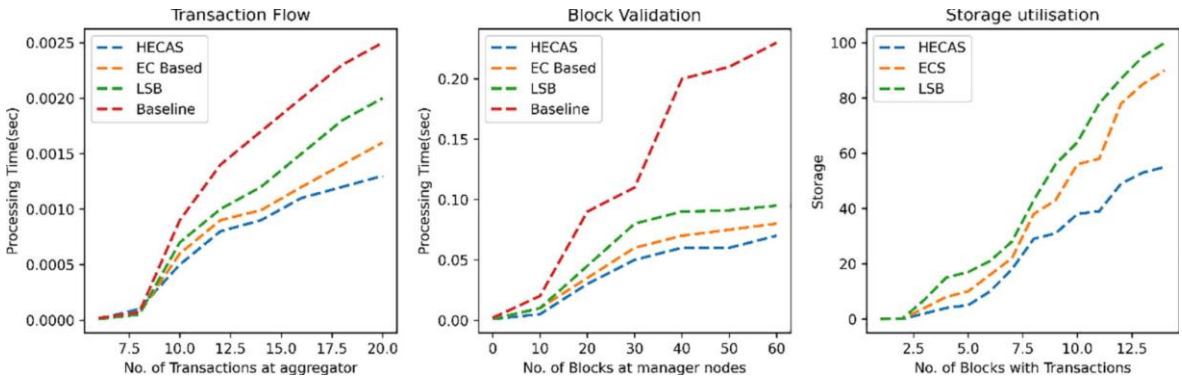
2.3. Phân tích tính hiệu quả của mô hình

So sánh lược đồ Edwards với các phương pháp chữ ký dựa trên tổng hợp và biểu diễn bằng đồ thị thời gian thực hiện của mỗi phương pháp để tính toán các chữ ký cho dữ liệu. Luồng dữ liệu được tăng tuyến tính tại các khoảng thời gian cố định và được vẽ biểu đồ dựa trên thời gian xử lý TSign

$$T_{Sign} = (T_{SC} - T_{SS}) + T_{TL}$$



Hình 2.12. So sánh thời gian ký và xác minh giao dịch



Hình 2.13. So sánh thời gian luồng xử lý và dung lượng cache giao dịch

Mô hình này đã trình bày một lược đồ chữ ký tổng hợp dựa trên đường cong Edwards hiệu suất cao để đảm bảo hiệu tính toàn vẹn của giao dịch. So với sơ đồ chữ ký cá nhân, giảm 40% dung lượng lưu trữ, trong khi các tác vụ ký và xác minh đạt được thời gian xử lý ngắn

hơn 10% và 13%, tương ứng so với sơ đồ chữ ký số thông thường. Những cải tiến này có tác động đáng kể đến các yếu tố khác, chẳng hạn như đạt được mức tăng 10% trong tốc độ dòng giao dịch và cải thiện việc xác thực blockchain.

2.4. Kết luận chương

Xác minh nhanh hơn: Thuật toán của EdDSA đơn giản hơn ECDSA và cả hai đều dễ hiểu và dễ tích hợp. Chính vì sự đơn giản này, EdDSA có hiệu năng sử dụng nhỉnh hơn ECDSA một chút.

Khả năng bảo mật đã được chứng minh: Chữ ký EdDSA đã được chứng minh là an toàn. Cụ thể hơn, các thông tin được mã hóa bởi nó vô cùng khó bị làm giả và gần như bất biến. Mặc khác, chữ ký ECDSA đã từng bị thay đổi và gây nên nhiều vấn đề đối với Bitcoin.

Tính tuyến tính: Chúng ta có thể thêm vài chữ ký EdDSA và kết quả vẫn là một chữ ký hợp lệ. Điều này có thể giúp tiết kiệm năng lượng tính toán và hình thành block cho các cấp độ xây dựng cao hơn mà cải thiện cả về hiệu năng lẫn tính bảo mật, như là giao dịch đa chữ ký, v.v.

CHƯƠNG 3. ỨNG DỤNG CHỮ KÝ SỐ NGƯỠNG TRONG CÔNG NGHỆ BLOCKCHAIN

3.1. Triển khai thử nghiệm mô hình

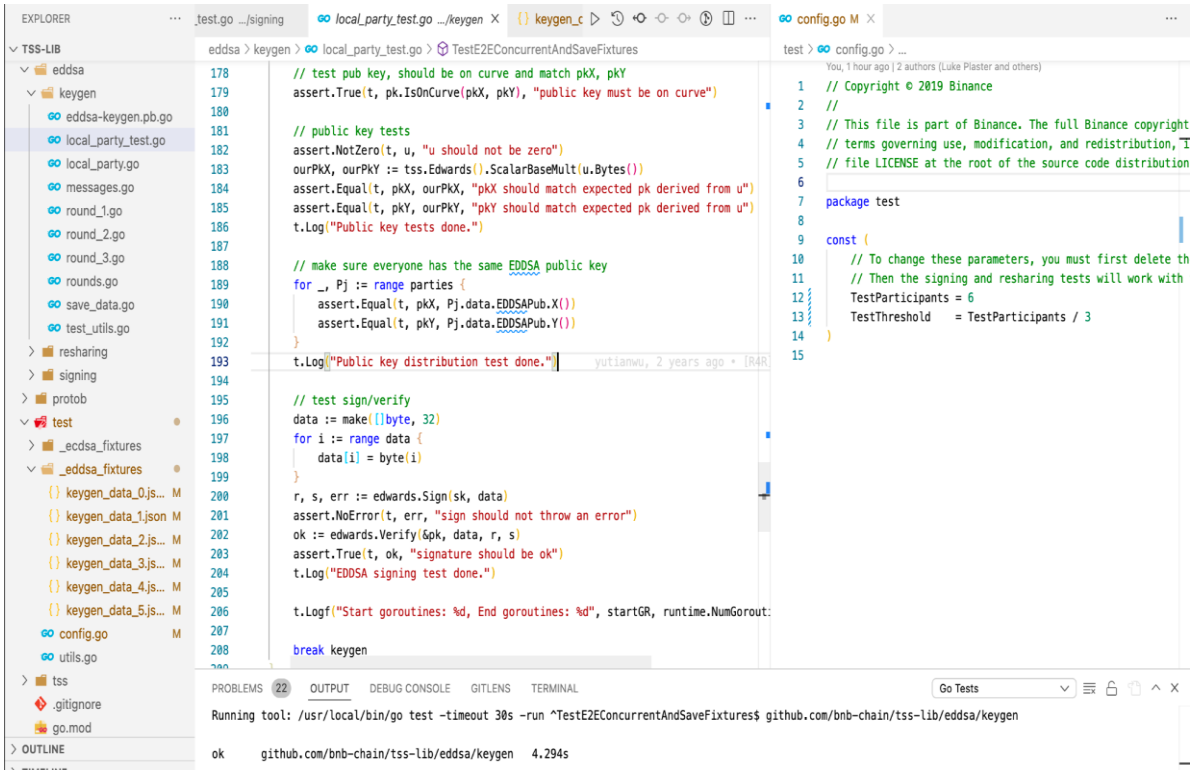
Để triển khai được mô hình trên hệ thống blockchain, tôi sử dụng bộ thư viện:

- TSS-BNB: https://github.com/bnb-chain/tss-lib
- ZenGo-X: https://github.com/ZenGo-X
- Zilliqa: https://dev.zilliqa.com/

Trong đó TSS-BNB hỗ trợ tạo các public key EdDSA, ZenGo có hỗ trợ thuật toán chữ ký số EdDSA và Zilliqa dùng để test mô hình trên hệ thống blockchain online. Ngôn ngữ sử dụng golang, rust và typescript.

Môi trường cài đặt:

- nvm use 10.16.3
- rustup install nightly-2019-07-10
- rustup override set nightly-2019-07-10
- brew install golang



Hình 3.1. Cấu hình số lượng node và ngưỡng chữ ký trong giao dịch

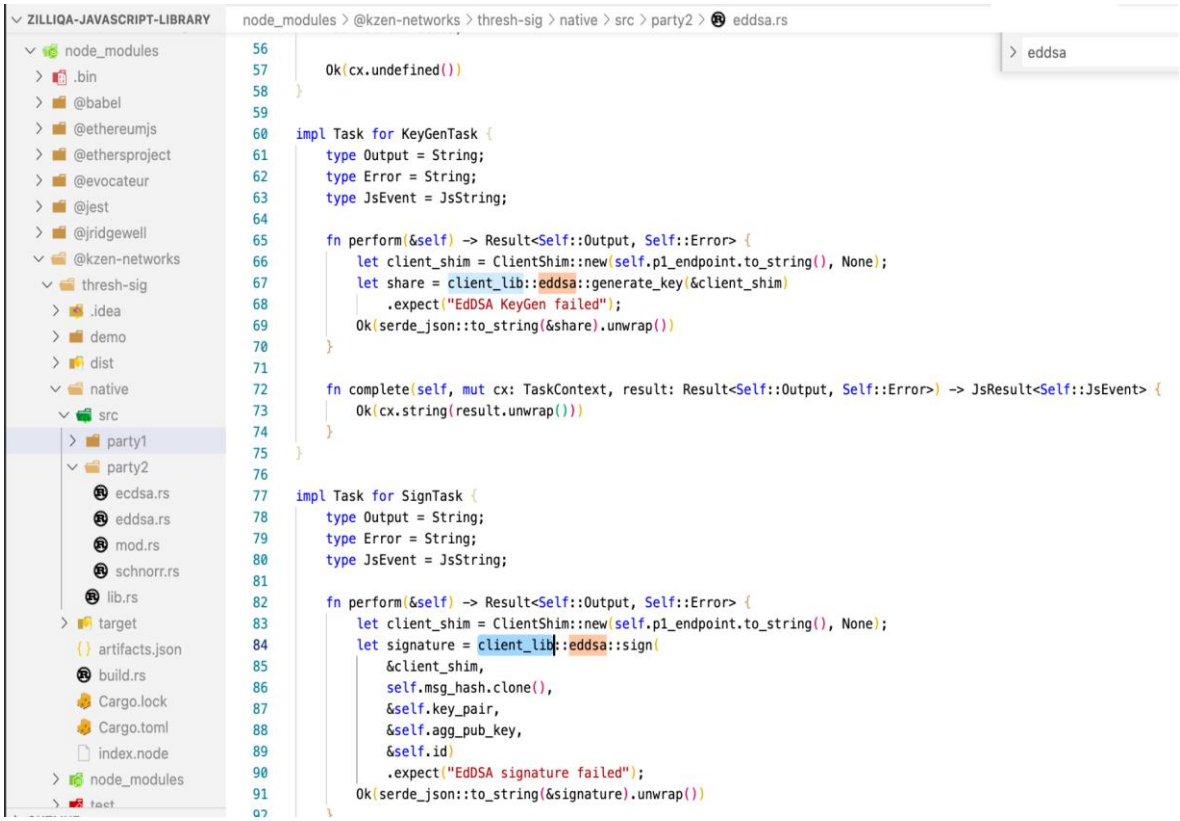
Genarate keys

$go test -timeout 30s -run ^TestE2EConcurrentAndSaveFixtures$ github.com/bnb-chain/tss-lib/eddsa/keygen

ok github.com/bnb-chain/tss-lib/eddsa/keygen 4.294s

Theo cấu hình ban đầu với số lượng node tham gia là 6 thì thuật toán sẽ tạo ra 6 EdDSA key khác nhau nhưng EdDSA public key giống nhau.

Hình 3.2. Cấu trúc một EdDSA key

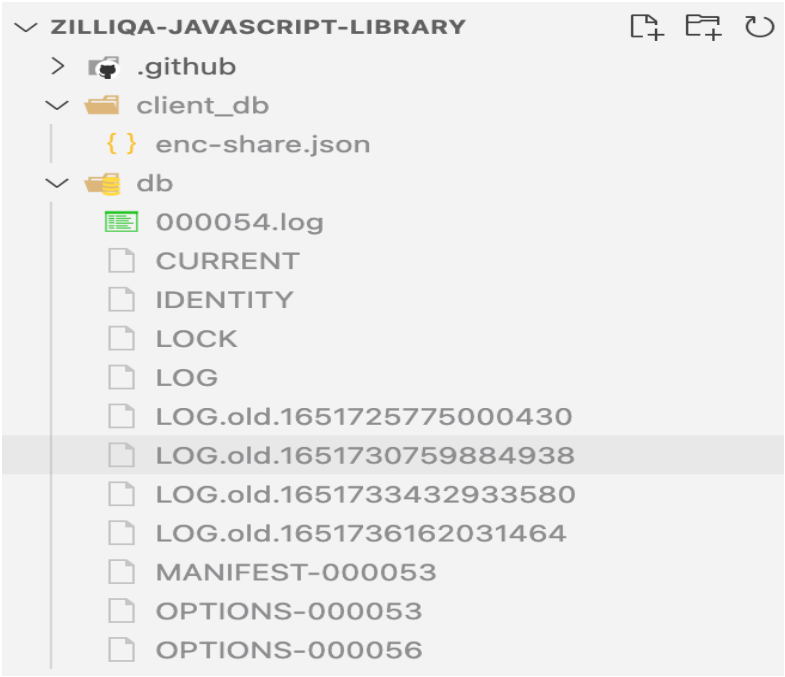


Hình 3.3. Cấu hình ký giao dịch bằng EdDSA

Để test được quá trình TSS khi giao dịch blockchain, trước tiên ta cần tạo một địa chỉ ví test. Ta có thể sử dụng api của Zilliqa hoặc tạo trên trang: https://dev-wallet.zilliqa.com/generate.

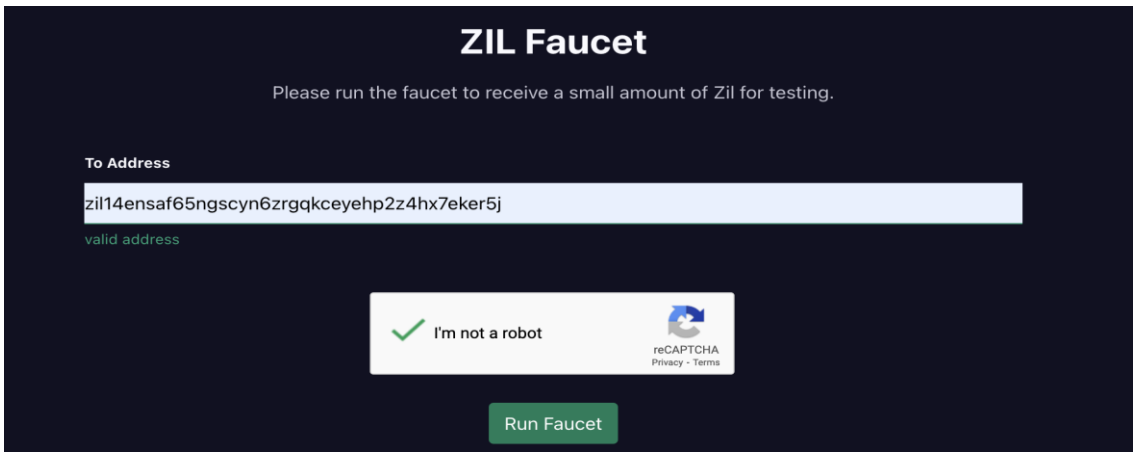
```
async function loadOrCreateWallet() {
  let address;
  let encryptedShare;
  if (fs.existsSync(ENCRYPTED_SHARE_PATH)) {
    encryptedShare = fs.readFileSync(ENCRYPTED_SHARE_PATH);
  }

  if (encryptedShare) {
    address = await zilliqa.wallet.addByKeystore(encryptedShare, DEFAULT_PASSPHRASE);
  } else {
    ensureDirSync(CLIENT_DB_PATH);
    address = await zilliqa.wallet.create();  // run two-party key generation and store a share in default account
    const encryptedShare = await zilliqa.wallet.export(address, DEFAULT_PASSPHRASE);
    fs.writeFileSync(ENCRYPTED_SHARE_PATH, encryptedShare);
  }
  return address;
}
```

Hình 3.4. Tạo ví qua api của Zilliqa

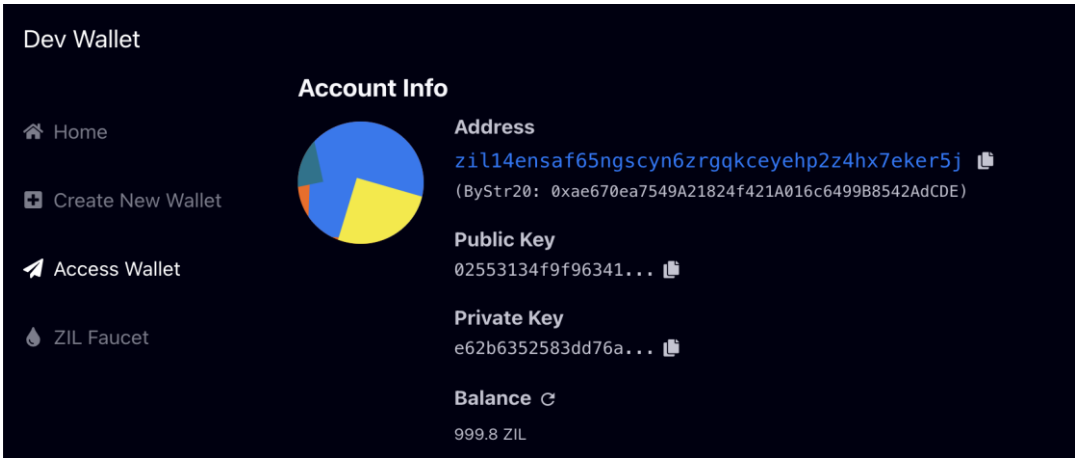


Hình 3.5. Thông tin ví vừa tạo được lưu ở client_db

Dùng tính năng Faucet để deposit 1000 ZIL vào địa chỉ ví vừa tạo. Ví cần có ZIL token để test được giao dịch.



Hình 3.6. Nạp ZIK token vào ví



Hình 3.7. Kiểm tra thông tin ví qua Dev Wallet

```
VFCs-MacBook-Pro:Zilliqa-JavaScript-Library vfcit$ demo/client address
zil14ensaf65ngscyn6zrgqkceyehp2z4hx7eker5j
VFCs-MacBook-Pro:Zilliqa-JavaScript-Library vfcit$ demo/client balance zil14ensa
f65ngscyn6zrgqkceyehp2z4hx7eker5j
{ id: 1,
  jsonrpc: '2.0',
  result: { balance: '999800000000000', nonce: 2 },
  req:
   { url: 'https://dev-api.zilliqa.com',
     payload:
      { id: 1, jsonrpc: '2.0', method: 'GetBalance', params: [Array] } } }
```

Hình 3.8. Kiểm tra thông tin địa chỉ và số dư qua api Zilliqa

```
VFCs-MacBook-Pro:Zilliqa-JavaScript-Library vfcit$ demo/server
🔧 Configured for production.
    => address: 0.0.0.0
    => port: 8000
    => log: critical
    => workers: 8
    => secret key: private-cookies disabled
    => limits: forms = 32KiB
    => keep-alive: 5s
    => tls: disabled
🚀 Rocket has launched from http://0.0.0.0:8000
```

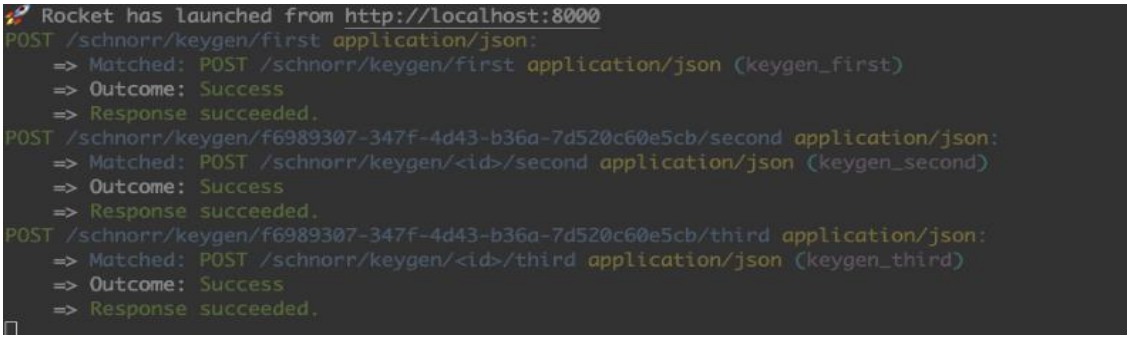
Hình 3.9. Start demo server

```
program
  .command('transfer <from> <to> <amount>')
  .action(async (from, to, amount) => {
    await loadOrCreateWallet();
    const minGasPriceResponse = await zilliqa.blockchain.getMinimumGasPrice();
    const minGasPrice = new BN(minGasPriceResponse.result);
    console.log('Sending... (confirmation may take around a minute)');
    zilliqa.blockchain.createTransaction(
      zilliqa.transactions.new({
        version: VERSION,
        toAddr: to,  // should be either a valid checksum or bech32 address
        amount: new BN(units.toQa(amount, units.Units.Zil)),
        gasPrice: minGasPrice,
        gasLimit: Long.fromNumber(50),
      })
    ).then((tx) => {
      console.log(tx);
    }).catch((e)=>{
      console.log(e);      You, 5 hours ago • Uncommitted changes
    })
  });
```

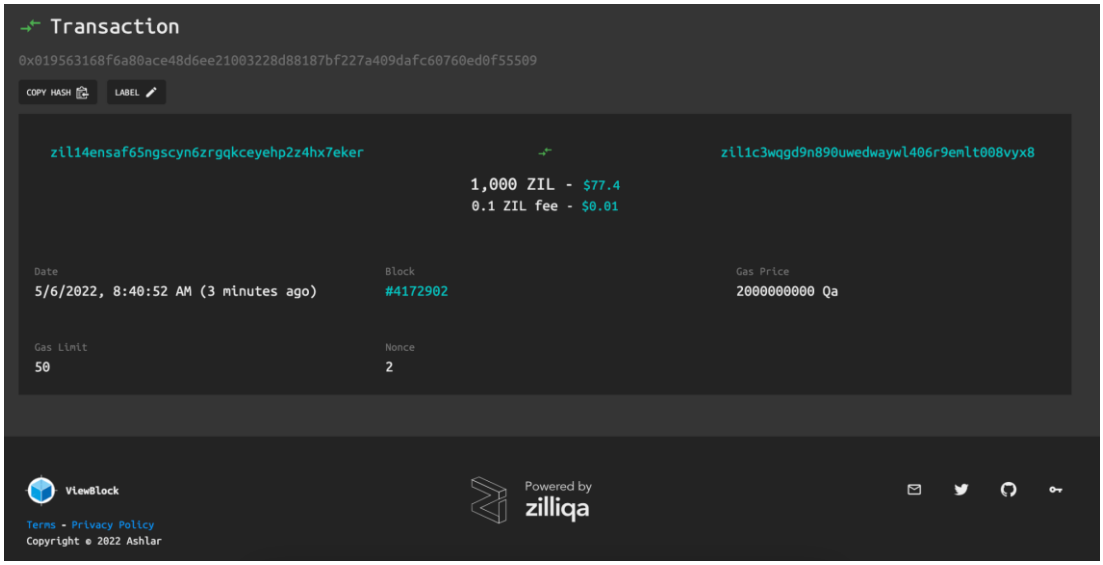
Hình 3.10. Mã code tạo giao dịch chuyển token

```
VFCs-MacBook-Pro:Zilliqa-JavaScript-Library vfcit$ demo/client transfer zil14ens
af65ngscyn6zrgqkceyehp2z4hx7eker5j zil1c3wqgd9n890uwedwaywl406r9emlt008vyx8zp 10
00
Sending... (confirmation may take around a minute)
Transaction {
  code: '',
  data: '',
  version: 21823489,
  toAddr: '0xC45c0434b3395fc765AeE91DFabF432e77F5bdE7',
  nonce: 2,
  pubKey:
   '02553134f9f9634197780072a3185375edf9ac97cb6620a65d467efca3adb1db92',
  amount: <BN: 38d7ea4c68000>,
  signature:
   '45048246388d4c188445f962c69a1f99eabd1d3b4ceb6d8e2aed29f25c59696843593b2fdd8a
4edfd14d8a921f9a9d84fd5c0502141d48a6b285a3bd0489a00a',
  gasPrice: <BN: 77359400>,
  gasLimit: Long { low: 50, high: 0, unsigned: false },
  receipt: { cumulative_gas: 50, epoch_num: '4172902', success: true },
  provider:
   HTTPProvider {
     middleware: { request: [Object], response: [Object] },
     nodeURL: 'https://dev-api.zilliqa.com',
     reqMiddleware: Map { 'CreateTransaction' => [Array] },
     resMiddleware: Map {} },
  status: 2,
  toDS: false,
  blockConfirmation: 0,
  eventEmitter:
   EventEmitter {
     handlers: {},
     emitter:
      { on: [Function: on],
        off: [Function: off],
        emit: [Function: emit] },
     off: [Function: bound off],
     emit: [Function: bound emit],
     resolve: [Function],
     reject: [Function],
     promise: Promise { <pending> },
     then: [Function: bound then] },
  id:
   '019563168f6a80ace48d6ee21003228d88187bf227a409dafc60760ed0f55509' }
```

Hình 3.11. Tạo một giao dịch gửi 1000 ZIL đến một ví khác



Hình 3.12. Giao dịch pass qua ngưỡng 3 chữ ký



Hình 3.13. Kiểm tra giao dịch trên viewblock qua mã transactionId

3.2. Phân tích đánh giá ưu nhược điểm của mô hình

Qua thử nghiệm thì điểm đầu tiên ta có thể thấy được là tính độc lập của quá trình tạo khoá, nếu áp dụng đa chữ ký thì khả năng bảo mật của thuật toán là rất cao. Về tốc độ xử lý thì trong quy mô thử nghiệm thì một giao dịch được thực hiện trong khoảng 15 giây. Vì giới hạn về số lượng node do chưa đủ hạ tầng phần cứng để thử nghiệm trong mạng lớn hơn nên tốc độ và hiệu suất của thuật toán trong phạm vi luận văn là chấp nhận được. Các đánh giá từ các kỹ sư phát triển sàn Binance cũng đánh giá thuật toán EdDSA có các ưu điểm như trên.

3.3. Kết luận chương

Trong những năm gần đây, số lượng các triển khai TSS đã tăng lên đáng kể. Tuy nhiên, là một công nghệ khá mới mẻ, nó vẫn có những hạn chế và một số vấn đề cần cân nhắc. So với công nghệ mã hóa khóa công khai cổ điển, các giao thức TSS có thể rất phức tạp nhưng vẫn chưa được "kiểm thử trên thực tế". So với các chữ ký số đơn giản, TSS thường yêu cầu các giả định mã hóa bổ sung yếu hơn. Do đó, các vector tấn công mã hóa không tồn tại trong các thiết lập truyền thống giờ đây đang được khám phá. Hội thảo Breaking Bitcoin Conference năm 2019 có tìm ra một số lỗi và chỉ ra những điểm có thể cải thiện trong thuật toán. Sàn Binance là sàn blockchain lớn nhất hiện nay cũng đang chuẩn bị ứng dụng công nghệ chữ ký ngưỡng dựa trên đường cong Edwards, giai đoạn này Binance vẫn đang open source code phần TSS-EdDSA để cộng đồng thử nghiệm và đánh giá. Bên cạnh đó một số nhà phát triển đã mạnh dạn áp dụng thuật toán EdDSA để làm token như Cardano, NANO, Stellar Lumens, WAVES, Libra.

PHẦN KẾT LUẬN

Trong phạm vi luận văn đã thực hiện nghiên cứu về các loại chữ ký số, chữ ký ngưỡng. Thực hiện tìm hiểu một số giải thuật áp dụng cho bài toán chữ ký ngưỡng trong Blockchain.

Luận văn đã thực hiện nghiên cứu chữ ký ngưỡng áp dụng đường cong Edwards, xây dựng thử nghiệm để chứng minh tính khả thi của thuật toán.

Trong quá trình nghiên cứu, nhiều hạn chế được phát hiện nhưng để giải quyết đòi hỏi nền tảng tri thức sâu và rộng hơn. Các hướng nghiên cứu chính tiếp theo được đề xuất như sau:

- Nghiên cứu về đa chữ ký số trong chữ ký số ngưỡng.
- Nghiên cứu các vấn đề cần cải thiện từ Hội thảo Breaking Bitcoin Conference.