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

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI - 2022

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

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC:

TS. ĐẶNG MINH TUẤN

HÀ NỘI - 2022

LỜI CAM ĐOAN

Tôi xin cam đoan Luận văn thạc sĩ với đề tài: "Nghiên cứu chữ ký số ngưỡng và khả năng ứng dụng trong công nghệ Blockchain" dưới sự hướng dẫn của thầy giáo - TS. Đặng Minh Tuấn là công trình nghiên cứu của riêng tôi. Các kết quả nghiên cứu trong luận văn là trung thực, các tài liệu tham khảo được trích dẫn đầy đủ.

Hà Nội, ngày 12 tháng 05 năm 2022

Học viên

Lê Trọng Quý

LỜI CẢM ƠN

Đầu tiên, tôi xin được gửi lời cảm ơn sâu sắc đến Học viện công nghệ Bưu chính Viễn thông nói chung và các Thầy/Cô đã giảng dạy tôi nói riêng, Thầy/Cô đã truyền đạt những kiến thức và kinh nghiệm quý báu trong suốt quá trình tôi học tập tại Học viện.

Tôi xin được gửi lời tri ân sâu sắc đến thầy giáo - TS. Đặng Minh Tuấn, người đã dìu dắt và hướng dẫn tôi trong suốt quá trình thực hiện luận văn. Sự chỉ bảo và định hướng của thầy đã giúp tôi nghiên cứu và giải quyết các vấn đề một cách khoa học và đúng đắn hơn.

Tiếp theo, tôi xin được gửi lời cảm ơn tới bố mẹ, bạn gái và anh chị em đồng nghiệp đã luôn động viên, giúp đỡ tôi vượt qua những khó khăn trong học tập, công việc và cuộc sống.

Trong quá trình thực hiện luận văn, dù đã rất cố gắng nhưng không thể tránh khỏi những thiếu sót, tôi rất mong nhận được sự đóng góp ý kiến từ Thầy/Cô và các bạn để luận văn của tôi được hoàn thiện hơn.

Tôi xin chân thành cảm ơn!

Hà Nội, ngày 12 tháng 05 năm 2022

Học viên

Lê Trọng Quý

MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ, CHỮ VIẾT TẮT

Viết tắt	Tiếng Anh	Tiếng Việt
EdDSA	Edwards-curve Digital Signature Algorithm	Thuật toán sinh chữ ký số dựa trên đường cong Edwards
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán sinh chữ ký số dựa trên đường cong Elliptic
CA	Certificate Authority	Nhà cung cấp chứng thực số
TSS	Threshold Signature Scheme	Lược đồ chữ ký ngưỡng
PKC	Public Key Cryptography	Khoá mã hoá công khai
MPC	Multi-party Computation	Tính toán nhiều bên an toàn
DKG	Distributed Key Generation	Tạo khóa phân tá
Multisig	Multi-Signature	Đa chữ ký
DLT	Distributed Ledger Technology	Sổ cái phân tán
DSA	Digital Signature Algorithm	Giải thuật ký số

DANH SÁCH HÌNH VẼ

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. Trong các giao dịch tài chính, người thực hiện có thể quan sát trạng thái chuyển giao trên Blockchain theo thời gian thực, thay vì không biết tình trạng giao dịch như thế nào cho đến khi giao dịch kết thúc, đó là vấn đề thường xảy ra trong các hệ thống hiện hành. Tính minh bạch không đổi khi áp dụng với mọi giá trị được ghi trên Blockchain .

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

Thuật toán đồng thuận giúp bảo vệ Blockchain đã được chứng minh là rất hiệu quả. Tuy nhiên với sự phát triển của công nghệ, hiện nay đã có một số dạng tấn công tiềm năng có thể thực hiện để nhắm vào các mạng Blockchain.

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). Từ khóa công khai, chúng ta có thể lấy được địa chỉ công khai theo cách thức giống

như ở hệ thống truyền thống, khiến cho Blockchain không thể biết địa chỉ được tạo ra như thế nào. Cơ chế này có ưu điểm là khóa cá nhân sẽ không còn là điểm lỗi duy nhất nữa, bởi vì mỗi bên chỉ nắm giữ một phần của nó. Vì vậy có thể tăng tính an toàn cho các bên tham gia.

3. Mục đích nghiên cứu

Blockchain là công nghệ lưu trữ và truyền tải thông tin dữ liệu bằng các khối (block) được liên kết với nhau và mở rộng theo thời gian. Từng khối chứa đựng các thông tin về thời gian khởi tạo và được liên kết với các khối trước đó. 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 là một tập con của chữ ký điện tử. Có thể dùng định nghĩa về chữ ký điện tử cho chữ ký số. Chữ ký điện tử là thông tin đi kèm theo dữ liệu (văn bản, hình ảnh, video...) nhằm mục đích xác định người chủ của dữ liệu đó. 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.

Chữ ký số đóng vai trò như chữ ký đối với cá nhân hay con dấu đối với doanh nghiệp và được thừa nhận về mặt pháp lý. Quá trình sử dụng chữ ký số bao gồm 2 quá trình: tạo chữ ký và kiểm tra chữ ký.

Công dụng của chữ ký số:

- Các cá nhân, cơ quan, tổ chức, doanh nghiệp có thể dùng chữ ký số như trong những công cụ bảo mật các email của mình để thực hiện việc trao đổi các thông tin, giấy tờ nhanh chóng, an toàn.
- Các doanh nghiệp có thể tiến hành giao dịch với đối tác mà các bên không cần phải trực tiếp gặp mặt trao đổi công việc, đầu tư chứng khoán, mua bán hàng hóa hoặc chuyển các hồ sơ giấy mà không phải lo sợ giả danh hoặc mất cắp mà chỉ cần giao dịch trực tuyến thì mức độ bảo mật và an ninh cũng cao hơn.
- Chữ ký số được sử dụng thay cho chữ ký thông thường trong tất cả các trường hợp giao dịch điện tử và luôn bảo đảm tính pháp lý tương đương theo quy định của luật giao dịch điện tử như khi ký kết hợp đồng của các cá nhân, cơ quan tổ chức.
- Chữ ký số có thể giúp người sử dụng thực hiện các thủ tục hành chính như đăng ký thành lập doanh nghiệp, bổ sung ngành nghề kinh doanh, thay đổi con dấu,

thay đổi người đại diện pháp luật, kê khai và nộp thuế điện tử, kê khai và đóng bảo hiểm xã hội, bảo hiểm thất nghiệp, bảo hiểm tai nạn lao động và bệnh nghề nghiệp,… mà không cần phải trực tiếp đến cơ quan nhà nước.

Ưu điểm của chữ ký số:

- Khả năng xác định nguồn gốc: Các hệ thống mật mã hóa khóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có người chủ của khóa biết. Để sử dụng chữ ký số thì văn bản cần phải được mã hóa hàm băm (thường có độ dài cố định và ngắn hơn văn bản). Sau đó dùng khoá bí mật của người chủ khóa để mã hóa, khi đó ta được chữ ký số. Khi cần kiểm tra, bên nhận giải mã với khóa công khai để lấy lại hàm băm và kiểm tra với hàm băm của văn bản nhận được. Nếu hai giá trị này khớp nhau thì bên nhận có thể tin tưởng rằng văn bản đó xuất phát từ người sở hữu khóa bí mật.
- Tính không thể phủ nhận: Trong giao dịch, một bên có thể từ chối nhận một văn bản nào đó là do mình gửi. Để ngăn ngừa khả năng này, bên nhận có thể yêu cầu bên gửi phải gửi kèm chữ ký số với văn bản. Khi có tranh chấp, bên nhận sẽ dùng chữ ký này như một chứng cứ để bên thứ ba giải quyết.
- Tính toàn vẹn: Cả hai bên tham gia vào quá trình thông tin đều có thể tin tưởng là văn bản không bị sửa đổi trong khi truyền vì nếu văn bản bị thay đổi thì hàm băm cũng sẽ thay đổi và lập tức bị phát hiện. Quy trình mã hóa sẽ ẩn nội dung đối với bên thứ ba.
- Tính bảo mật của chữ ký số: Về kỹ thuật công nghệ của chữ ký số là dựa trên hạ tầng mã hóa công khai (PKI), trong đó phần quan trọng nhất là thuật toán mã hóa công khai RSA. Công nghệ này đảm bảo chữ ký số khi được một người dùng nào đó tạo ra là duy nhất, không thể giả mạo được và chỉ có người sở hữu khóa bí mật mới có thể tạo ra được chữ ký số đó (đã được chứng minh về mặt kỹ thuật mã hóa).

Các loại chữ ký số:

Hiện nay, trên thị trường có rất nhiều loại chữ ký số đa dạng từ hình thức đến tính năng sử dụng, nhiều lựa chọn dẫn đến người sử dụng nên cân nhắc kỹ trước khi

tiến hành mua chữ ký số cho phù hợp với mục đích cá nhân hay doanh nghiệp. Nhìn chung có 4 loại chữ ký số phổ biến nhất hiện nay gồm:

- Chữ ký số USB token: Hiện nay, hầu hết các doanh nghiệp vẫn đang sử dụng chữ ký số USB token cho hoạt động ký số tài liệu, hợp đồng, chứng từ của Doanh nghiệp. Đặc điểm của dòng chữ ký số này là sử dụng một thiết bị phần cứng (USB token) để lưu trữ khóa bí mật giúp tạo lập chữ ký số. Chính đặc điểm ấy khiến cho loại chữ ký số này xuất hiện nhiều bất cập không tránh khỏi. Chẳng hạn như USB token dễ thất lạc hoặc xảy ra sự cố khi kết nối với máy tính, chưa đáp ứng được nhu cầu sử dụng nhiều người trên 1 token và không thể kiểm soát lịch sử ký số. Ưu điểm của chữ ký số USB token bao gồm những lợi ích vượt trội sau:

+ Tính an toàn, bảo mật thông tin cao.

+ Rút gọn quy trình, thủ tục rườm rà khi xin chữ ký thường, tiết kiệm thời gian.

+ Tiết kiệm chi phí giấy tờ, đi lại, công văn xác nhận chữ ký.

+ Có ý nghĩa pháp lý được công nhận.

+ Nguồn gốc văn bản được xác nhận.

- Chữ ký số Smartcard: Chữ ký số Smart Card là một loại chữ ký số được thiết lập sẵn trên thẻ thông minh, phổ biến nhất là SIM do từng nhà mạng phát hàng, là dạng chữ ký số được thiết lập sẵn trên SIM do nhà mạng phát triển, có thể giúp người sử dụng trên thiết bị di động nhanh chóng trong các hoạt động như trả hóa đơn điện nước, kê khai thuế thu nhập cá nhân…Có hai đặc điểm nổi bật của chữ ký số SmartCard so với các loại chữ ký khác, liên quan đến tích hợp thẻ SIM và thiết bị sử dụng: Chữ ký số SmartCard được tích hợp trên sim điện thoại di động, do các nhà mạng nghiên cứu và phát triển và việc sử dụng chữ ký số này có thể tiến hành ngay trên thiết bị di động cá nhân mà không phụ thuộc vào Internet. Ưu điểm của chữ ký số SmartCard: tính linh động sử dụng ngay trên thiết bị di động của mình, tích hợp với SIM; chi phí thấp.

- Chữ ký số HSM: HSM (Hardware Security Module) là một thiết bị vật lý được dùng để bảo vệ và quản lý các cặp khóa chứng thư số cho các ứng dụng có tính

xác thực mạnh và xử lý mật mã. Về hình thức, HSM được sản xuất dưới dạng một card PCI cắm vào máy tính hoặc là một thiết bị phần cứng độc lập có kết nối internet. Là một trong những loại chữ ký số được sử dụng khá phổ biến, chữ ký số HSM mang những đặc điểm sau:

+ Khả năng xác thực danh tính: Chữ ký số HSM sử dụng thiết bị phần cứng HSM để tạo ra và bảo vệ cặp khóa (gồm khóa bí mật và khóa công khai). Thông qua chữ ký số HSM có thể xác thực danh tính chủ nhân của chữ ký.

+ Đảm bảo tính toàn vẹn cho văn bản, hợp đồng, tài liệu đã ký trên môi trường điện tử. Bên cạnh đó, khác với chữ ký số USB Token chỉ hỗ trợ một người ký tại 1 thời điểm, chữ ký số HSM có thể linh hoạt phân quyền và ký số nhiều cùng lúc một cách nhanh chóng, dễ dàng.

+ Không cần luôn mang theo thiết bị HSM bên người, chữ ký số HSM có thể hỗ trợ ký số trực tuyến thông qua tài khoản online kết nối mà nó tạo ra.

+ Chữ ký số HSM được cấu tạo bởi module bảo mật phần cứng đạt chuẩn FIPS 140-2, cho khả năng thực hiện ký số lên đến 1200 lượt ký/ giây. Đây là lý do giúp HSM có thể đáp ứng các tác vụ ký số nhiều, nhanh (ký tự động).

+ Tuy nhiên, nhược điểm của chữ ký số HSM là giá thành khá cao, thường chỉ dùng cho doanh nghiệp lớn có hệ thống quản lý quy mô lớn và cơ sở hạ tầng tốt. HSM cho phép nhiều người cùng ký số tại các điểm khác nhau nhưng thường giới hạn dưới 20 điểm truy cập ký số.

- Chữ ký số từ xa: là một loại chữ ký số kiểu mới sử dụng công nghệ đám mây (cloud-based) để ký số mà không cần sử dụng thêm bất kỳ thiết bị phần cứng nào. Với chữ ký số từ xa, người dùng không còn phải dùng USB token hay SIM để ký nữa, thay vào đó có thể ký trực tiếp ngay trên máy tính, điện thoại hoặc máy tính bảng. Nhờ có ưu điểm này mà người dùng có thể ký số mọi lúc mọi nơi, ngay cả khi đi công tác hay làm việc tại nhà. Ngoài ra, vấn đề bảo mật cũng được đảm bảo an toàn tuyệt đối bởi công nghệ ký số từ xa phải áp dụng tiêu chuẩn châu Âu eIDAS về "Định danh, xác thực điện tử và dịch vụ tin cậy" – đây được coi là bộ quy định hoàn chỉnh nhất về định danh số hiện nay. Áp dụng thêm tính năng xác thực 2 yếu tố và

định danh thiết bị trên điện thoại thì người dùng hoàn toàn có thể yên tâm về bảo mật khi sử dụng loại chữ ký số này.

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...). Trong mô hình này, đối tượng ký là một hay một nhóm thành viên của một tổ chức và được phép ký lên các thông điệp dữ liệu với danh nghĩa thành viên của tổ chức. Cũng trong mô hình này, CA (Certificate Authority) là bộ phận có chức năng bảo đảm các dịch vụ chứng thực số, như: chứng nhận một thực thể là thành viên của tổ chức, chứng thực các thông điệp dữ liệu được ký bởi các thực thể là thành viên trong một tổ chức, mà CA là cơ quan chứng thực thuộc tổ chức này. Tính hợp lệ về nguồn gốc và tính toàn vẹn của một thông điệp dữ liệu ở cấp độ của một tổ chức chỉ có giá trị khi nó đã được CA thuộc tổ chức này chứng thực. Việc chứng thực được thực hiện bằng chữ ký của CA tương tự như việc CA chứng thực khóa công khai cho các thực thể cuối trong các mô hình PKI truyền thống. Trong mô hình này, chữ ký của CA cùng với chữ ký cá nhân của các thực thể ký hình thành nên chữ ký tập thể cho một thông điệp dữ liệu. Nói chung, một CA trong mô hình được đề xuất có những chức năng cơ bản như sau:

- Chứng nhận tính hợp pháp của các thành viên trong một tổ chức: thực chất là chứng nhận khóa công khai và danh tính (các thông tin nhận dạng) của các thành viên trong tổ chức bằng việc phát hành Chứng chỉ khóa công khai (PKC - Public Key Certificate). Ngoài ra, CA còn có trách nhiệm thu hồi PKC hết hạn lưu hành hoặc vi phạm chính sách an toàn của tổ chức.
- Chứng thực nguồn gốc và tính toàn vẹn của các thông điệp: được ký bởi các đối tượng là thành viên của tổ chức mà CA là cơ quan chứng thực của tổ chức này.
- Phát hành, quản lý chứng chỉ khóa công khai: Trong mô hình chữ ký tập thể, chứng chỉ khóa công khai (PKC) được sử dụng để một tổ chức chứng nhận các đối tượng ký là thành viên của nó. Cấu trúc cơ bản của một PKC bao gồm khóa công

khai của chủ thể chứng chỉ và các thông tin khác như: thông tin nhận dạng của chủ thể, trạng thái hoạt động của chứng chỉ, số hiệu chứng chỉ, thông tin nhận dạng của CA,... Không làm mất tính tổng quát, ở đây sử dụng thuật ngữ thông tin nhận dạng (IDi) của đối tượng ký để đại diện cho các thành phần thông tin nói trên . Trong thực tế, có thể sử dụng khuôn dạng chứng chỉ X.509 cho chứng chỉ khóa công khai trong mô hình mới đề xuất.

- Hình thành và kiểm tra chữ ký số tập thể: Trong mô hình được đề xuất, chữ ký tập thể hình thành trên cơ sở chữ ký của một hoặc một nhóm đối tượng ký và chứng nhận của CA với vai trò chứng thực của tổ chức đối với một thông điệp dữ liệu cần ký.

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. 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. Tuy nhiên, bất chấp những khả năng này, TSS vẫn là một công nghệ mới, bởi vậy chúng ta cũng cần xem xét những rủi ro và hạn chế mà nó đem lại.

Để hiểu về TSS, trước hết chúng ta cần có hiểu biết cơ bản về công nghệ mã hóa. 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.

Mã hóa và chữ ký số là hai ứng dụng phổ biến nhất của PKC. Cả hai hệ thống mã hóa và chữ ký số đều dựa trên ba thuật toán như sau. Thứ nhất là thuật toán tạo cặp khóa công khai và khóa cá nhân, thứ hai là thuật toán tạo văn bản mã hóa/chữ ký, và thứ ba là quy trình giải mã/xác thực. Ở các hệ thống chữ ký số, thuật toán chữ ký cần biết khóa cá nhân để có thể tạo một chữ ký duy nhất, chỉ người sở hữu nó mới

biết khóa cá nhân này. Chữ ký này sau đó được đính kèm với tin nhắn sao cho bất kỳ ai có khóa công khai cũng có thể xác thực đó là chữ ký thực và chính xác.

Kỹ thuật tính toán nhiều bên (MPC) là một nhánh của công nghệ mã hóa, kỹ thuật này có nguồn gốc từ công trình của Andrew C. Yao gần 40 năm trước. Trong MPC, một tập hợp các bên không tin tưởng lẫn nhau cùng tính toán chung một hàm với các dữ liệu đầu vào của họ mà không tiết lộ các dữ liệu đầu vào đó cho các bên còn lại.

Hãy lấy một ví dụ, giả sử có n nhân viên của một công ty muốn biết ai là người được trả lương cao nhất trong số họ, tuy nhiên không muốn cho người khác biết mức lương của mình. Trong ví dụ này, các dữ liệu đầu vào cá nhân là mức lương, và kết quả đầu ra sẽ là tên của nhân viên được trả lương cao nhất. Bằng việc sử dụng kỹ thuật MPC, chúng ta có thể đảm bảo thông tin về mức lương của mỗi cá nhân không bị tiết lộ trong quá trình tính toán.

Hai thuộc tính của MPC là tính chính xác và tính riêng tư:

- Tính chính xác: kết quả được thuật toán tính chính xác (theo kỳ vọng).
- Tính riêng tư: dữ liệu đầu vào bí mật của một bên sẽ không bị tiết lộ cho các bên khác.

Chúng ta sẽ sử dụng MPC để tính chữ ký số theo cách phân tán. Hãy xem các thuộc tính trên được áp dụng như thế nào cho chữ ký. Như đã nói ở trên, hệ thống chữ ký gồm ba bước:

- Tạo khóa: bước đầu tiên cũng là bước phức tạp nhất. Chúng ta cần tạo một khóa công khai, khóa này sẽ được sử dụng để xác thực các chữ ký. Tuy nhiên, chúng ta cũng cần tạo ra một thông tin bí mật cho mỗi bên, ở đây chúng ta sẽ gọi là phần thông tin bí mật. Để đảm bảo tính chính xác và tính riêng tư, hàm sẽ xuất một khóa công khai chung cho tất cả các bên và một phần thông tin bí mật cho mỗi bên để thỏa mãn hai thuộc tính: (1) tính riêng tư: không một bên nào được biết phần thông tin bí mật của bên khác, và (2) tính chính xác: khóa công khai là một hàm của các phần thông tin bí mật.

- Ký tên: bước này bao gồm một hàm tạo chữ ký. Mỗi cá nhân sẽ nhập dữ liệu đầu vào là phần thông tin bí mật của mình, phần thông tin này là đầu ra của bước thứ nhất (tạo khóa phân tán). Ngoài ra, có một dữ liệu đầu vào mà tất cả các bên đều có thể thấy, đó chính là thông điệp cần ký tên. Kết quả đầu ra của bước này là một chữ ký số, thuộc tính tính riêng tư bảo đảm rằng không có dữ liệu bí mật nào bị tiết lộ trong quá trình tính toán.
- Xác thực: thuật toán xác thực vẫn giống như trong công nghệ mã hóa cổ điển. Để tương thích với các chữ ký một khóa, tất cả những người biết khóa công khai đều có thể kiểm tra và xác thực các chữ ký. Đây chính xác là công việc của các node xác thực blockchain.

Sự kết hợp kỹ thuật tạo khóa phân tán (DKG) và ký tên phân tán này là lược đồ chữ ký ngưỡng (TSS). Bằng cách sử dụng TSS, 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). Từ khóa công khai, chúng ta có thể lấy được địa chỉ công khai theo cách thức giống như ở hệ thống truyền thống, khiến cho blockchain không thể biết địa chỉ được tạo ra như thế nào. Cơ chế này có ưu điểm là khóa cá nhân sẽ không còn là điểm hư hỏng duy nhất nữa, bởi vì mỗi bên chỉ nắm giữ một phần của nó.

Quy trình tương tự được sử dụng khi ký các giao dịch. Khi ký các giao dịch, thay vì chỉ một bên ký với khóa cá nhân của mình, chúng ta chạy một quy trình tạo chữ ký phân tán có sự tham gia của nhiều bên. Như vậy mỗi bên có thể tạo một chữ ký hợp lệ, miễn là họ hành động trung thực. Như vậy, chúng ta đã chuyển đổi từ tính toán cục bộ (một điểm hư hỏng duy nhất) sang tính toán tương tác.

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. Có thể xây dựng các ứng dụng phân quyền, các giải pháp mở rộng lớp 2, hoán đổi nguyên tử, pha trộn, kế thừa và các tính năng khác trên

khung TSS. Cuối cùng, điều này sẽ cho phép thay thế các hoạt động vận hành hợp đồng thông minh trên chuỗi đắt đỏ và rủi ro bằng các lựa chọn thay thế rẻ tiền và đáng tin cậy hơn. Một số ví dụ có thể kể đến bao gồm: Khóa nhiều bước nhảy sử dụng chữ ký hai bên một cách thông minh, và với mạng lưới kênh thanh toán bảo mật và riêng tư hơn, nó có thể được sử dụng để thay thế mạng lưới Bitcoin lightning network. ShareLock[10] có lẽ là giải pháp pha trộn trên chuỗi có chi phí hợp lý nhất cho Ethereum, dựa trên việc xác thực một chữ ký ngưỡng duy nhất.

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 véc-tơ tấn công mã hóa không tồn tại trong các thiết lập truyền thống giờ đây đang được khám phá. Các kỹ sư về bảo mật và các nhà mật mã học ứng dụng có thể hỗ trợ để triển khai TSS một cách an toàn cho hệ thống.

1.1.4. Đa chữ ký

Multisig là viết tắt của multi-signature (đa chữ ký), là một loại chữ ký điện tử giúp cho hai hoặc nhiều người dùng ký vào tài liệu như là một nhóm. Do đó, một đa chữ ký được tạo ra bằng sự kết hợp của nhiều chữ ký. Công nghệ đa chữ ký đang được dùng trong thế giới tiền điện tử, nhưng nguyên lý của nó đã có mặt từ lâu trước khi tạo ra Bitcoin. Trong ngữ cảnh của tiền điện tử, công nghệ lần đầu tiên được áp dụng cho các địa chỉ tiền điện tử trong năm 2012, cuối cùng dẫn đến việc tạo ra các ví đa chữ ký một năm sau đó. Địa chỉ đa chữ ký có thể được sử dụng trong các ngữ cảnh khác nhau, nhưng hầu hết các trường hợp sử dụng đều liên quan đến các vấn đề bảo mật. Trong bài này, chúng ta sẽ thảo luận về việc sử dụng chúng trong các ví đa chữ ký.

Sự an toàn và bảo mật của tiền điện tử được nhấn mạnh bằng công nghệ đa chữ ký. Tất cả các ví đa chữ ký hoạt động theo kiến trúc này. Theo thiết kế, tất cả các ví đa chữ ký cần chữ ký M của N cho bất kỳ giao dịch nào để thực hiện. Ví dụ, nếu

bạn có ví đa chữ ký (Multi Signature wallet) được cấu hình cho 3 trong số 5 chữ ký, điều này có nghĩa là đối với bất kỳ giao dịch nào được xử lý, bạn sẽ cần ít nhất ba trong năm chữ ký để phê duyệt trước khi giao dịch được xác nhận.

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.

Về cơ bản, các quỹ được lưu trữ trên một địa chỉ đa chữ ký chỉ có thể được truy cập bằng cách sử dụng 2 hoặc nhiều chữ ký. Vì vậy, việc sử dụng một ví đa chữ ký cho phép người dùng tạo thêm một lớp bảo mật cho quỹ của mình. Nhưng trước khi đi xa hơn, điều quan trọng là phải hiểu những nét cơ bản của một địa chỉ Bitcoin chuẩn, dựa trên đơn chìa khóa thay vì đa chìa khóa (địa chỉ một chìa khóa).

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.

Việc quản lý một địa chỉ đơn chìa khóa là nhanh hơn và dễ dàng hơn so với một địa chỉ đa chìa khóa, nhưng có một số vấn đề, đặc biệt là liên quan đến bảo mật. Với việc có một chìa khóa duy nhất, quỹ được bảo vệ bởi một điểm chịu lỗi duy nhất, và đó là lý do tại sao bọn tội phạm mạng liên tục phát triển các kỹ thuật lừa đảo mới để ăn cắp tiền của người dùng tiền điện tử.

Hơn nữa, các địa chỉ đơn chìa khóa không phải là lựa chọn tốt nhất cho các doanh nghiệp có liên quan đến tiền điện tử. Hãy tưởng tượng về trường hợp quỹ của một công ty lớn đang được lưu trữ tại một địa chỉ tiêu chuẩn có một chìa khóa cá nhân tương ứng. Điều này có nghĩa là chìa khóa cá nhân sẽ được giao phó cho một người hoặc cho nhiều người cùng một lúc – và rõ ràng đó không phải là cách an toàn nhất.

Ví đa chữ ký cung cấp một giải pháp tiềm năng cho cả hai vấn đề này. Không giống như địa chỉ đơn chìa khóa, quỹ được lưu trữ trên một địa chỉ đa chữ ký chỉ có thể được chuyển đi nếu có đa chữ ký (được tạo ra bằng cách sử dụng các chìa khóa cá nhân khác nhau).

Theo cách cấu hình cho một địa chỉ đa chữ ký, việc mở khóa có thể yêu cầu sự kết hợp của các chìa khóa khác nhau: 2-of-3 là phổ biến nhất, trong đó chỉ có 2 chữ ký là đủ để truy cập vào quỹ của một địa chỉ 3 chữ ký. Tuy nhiên, có nhiều biến thể khác, chẳng hạn như 2-of-2, 3-of-3, 3-of-4, v.v.

Các tài khoản đa chữ ký (multisig) là tài khoản Bitcoin không chuẩn phổ biến nhất cho đến nay và đã được sử dụng từ năm 2012. Các địa chỉ thay vì 1, thì sẽ bắt đầu bằng 3.

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.

Tính năng này thường hoạt động giống như cách các ngân hàng cần ký tên. Tuy nhiên, kể từ khi công nghệ Blockchain không hoạt động dựa trên sự tin tưởng, nó được xây dựng trên sự đồng thuận và mật mã, thứ khiến cho nó hầu như không thể đánh bại. Do đó, một tổ chức hoặc cá nhân sẽ không thể giữ tiền của bạn một cách tùy ý tại bất cứ thời điểm nào.

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. Có thể ví Blockchain như một cuốn sổ cái ghi lại toàn bộ dữ liệu trong hệ thống. Blockchain khác với các dữ liệu thông thường ở cấu trúc lưu trữ dữ liệu. Blockchain sẽ thu thập thông tin dữ liệu và nhóm chúng thành các khối chứa tập hợp nhiều thông tin .Có thể khẳng định blockchain là một công nghệ rất mạnh mẽ. Nó cung cấp một lớp đồng thuận, lớp này tổ chức và ghi lại các sự kiện. Cơ sở hạ tầng này cho phép những người dùng như chúng ta xây dựng được các nền kinh tế, và thậm chí là cả các chính phủ, phân quyền.

Tuy nhiên, công nghệ mã hóa được sử dụng để vận hành một blockchain cơ bản có thể được dựa hoàn toàn trên các chữ ký số. Trong blockchain, các khóa cá nhân tượng trưng cho danh tính, còn chữ ký là một tuyên bố hoặc một xác nhận công khai mà danh tính đó đưa ra. Blockchain sẽ yêu cầu các tuyên bố đó và xác thực chúng dựa trên một bộ quy tắc, bộ quy tắc này đảm bảo các chữ ký chính xác và không thể giả mạo được.

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. Do đó, Blockchain tránh được rủi ro từ các bên thứ ba.
- 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 do các đặc điểm của thuật toán đồng thuận và mã hash. Các dữ liệu được lưu trữ mãi mãi.

- 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. Dựa vào đó, có thể kiểm tra và truy xuất lịch sử giao dịch. Mọi người thậm chí có thể được phân quyền để cho phép người khác truy cập một phần thông tin trên Blockchain.

- Tích hợp hợp đồng thông minh: Hợp đồng thông minh là các kỹ thuật số được tạo bởi một đoạn code if-this-then-that (IFTTT) trong hệ thống công nghệ. Hợp đồng này cho phép blockchain tự thực thi mọi thứ mà không cần bên thứ ba tham gia vào hệ thống. Các điều khoản được viết trong hợp đồng thông minh, nó được thực thi khi các điều kiện trước đó được đáp ứng và không ai có thể ngăn chặn hoặc hủy bỏ nó.

- Không thể phá hủy hoặc làm giả: Về lý thuyết, chỉ có máy tính lượng tử mới có thể can thiệp và giải mã blockchain. Blockchain có thể bị phá hủy hoàn toàn khi không còn Internet trên thế giới, nhưng tất nhiên điều này là không thể xảy ra.

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
- Mỗi khối bao gồm 3 thành phần chính: Data (Dữ liệu), Mã Hash của khối hiện tại (Mã hàm băm) và Mã Previous Hash (mã Hash khối trước đó).
- Data (Dữ liệu): Các bản ghi dữ liệu đã xác minh của bạn được bảo vệ bằng các thuật toán mã hóa phụ thuộc vào mỗi chuỗi khối. Ví dụ: thông tin người gửi, người nhận, số lượng coin đã được gửi…
- Mã Hash của khối hiện tại (Mã hàm băm): Đây là một chuỗi ký tự và số được tạo ngẫu nhiên không hoàn toàn giống nhau. Nó đại diện cụ thể cho khối và sử

dụng một thuật toán mã hóa để mã hóa nó. Mã này được sử dụng để phát hiện các thay đổi trong khối. Mã này giống như dấu vân tay của chúng ta, là duy nhất, không trùng nhau.

- Mã Previous Hash (mã Hash khối trước đó): Nó được sử dụng để cho các khối liền kề biết khối nào ở phía trước và khối nào ở sau, để liên kết đúng với nhau. Tuy nhiên khối đầu tiên, bởi vì không có khối nào trước nó nên mã Hash của nó là một chuỗi số 0. Khối đầu tiên này được gọi là Genesis block tức là "Khối nguyên thủy" hay khối gốc.

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.

Ví dụ: Bản ghi hồ sơ cho thấy bạn muốn bán 3 bitcoin => hệ thống xác nhận rằng có 3 bitcoin trong ví của bạn => bản ghi hợp lệ.

Nếu bạn chỉ có 1 bitcoin => hệ thống xác định rằng ví của bạn không có đủ bitcoin cho giao dịch => bản ghi không hợp lệ.

Tiếp theo, các bản ghi đã được xác minh có giá trị của bạn và một loạt các bản ghi đã được xác minh từ các nhà giao dịch khác sẽ được nhóm lại thành một khối.

Cuối cùng, khối (Block) mới được tạo được sẽ kết nối khối trước đó bằng cách kết nối Previous Hash của khối được thêm vào và kết quả là tạo thành một chuỗi khối (Blockchain).

Nếu kẻ trộm đột nhập muốn thay đổi bất kỳ thông tin nào trong Blockchain, chúng phải thay đổi toàn bộ thông tin của khối và chuỗi. Điều đó gần như là bất khả thi và chỉ cần thay đổi nhỏ cũng khiến chúng ta phát hiện ra lỗ hổng. Vì vậy Blockchain gần như an toàn tuyệt đối.

1.2.3. Ứng dụng của Blockchain trong thương mại điện tử

Ứng dụng Blockchain trong bảo mật & bảo vệ dữ liệu

Thương mại điện tử liên quan đến rất nhiều giao dịch tài chính. Đây là nơi có thể ứng dụng Blockchain trong việc làm cho các giao dịch này an toàn hơn và nhanh hơn.

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.

- Không có người trung gian: Với tiền điện tử, hầu như không có người trung gian như ngân hàng, nền tảng thanh toán như PayPal hoặc mạng thanh toán như Visa, MasterCard.
- Hệ thống phi tập trung: Không có bên thứ ba hoặc chính phủ nào có thể thao túng hoặc thông qua các giao dịch của bạn. Các ngân hàng hoặc chính phủ không thể thổi phồng hoặc phá giá tiền điện tử, các tình huống địa chính trị cũng không có bất kỳ ảnh hưởng nào đến tiền điện tử.
- Dễ sử dụng: Tiền điện tử dễ sử dụng hơn cho cả người bán và người mua Thương mại điện tử. Người bán được hưởng lợi từ phí xử lý thấp hoặc bằng không, không có khoản bồi hoàn hoặc phí sử dụng quốc tế và trên hết là thiết lập nhanh chóng và dễ dàng. Người mua được hưởng lợi từ việc dễ dàng thanh toán, mạng an toàn và không có phí đánh dấu khi thanh toán bằng các đơn vị tiền tệ khác.
- Giao dịch nhanh hơn: Các khoản thanh toán được thực hiện bằng tiền điện tử chỉ mất vài giây, không giống như các loại tiền truyền thống có thể mất thời gian, đặc biệt là trong các giao dịch quốc tế. Không có giới hạn về số tiền có thể được chuyển hoặc thời gian mà bạn có thể thực hiện giao dịch.

Quản lý chuỗi cung ứng tốt hơn

Quản lý chuỗi cung ứng là mối quan tâm chính đối với bất kỳ doanh nghiệp Thương mại điện tử nào ngoài đó.

Việc ứng dụng Blockchain có tiềm năng giảm chi phí vận chuyển và cung cấp khả năng theo dõi tốt hơn cho người mua. Nhiều nhà bán lẻ trực tuyến lớn đang thử nghiệm và triển khai các hệ thống blockchain vào chuỗi cung ứng của họ. 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. Blockchain cũng có thể giúp tránh giả mạo dữ liệu quan trọng như nguồn gốc sản phẩm, khả năng truy xuất nguồn gốc và thời hạn hoặc hiệu lực của hàng hóa dễ hư hỏng. Bằng cách này, nó làm cho hệ thống quản lý hàng tồn kho tổng thể trở nên mạnh mẽ và tiết kiệm chi phí cho các chủ cửa hàng Thương mại điện tử.

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

Đối với cấu trúc truyền thống, nhờ có các cơ quan trung ương mà mà sự đồng thuận không phải là vấn đề cần được giải quyết thường xuyên. Nhưng đối với blockchain là một hệ thống phân tán thì ngược lại. Từng giao điểm đóng vai trò vừa

là máy chủ và cũng là nơi lưu trữ data dữ liệu. Chính vì thế, giao điểm này cần phải trao đổi data cùng với các giao điểm khác để tạo ra sự đồng thuận. Điều này dẫn đến các thuật toán đồng thuận blockchain ra đời.

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:

- Đối với thị trường tập trung, mọi vấn đề đều được xử lý và thông tin được tập trung bởi một cơ quan hay còn gọi là cơ quan trung ương. Thế nhưng đối với Blockchain, đây là một hệ thống phi tập trung, nó phổ rộng khắp các nơi thế giới. 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. Nó giúp các hoạt động diễn ra một cách an toàn và chính xác hơn.

1.3.2. Các loại thuật toán đồng thuận

Trong thực tế, có rất nhiều thuật toán đồng thuận được sử dụng. Tuy nhiên có 4 thuật toán đồng thuận hàng đầu được sử dụng phổ biến nhất gồm: Bằng chứng công việc PoW – Proof of Work, Bằng chứng cổ phần PoS – Proof of Stake, Bằng chứng ủy quyền cổ phần DPoS – Delegated Proof of Stake và Cơ chế đồng thuận chống gian lận BFT – Byzantine Fault Tolerance.

Bằng chứng công việc PoW – Proof of Work:

Là thuật toán đồng thuận thành công đầu tiên cho công nghệ blockchain. Hiện nay, Proof of Work vẫn đang được sử dụng bởi Bitcoin và một số các đồng cryptocurrency khác như Ethereum, Litecoin, ZCash, Monero và một số đồng khác.

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. Ví dụ như với Bitcoin, "thợ mỏ" cạnh tranh để thêm một bộ giao dịch, được gọi là một block, vào chuỗi blockchain toàn cầu trong mạng lưới. Để làm được điều này, người khai thác mỏ phải là người đầu tiên tìm ra "nonce" một cách chính xác, một chữ số sẽ được nối vào cuối chuỗi để tạo một hash bắt đầu với bằng một số chữ số "0".

Ưu điểm lớn nhất của Proof of Work đã được chứng minh là khả năng hoạt động được trong một thời gian dài cỡ vào năm – đây là ưu điểm vượt trội hơn hẳn của Proof of Work so với các thuật toán đồng thuận khác.

Về khuyết điểm, Proof of Work tiêu thụ rất nhiều điện năng cho quá trình khai thác mỏ và thông lượng giao dịch thấp.

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. Thay vì "đào" bằng cách giải quyết những vấn đề khó khăn và phức tạp đòi hỏi chuyên sâu về tính toán để xác minh các giao dịch, người thợ mỏ sẽ đặt cọc tiền vào các giao dịch bằng cách khóa khoản cryptocurrency đó lại. Thợ mỏ được chọn để hoàn thành block này thường được lựa chọn dựa trên các tiêu chí như giá trị mà họ đặt vào mạng lưới so với tổng giá trị của mạng lưới hoặc thời gian mà khoản cryptocurrency sẽ bị khóa hoặc tiêu chí khác để đảm bảo rằng người thợ đào phù hợp với lợi ích lâu dài của cả mạng lưới.

Hiện nay, thuật toán Proof of Stake được sử dụng bởi Peercoin, Decred và Ethereum cũng đang có những động tác chuyển đổi thuận toán đồng thuận của mình từ Proof of Work sang Proof of Stake.

Ưu điểm của Proof of Stake là hiệu quả sử dụng năng lượng và khả năng ngăn chặn các cuộc tấn công tốt hơn Proof of Work, tuy nhiên ưu điểm này chưa được chứng minh là thực sự hiệu quả khi sử dụng để thực hiện các dự án lớn.

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

Tuy Delegated Proof of Stake có tên tương tự như Proof of Stake nhưng đi vào chi tiết thì hoạt động của hai thuật toán này là hoàn toàn khác nhau.

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. DPoS vẫn "phân cấp" theo ý nghĩa rằng tất cả trong mạng lưới tham gia vào việc lựa chọn các nút nào xác thực các giao dịch, nhưng tập trung theo nghĩa một nhóm nhỏ hơn đưa ra các quyết định làm tăng tốc độ giao dịch và xác minh.

DPoS đảm bảo sự trung thực và công bằng bằng việc thực hiện các hoạt động bỏ phiếu liên tục và cũng liên tục xáo trộn trong hệ thống để đảm bảo những người được chọn trung thực và có trách nhiệm.

Ưu điểm của DPoS là khả năng mở rộng và thực hiện quá trình xác minh giao dịch nhanh, nhưng có khuyết điểm là nó chỉ tập trung vào một phần và mô hình quản trị vẫn chưa được chứng minh là có hiệu quả trong một dự án lớn.

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. Ưu điểm của BFT khả năng mở rộng và các giao dịch với chi phí thấp.

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 [11] 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.

Để giải thích rõ hơn, trước hết tôi sẽ mô tả ngắn gọn cách thức tạo các địa chỉ trên thiết kế blockchain cổ điển. Một cách đơn giản, chúng ta có thể tạo một địa chỉ mới bằng cách tạo một khóa cá nhân, sau đó tính toán khóa công khai từ khóa cá nhân. Sau đó, chúng ta dẫn xuất địa chỉ công khai từ khóa công khai.

Bây giờ, bằng cách sử dụng TSS, 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). Từ khóa công khai, chúng ta có thể lấy được địa chỉ công khai theo cách thức giống như ở hệ thống truyền thống, khiến cho blockchain không thể biết địa chỉ được tạo ra như thế nào. Cơ chế này có ưu điểm là khóa cá nhân sẽ không còn là điểm hư hỏng duy nhất nữa, bởi vì mỗi bên chỉ nắm giữ một phần của nó.

Quy trình tương tự được sử dụng khi ký các giao dịch. Khi ký các giao dịch, thay vì chỉ một bên ký với khóa cá nhân của mình, chúng ta chạy một quy trình tạo chữ ký phân tán có sự tham gia của nhiều bên. Như vậy mỗi bên có thể tạo một chữ ký hợp lệ, miễn là họ hành động trung thực. Như vậy, chúng ta đã chuyển đổi từ tính toán cục bộ (một điểm hư hỏng duy nhất) sang tính toán tương tác. Thực hiện tạo khóa phân tán theo cách thức cho phép các cấu trúc tiếp cận khác nhau: cài đặt chung "t trong tổng số n" sẽ có thể chống lại lên tới t sự hư hỏng tùy ý trong các hoạt động vận hành liên quan đến khóa cá nhân mà không ảnh hưởng đến tính bảo mật.

1.4.1. Ví ngưỡng

Có một số khác biệt giữa ví dựa trên công nghệ TSS và ví tiền mã hóa. Ví truyền thống thường tạo một cụm từ chứa thông tin khôi phục (seed phrase) và sử dụng nó để dẫn xuất các địa chỉ theo phương thức tất định. Sau đó người dùng có thể dùng cấu trúc tất định theo cấp bậc (hierarchical deterministic - HD) để 1) xác định các khóa cá nhân tương ứng với các địa chỉ công khai của ví và ký các giao dịch với các khóa đó và 2) khôi phục tất cả các khóa của ví bằng cách sử dụng cụm từ chứa thông tin khôi phục.

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. Các cụm từ chứa thông tin khôi phục được tạo riêng biệt và chúng không bao giờ được kết hợp với nhau để một bên không thể dẫn xuất các khóa cá nhân từ thông tin khôi phục của nó.

Các ví dựa trên TSS cũng có một tính năng bảo mật thú vị, tính năng này cho phép xoay khóa cá nhân mà không phải thay đổi khóa công khai và địa chỉ blockchain tương ứng. Xoay khóa cá nhân, hay còn gọi là chia sẻ bí mật chủ động, vẫn không phải là một giao thức MPC khác sử dụng các phần thông tin bí mật làm dữ liệu đầu vào và xuất kết quả đầu ra là một tập hợp thông tin bí mật mới. Có thể xóa các phần thông tin bí mật cũ và sử dụng các phần thông tin bí mật mới theo cách tương tự.

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. Có thể xây dựng các ứng dụng phân quyền, các giải pháp mở rộng lớp 2, hoán đổi nguyên tử, pha trộn, kế thừa và các tính năng khác trên khung TSS. Cuối cùng, điều này sẽ cho phép thay thế các hoạt động vận hành hợp đồng thông minh trên chuỗi đắt đỏ và rủi ro bằng các lựa chọn thay thế rẻ tiền và đáng tin cậy hơn.

Một số ví dụ có thể kể đến bao gồm: Khóa nhiều bước nhảy sử dụng chữ ký hai bên một cách thông minh, và với mạng lưới kênh thanh toán bảo mật và riêng tư hơn, nó có thể được sử dụng để thay thế mạng lưới Bitcoin lightning network. ShareLock[10] có lẽ là giải pháp pha trộn trên chuỗi có chi phí hợp lý nhất cho Ethereum, dựa trên việc xác thực một chữ ký ngưỡng duy nhất.

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

ECDSA là viết tắt của Elliptic Curve Digital Signature Algorithm - thuật toán sinh chữ ký số dựa trên đường cong Elliptic. ECDSA được sử dụng để tạo chữ kí số cho dữ liệu, giúp chống lại sự giả mạo cũng như làm sai lệch dữ liệu, cung cấp một phương pháp xác thực mà không ảnh hưởng đến tính bảo mật của dữ liệu gốc. ECDSA được ứng dụng rộng rãi trong rất nhiều lĩnh vực cần tính bảo mật và sự riêng tư dữ liệu, đặc biệt như trong Blockchain.

ECDSA là thuật toán mã hoá bất đối xứng. Nó khác với các mã hoá đối xứng khác như AES, ta có một key duy nhất để mã hoá dữ liệu và giải mã. Nó đồng nghĩa với việc biết key là biết tất cả, và không biết key thì không biết gì. ECDSA thì khác, nó có một cặp key: private key (Khóa bí mật) và public key (Khóa công khai). Private key dùng để mã hoá, public key dùng để xác nhận (verify) tính đúng đắn của dữ liệu đã được mã hoá này, và chỉ vậy mà thôi. Public key không thể giải mã được dữ liệu đã được mã hoá, do đó dữ liệu gốc luôn luôn được an toàn. Sự hữu ích của nó thể hiện ở việc nó có thể tạo ra được chữ ký số. Với mỗi văn bản, hay giao dịch, hay dữ liệu bất kì, ta có thể tạo ra được một dữ liệu kèm chữ ký. Chữ ký này chỉ có thể được tạo ra bởi người có thông tin về khoá bí mật, và bất cứ ai cũng có thể tiếp cận được khoá công khai để có thể xác minh chữ ký này. Thuộc tính hữu ích này của mật mã bất đối xứng cho phép bất cứ ai cũng có thể xác minh mọi chữ ký trên mọi giao dịch, trong khi vẫn đảm bảo rằng chỉ những chủ sở hữu khoá bí mật mới có thể tạo ra được chữ ký hợp lệ.

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.

Vì sao private key lại quan trọng? Vì nó tạo ra chữ ký, và chứng minh rằng dữ liệu, hay tài sản thuộc về quyền sở hữu của người có private key. Chính vì vậy việc bảo vệ private key là vô cùng quan trọng. Tuyệt đối không chia sẻ private key cho ai khác, và hãy giữ private key ở một nơi an toàn, vì một khi mất đi sẽ không thể khôi phục lại được, đồng nghĩa với việc ta có thể sẽ mất đi toàn bộ quyền chứng thực với dữ liệu hay tài sản của ta

Khóa công khai:

Khác với private key, public key được công khai cho tất cả mọi người. Public key được tạo ra bởi phép nhân với private key trong đường cong Elliptic, ta sẽ nói rõ hơn ở phần tiếp theo.

Phép nhân đường cong Elliptic là một phép toán trap door (cửa lật), có nghĩa là nó dễ tính theo một chiều (phép nhân) và không thể tính được theo chiều ngược lại (phép chia). Do đó người sở hữu private key có thể dễ dàng tạo ra khoá công khai và yên tâm chia sẻ với mọi người mà không lo lắng rằng ai đó có thể đảo ngược public key để chiếm lấy private key của mình.

Lý thuyết này tạo nên nên tảng cho các chữ ký số an toàn và không thể làm giả, ví dụ được dùng để chứng minh quyền sở hữu đối với Bitcoin hay Ethereum trên các mạng blockchain.

Đường cong Elliptic (EC)

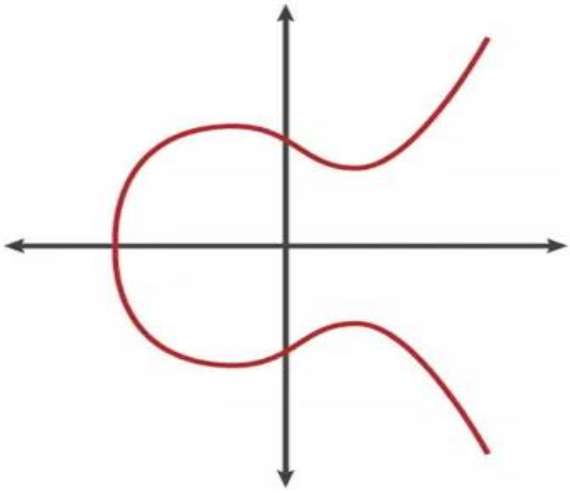
Công thức của đường cong Elliptic là:

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

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



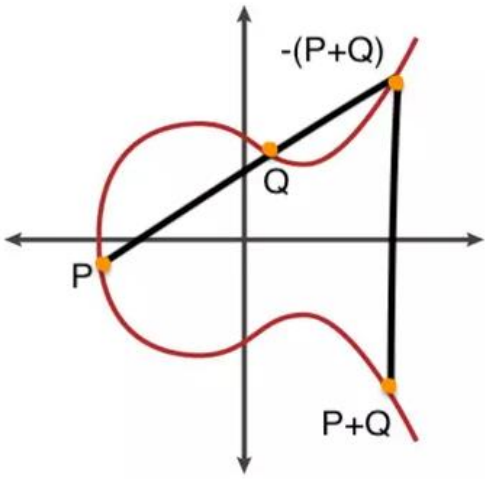
Hình 2.1. Minh họa đường cong Elliptic

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.

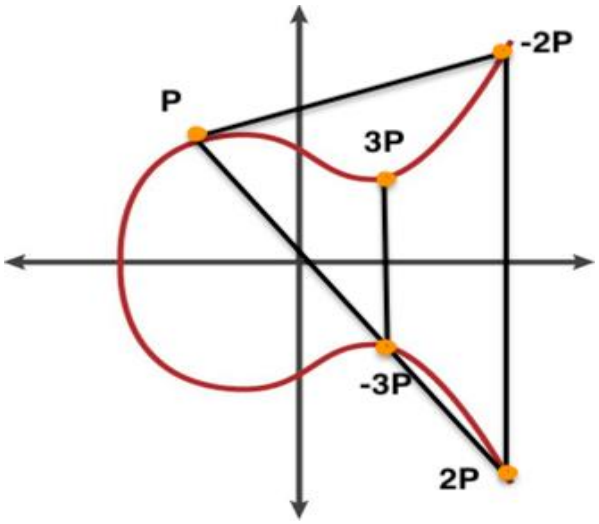


Hình 2.2. Mô tả phép cộng được tiến hành trong đường cong Elliptic

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.

Ví dụ trong phép toán tính 3P, ta sẽ tính 2P bằng cách tính P+P. Theo cách cộng ở bên trên, ta vẽ đường thẳng nối P và P, ở đây chính là tiếp tuyến của đường cong, nó cắt đường cong tại điểm -2P, lấy đối xứng qua trục hoành ta có 2P. Tiếp tục vẽ đường thẳng nối giữa 2P và P, cắt đường cong tại -3P, lấy đối xứng ta có 3P.



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:

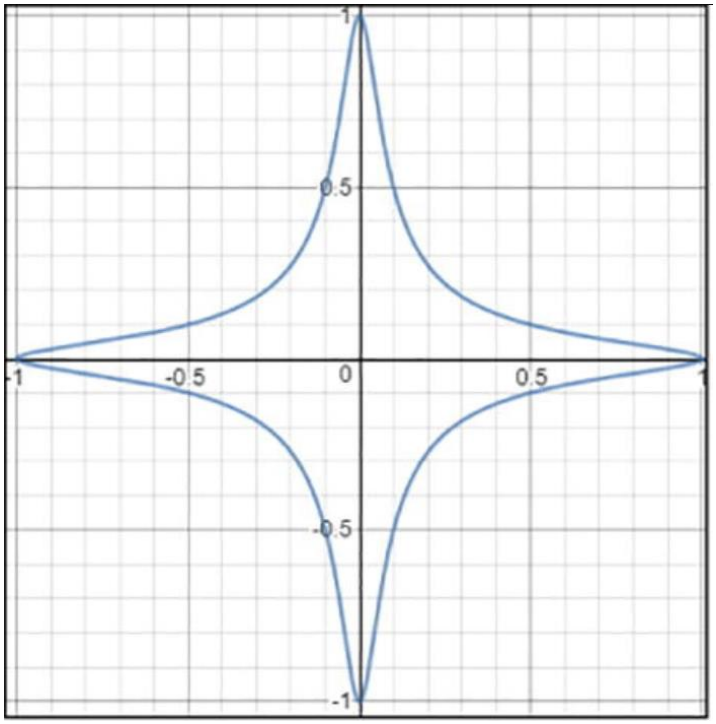
$$QA=dA\times G$$

với Bitcoin hay Ethereum thì:

G=04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

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. Đó là lý do tại sao ta có thể sinh ra khoá công khai từ khoá bí mật và có thể chia sẻ khoá công khai này với tất cả mọi người, mà không thể dùng khoá công khai để tìm ngược lại về khoá bí mật.

2.1.2. Hệ mật trên đường cong Edwards (EdDSA)



Hình 2.4. Đường cong Edwards

Đường cong Elliptic là một trong những phương pháp mã hóa mạnh mẽ nhất đang được ứng dụng rộng rãi ở thời điểm hiện tại, trong đó đường cong Edwards do Edwards (2007), đang là dạng ê líp mới nhất và tốt nhất. Thuật toán chữ ký số theo đường cong elip có thể giúp gửi thông tin nhanh hơn so với những thuật toán hiện nay như là RSA, DSA hay ElGamal. Khi được kết hợp với đường cong Edwards, thuật toán chữ ký kỹ thuật số theo đường cong Edwards (viết tắt là EdDSA) là một

sáng kiến chữ ký kỹ thuật số sử dụng những biến thể của chữ ký Schnorr dựa trên đường cong Edwards dạng xoắn.

Đường cong Edwards là sự tổng quát của EC để đạt được độ bảo mật siêu cao trên thiết bị hạn chế tài nguyên. Nó có khả năng cung cấp sự bảo vệ tương tự với một chiếc chìa khóa nhỏ hơn. Một chìa khóa nhỏ giúp giảm chi phí tính toán. Chi phí phát sinh ít tốn kém hơn EC dựa trên phép nhân điểm, cộng điểm và các phép toán vô hướng trên 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[13] 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 (x1, y1) và (x2, y2) trong đường cong Edward, trong Phương trình (3) sau đây, (x3, y3) 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

Thuật toán chữ ký số đường cong Edwards (EdDSA) là một sơ đồ chữ ký điện tử sử dụng một biến thể của chữ ký Schnorr[9]. EdDSA mạnh và đơn giản hơn ECDSA. EdDSA không phụ thuộc vào bộ tạo số ngẫu nhiên. Trong ECDSA, nếu hai chữ ký khác nhau được tạo bởi cùng một số ngẫu nhiên, khóa riêng sẽ bị rò rỉ hoặc gây ra sự cố xung đột. 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) (7)

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

Sự hội tụ này cho thấy sự cần thiết phải có một lược đồ chữ ký tốt hơn. Khả năng ứng dụng đường cong Edwards được cải thiện có vẻ khả thi và là một giải pháp thay thế khả thi cho sơ đồ hiện có.

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.

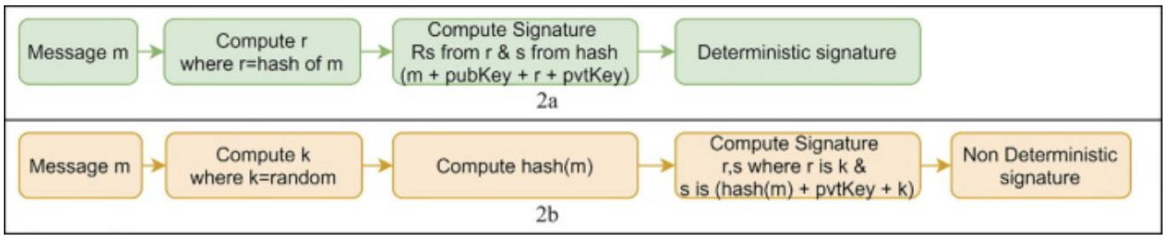
Đường cong	Phương trình	Đồ thị	Khái quát
Edwards	$x^2 + y^2 = 1 + dx^2 y^2$	x ^ 2 + y ^ 2 = 1–300 × ^ 2 y^2	nhanh và toàn vẹn
Elliptic	$y^2 = x^3 + ax + b$	y ^ 2 = x ^ 3–0.4 × + 0.7	tin cậy nhưng chậm và không toàn vẹn

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.



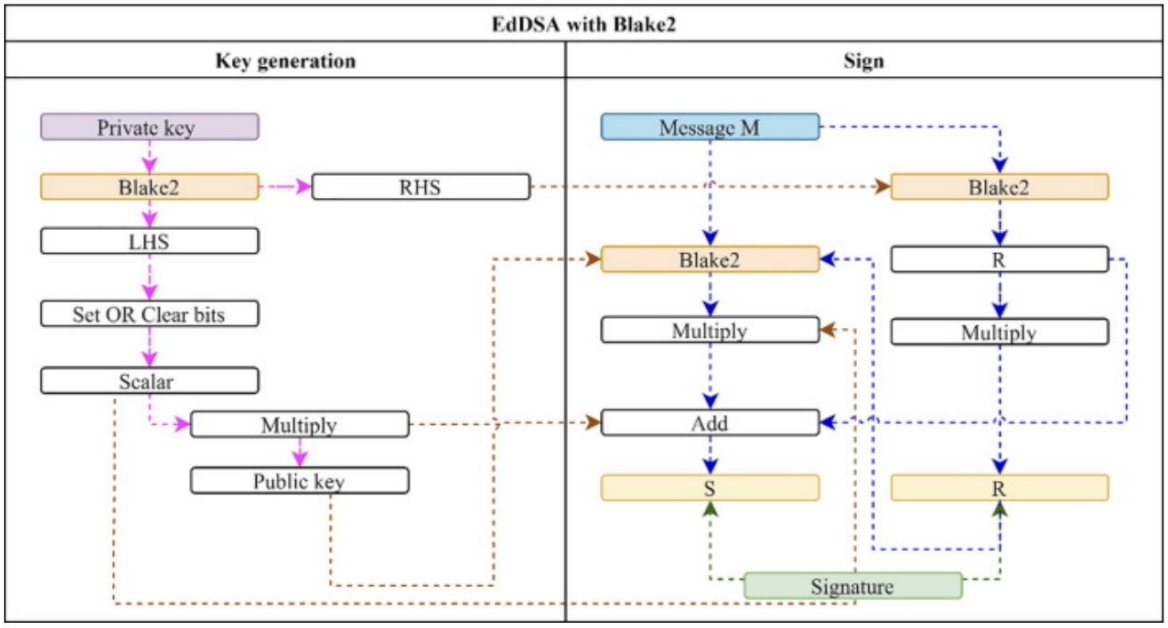
Hình 2.7.a) Luồng EdDSA. b) Luồng ECDSA

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) [14].

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.

Trong chức năng xác minh được trình bày trong Thuật toán 2.9, khóa công khai (pK), thông điệp tổng hợp và chữ ký tạo thành đầu vào. Đầu ra của hàm này là Boolean. Do đó, nó là Đúng trong trường hợp xác minh tích cực và Sai trong trường hợp xác minh không thành công.

```
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)
```

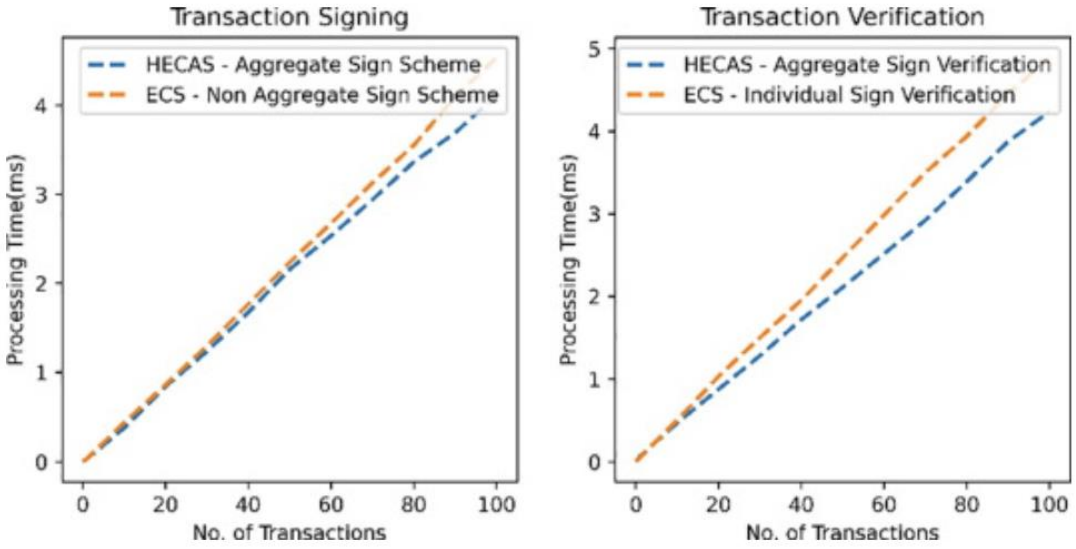
Hình 2.11. Xác minh chữ ký

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.

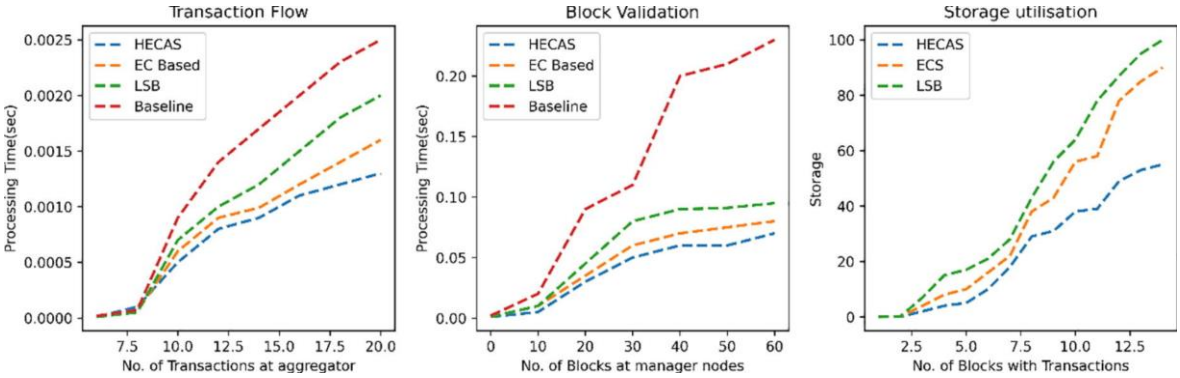
2.3. Phân tích tính hiệu quả của mô hình

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 T_{Sign}

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



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 [9]: 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[9]: 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

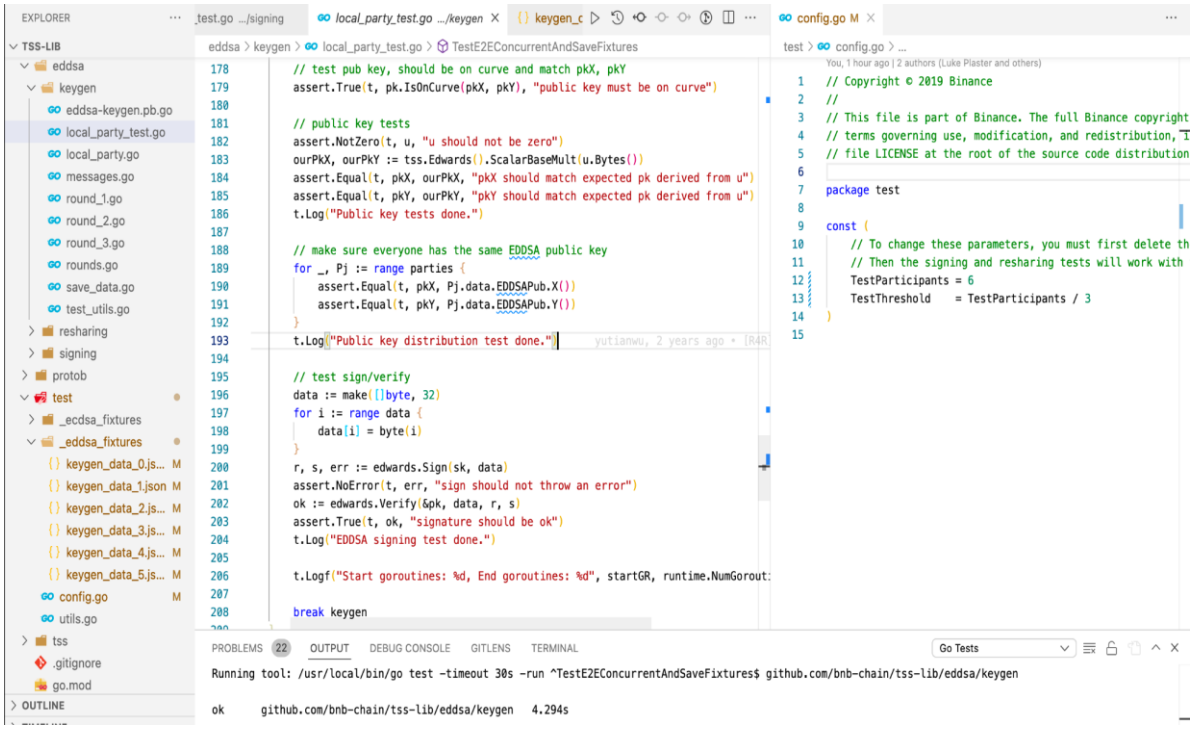
Để triển khai được mô hình trên hệ thống blockchain, tôi sử dụng bộ thư viện:

- 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

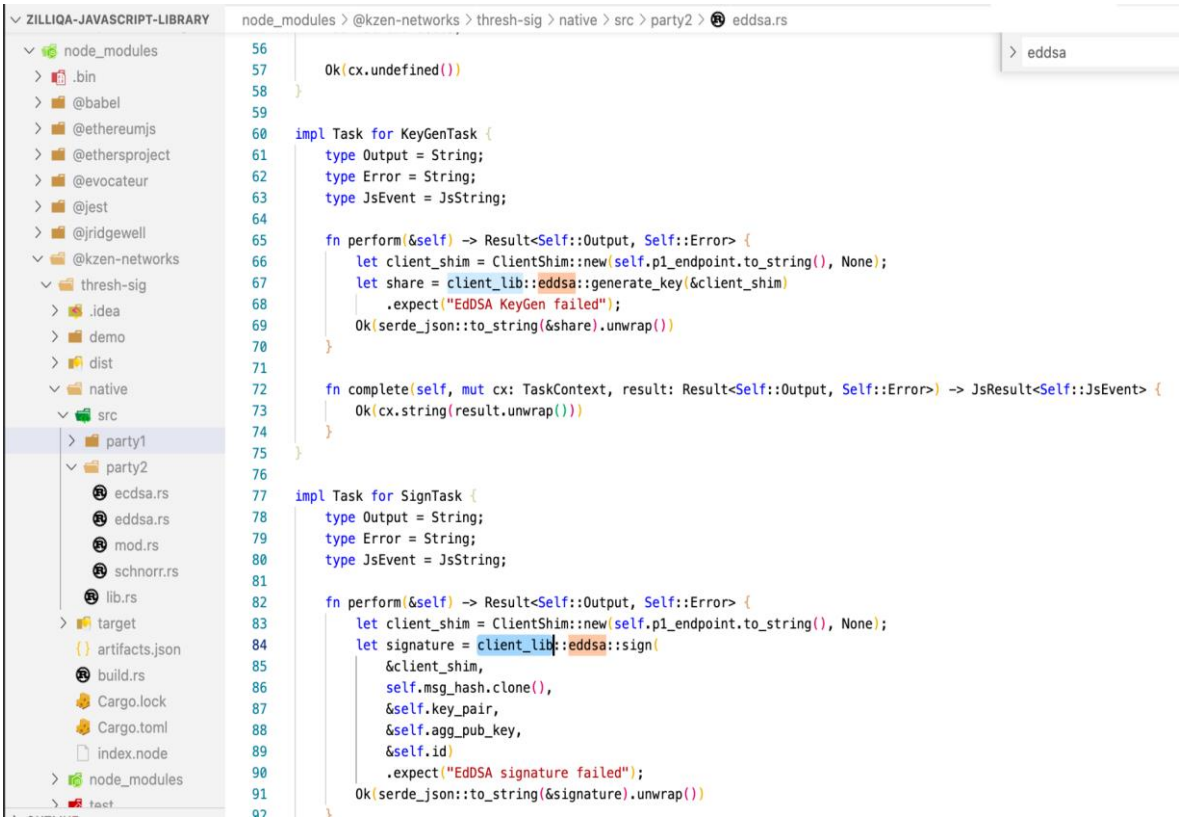
Genarate keys

$go test -timeout 30s -run ^TestE2EConcurrentAndSaveFixtures$ 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



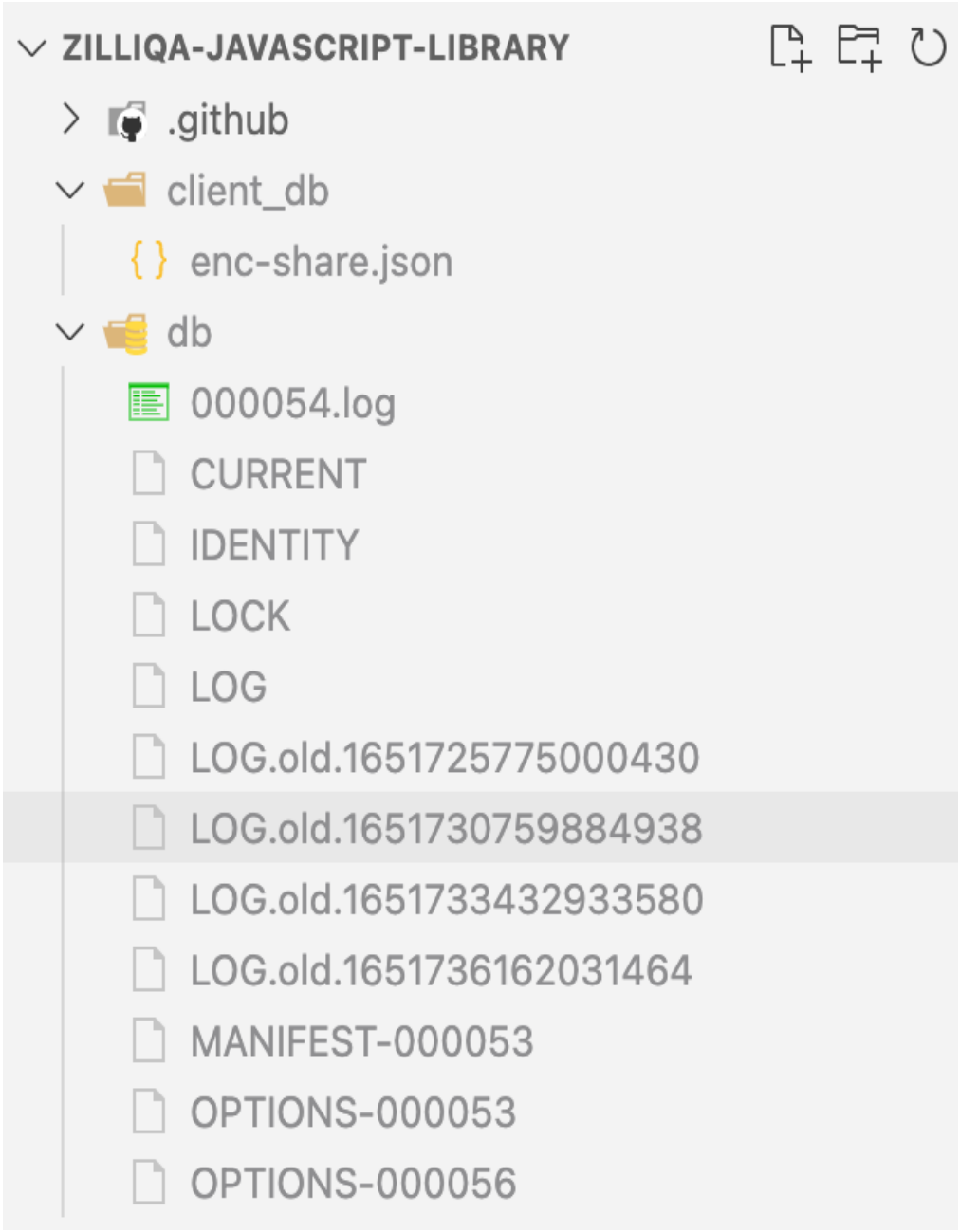
Hình 3.3. Cấu hình ký giao dịch bằng EdDSA

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.

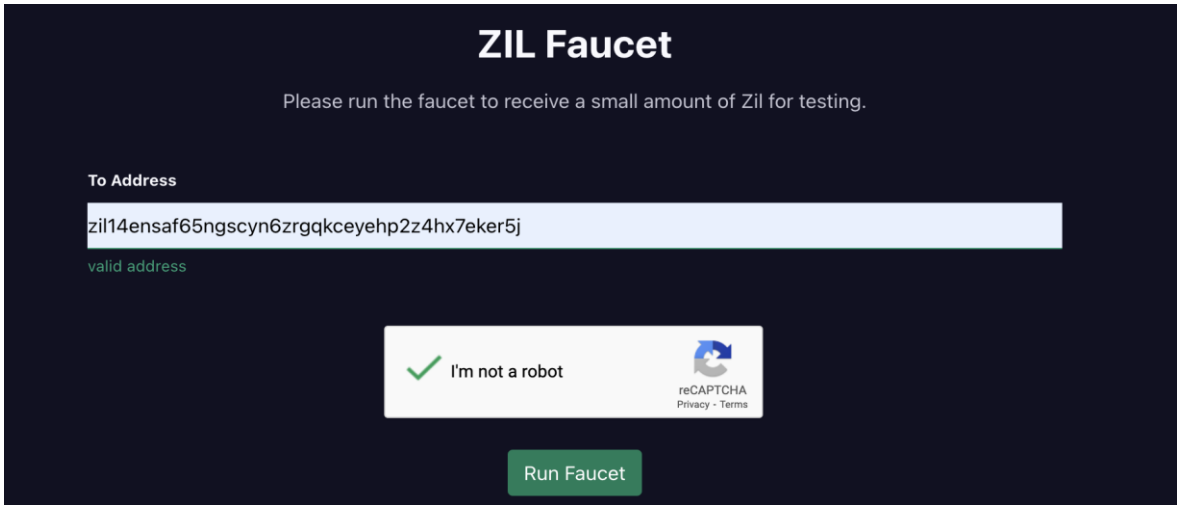
```
async function loadOrCreateWallet() {
  let address;
  let encryptedShare;
  if (fs.existsSync(ENCRYPTED_SHARE_PATH)) {
    encryptedShare = fs.readFileSync(ENCRYPTED_SHARE_PATH);
  }

  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



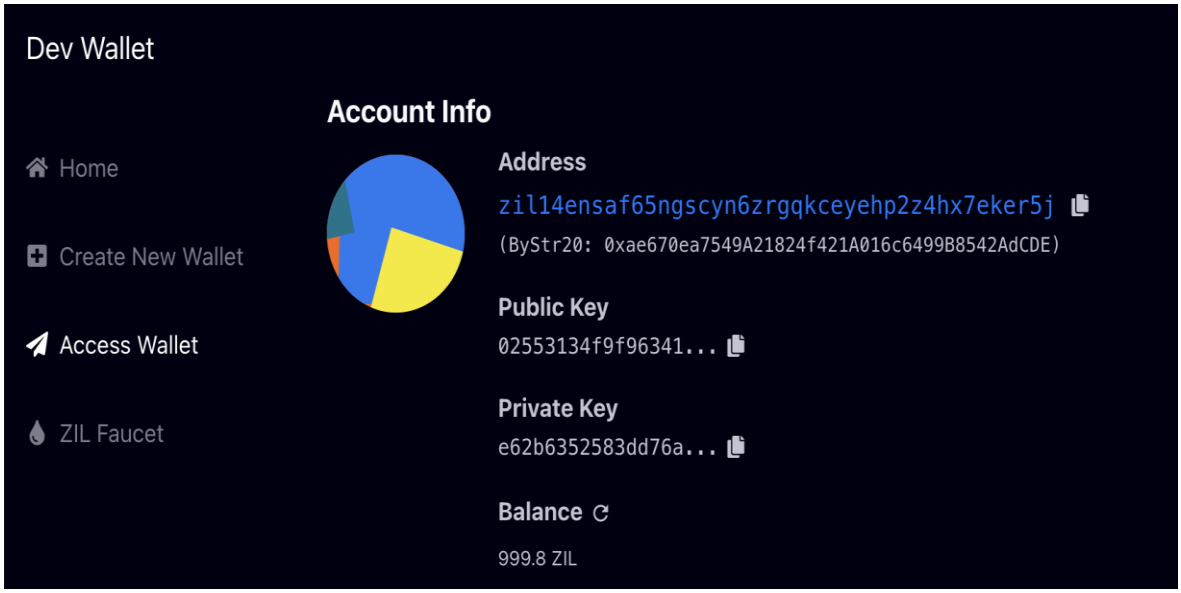
Hình 3.5. Thông tin ví vừa tạo được lưu ở client_db

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

Kiểm tra số dư trong địa chỉ ví vừa tạo



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
```

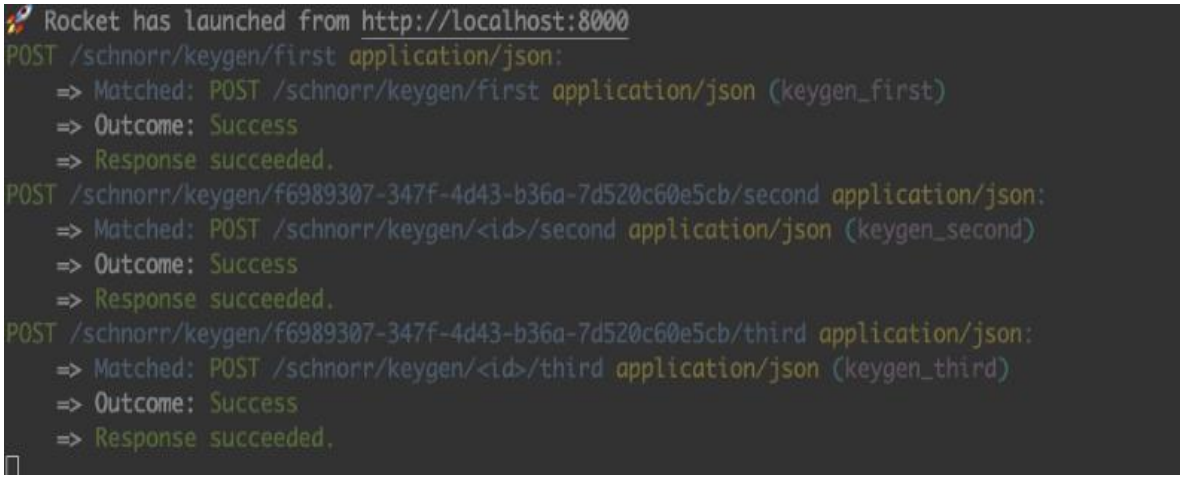
Hình 3.9. Start demo server

```
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
    })
  });
```

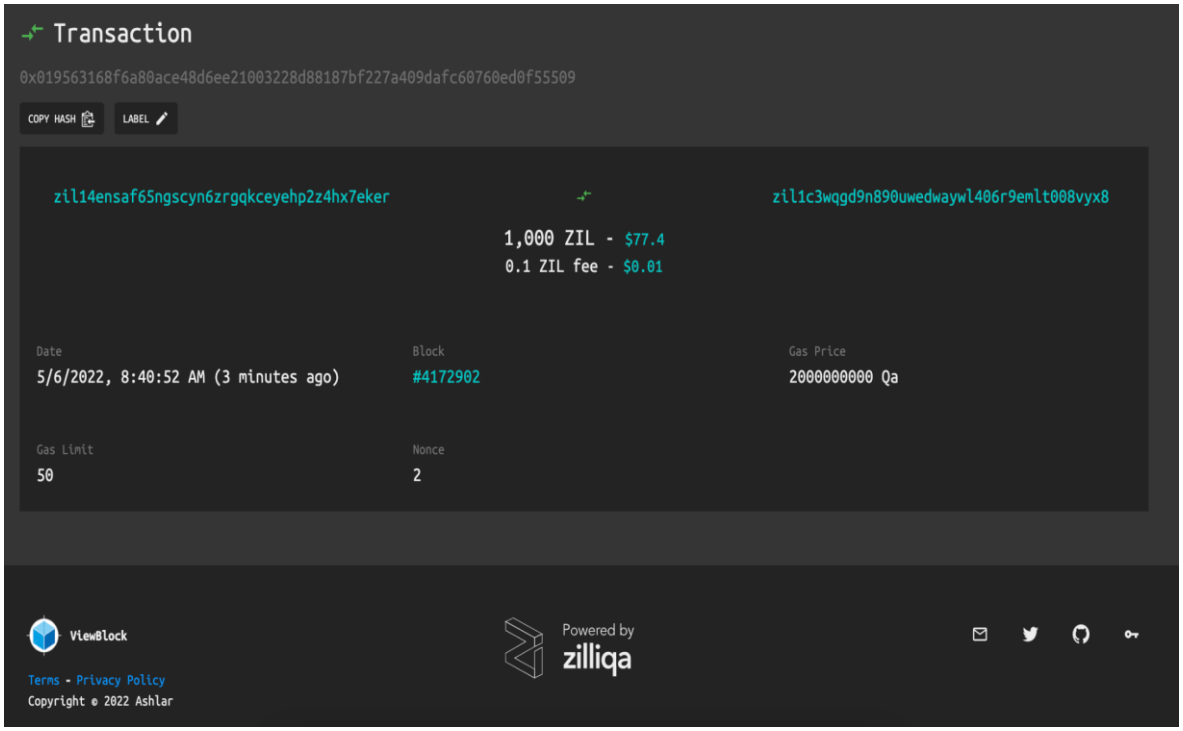
Hình 3.10. Mã code tạo giao dịch chuyển token

```
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[12] 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.

TÀI LIỆU THAM KHẢO

Tiếng Việt

[1]. Đặng Minh Tuấn, "Hệ mật mã hóa khóa công khai dựa trên đường cong elliptic," p. 41, 2016.

Tiếng Anh

[2]. J.-P. Aumasson, A. Hamelink, O. Shlomovits, and Z. X. Israel, "A Survey of ECDSA Threshold Signing."

[3]. M. S. Hwang and T. Y. Chang, "Threshold signatures: Current status and key issues," *Int. J. Netw. Secur.*, vol. 1, no. 3, pp. 123–137, 2005.

[4]. D. H. Kim, R. Ullah, and B. S. Kim, "RSP Consensus Algorithm for Blockchain," *2019 20th Asia-Pacific Netw. Oper. Manag. Symp. Manag. a Cyber-Physical World, APNOMS 2019*, pp. 1–4, 2019, doi: 10.23919/APNOMS.2019.8893063.

[5]. C. Stathakopoulou and C. Cachin, "Research Report: Threshold Signatures for Blockchain Systems," pp. 1–42, 2017.

Website

[6]. https://pkg.go.dev/filippo.io/edwards25519

[7].https://zengo.com/wp-content/uploads/2019/06/breaking_bitcoin19_updated.pdf

[8]. https://datatracker.ietf.org/doc/html/rfc8032

[9]. https://github.com/sipa/bips/blob/bip-taproot/bip-0340.mediawiki

[10]. https://github.com/ZenGo-X/ShareLock

[11]. https://academy.binance.com/vi/articles/what-are-nodes

[12]. https://academy.binance.com/en/glossary/satoshi-nakamoto

[13]. https://github.com/bnb-chain/tss-lib.

[14].https://www.sciencedirect.com/science/article/pii/S1319157821003359#b0115.