Xây dựng giải pháp đảm bảo tính bí mật và quyền riêng tư dựa trên Blockchain sử dụng công nghệ mật mã

Hoàng Sỹ Tương, Đỗ Quang Trung, Lục Như Quỳnh*

Học viện Kỹ thuật Mật mã

Ngày nhận bài 12/9/2022; ngày chuyển phản biện 15/9/2022; ngày nhận phản biện 11/10/2022; ngày chấp nhận đăng 14/10/2022

Tóm tắt:

Ý tưởng của nghiên cứu này là áp dụng các bài toán bảo mật như mã hóa đồng cấu đầy đủ, chữ ký số đường cong elliptic (Elliptic curve digital signature algorithm - ECDSA), thuật toán mã băm an toàn (Secure hash algorithms - SHA) trong việc xây dựng đồng tiền ảo Bitcoin (BTC) của riêng mình dựa trên hệ thống Blockchain mà vẫn đảm bảo được tính bí mật và quyền riêng tư cho đồng tiền ảo được tạo ra. Kết quả, các tác giả đã tạo ra đồng tiền ảo BTC của riêng mình được tích hợp các kỹ thuật bảo mật (gồm thuật toán SHA với độ dài 256 bit, chữ ký số ECDSA với độ dài 384 bit, mã hóa đồng cấu đầy đủ) và đảm bảo quyền riêng tư. Đồng tiền ảo BTC của nhóm tác giả tạo ra đạt được các thuộc tính bảo mật, quyền riêng tư trong các hệ thống và ứng dụng dựa trên Blockchain.

Từ khóa: **chuỗi khối, cơ chế đồng thuận, khóa bí mật, khóa công khai, sổ cái.**

Chỉ số phân loại: **1.2**

Đặt vấn đề

Ngày nay, công nghệ số đã và đang được phát triển rất mạnh mẽ; được hình thành với các thuật ngữ "công dân số, xã hội 4.0, xã hội 5.0", đồng thời được ứng dụng vào nhiều mặt của cuộc sống như trao đổi thông tin, mua bán, học tập… [1-3]. Công nghệ Blockchain ra đời có ý nghĩa quan trọng và đã được áp dụng trong nhiều lĩnh vực như: xử lý thanh toán và tiền tệ, quản lý chuỗi cung ứng... [4-7]. Hệ sinh thái Blockchain đang có sự phát triển mạnh mẽ, điển hình là sự ra đời của đồng tiền mật mã đầu tiên NFT (Non - fungible token) gần đây [7-10].

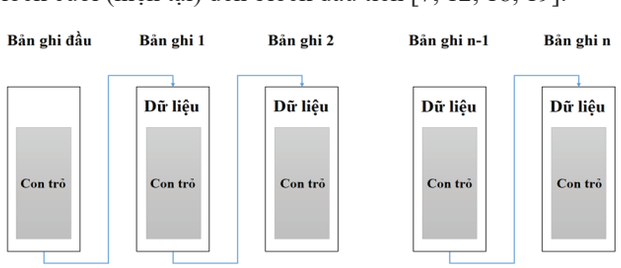
Ứng dụng Blockchain đầu tiên được biết đến là đồng tiền điện tử BTC, đồng tiền này có những ưu điểm nổi bật về độ bảo mật và sự minh bạch trong các giao dịch với thời gian thực [6]. Việc áp dụng được các giải pháp mật mã như: khóa công khai, SHA, chữ ký số ECDSA, mã hóa đồng cấu đầy đủ vào công nghệ Blockchain đã giúp mở ra hướng đi mới có thể đưa công nghệ bảo mật vào cuộc sống (các giao dịch tài chính, ngân hàng...) [9, 11]. Các hệ thống Blockchain được chia ra 3 loại đồng tiền ảo BTC theo 3 hướng chính [12-15]: (1) Các Blockchain công khai cho phép bất kỳ người dùng nào cũng có thể tương tác đọc và ghi dữ liệu (gọi là Public Blockchain) [12]. Quá trình xác thực các giao dịch hệ thống này cần có nhiều Blockchain cùng tham gia [13]; (2) Các Blockchain riêng chỉ cho phép chủ sở hữu hợp pháp mới có quyền đọc dữ liệu mà không được phép ghi dữ liệu và độ an toàn phụ thuộc vào bên tin cậy thứ ba - toàn quyền thay đổi liên quan tới hệ thống (gọi là Private Blockchain), điển hình như đồng tiền ảo Ripple và Ethereum [13, 14]. Do đó, các giao dịch sẽ diễn ra khá nhanh và cần ít Blockchain tham gia; (3) Các hệ thống Blockchain có sự hết hợp của cả hai hệ thống trên gồm cả công khai và riêng được gọi là Permissioned [14, 15]. Do đó, muốn tấn công vào các hệ thống Blockchain này đòi hỏi cần phải có hệ thống lớn với chi phí cao [15-17].

Trong bài báo này, các tác giả tập trung nghiên cứu các giải pháp bảo mật như mã hóa đồng cấu đầy đủ, chữ ký số ECDSA-384 bit, SHA-256 bit. Áp dụng các giải pháp bảo mật này để xây dựng đồng tiền ảo BTC của riêng mình dựa trên hệ thống Blockchain đảm bảo tính bí mật và quyền riêng tư cho nó.

Các nghiên cứu liên quan và phương pháp xây dựng BTC dựa trên Blockchain

Cơ sở lý thuyết xây dựng BTC dựa trên Blockchain

Hình 1 là chi tiết thông tin cấu trúc một khối (block) Blockchain được các tác giả sử dụng trong nghiên cứu này. Bản chất của Blockchain là tập dữ liệu gồm các block được liên kết dưới dạng danh sách cho phép truy xuất ngược từ block cuối (hiện tại) đến block đầu tiên [7, 12, 18, 19].



Hình 1. Kiến trúc của Blockchain [5].

*Tác giả liên hệ: Email: quynhln@actvn.edu.vn

Build a Blockchain-based confidentiality and privacy solution using cryptographic techniques

Sy Tuong Hoang, Quang Trung Do, Nhu Quynh Luc*

Academy of Cryptography Techniques

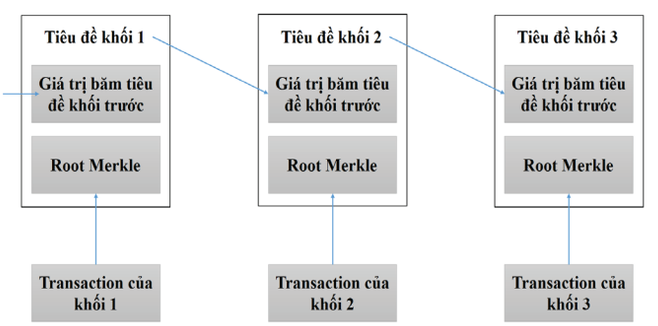
Received 12 September 2022; accepted 14 October 2022

Abstract:

This study aims to apply security problems such as homomorphic encryption algorithm, elliptic curve digital signature algorithm, and secure hash algorithms in building your own bitcoin virtual currency based on the Blockchain system; while still ensuring the confidentiality and privacy of the generated bitcoin virtual currency. The result achieved by the author team, who created their virtual currency bitcoin, has integrated security techniques (including secure hash algorithms with a length size of 256 bits; elliptic curve digital signature algorithm with a length size of 384 bits; full homomorphic encryption) and ensure privacy. The bitcoin virtual currency created by the team of creators achieves these security and privacy properties in Blockchain-based systems and applications.

Keywords: **Blockchain, consensus mechanism, ledger, private key, public key.**

Classification numbers: **1.2**



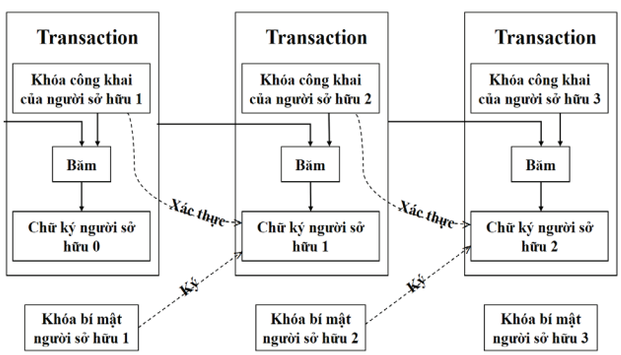
Hình 2. Sơ đồ chuỗi khối kết nối Blockchain [5].

Trong nghiên cứu này, kiến trúc Blockchain cho BTC là sổ cái phân tán (Distributed ledger). Ở hình 2, mỗi block được chứa đựng các thông tin như dữ liệu (data), giá trị mã băm (hash) và mã băm đối chiếu (Hash of previous block). Dữ liệu của block phụ thuộc vào loại Blockchain đang dùng, mã băm được dùng để nhận dạng cho block và mã băm đối chiếu để đảm bảo liên kết cho các "block". Điều này giúp khi có sự thay đổi của mỗi block trong BTC sẽ gây ảnh hưởng tới các block tiếp theo.

Các block có trong BTC được xây dựng với nền tảng công nghệ như: bảo mật [20], hệ thống mạng ngang hàng [21] và lý thuyết trò chơi [22]. Trong đó, giải pháp bảo mật được sử dụng với các hệ như RSA, ECDSA, SHA... để đảm bảo tính bí mật, toàn vẹn, riêng tư và minh bạch cho BTC. Hệ thống mạng ngang hàng được dùng để lưu trữ bản sao cho BTC. Điều này phải tuân thủ luật chơi đồng thuận (Proof of work - PoW, Proof of stake - PoS…) để đảm bảo gia tăng giá trị cho đồng tiền ảo.

Xây dựng giải pháp bảo mật cho BTC dựa trên Blockchain

Giải pháp mật mã sử dụng cho BTC dựa trên Blockchain: Hình 3 là chi tiết cơ chế mã hóa được tích hợp cho BTC dựa trên Blockchain. Các tác giả đã sử dụng sổ cái Blockchain làm giải pháp thực hiện kết nối giữa các block trong BTC dựa trên Blockchain. Khi đó, tích hợp các hệ mật mã cho BTC trên hệ thống Blockchain, BTC được đảm bảo bảo mật và quyền riêng tư khác với các đồng tiền ảo khác ở một số điểm như: (1) Hệ thống sử dụng cho BTC bảo mật khác với các hệ thống khác, các giao dịch được thực hiện khác hẳn với các hệ thống giao dịch khác (như hệ thống ngân hàng…) [3, 6]. Mặt khác, để đảm bảo cho các giao dịch và lưu trữ với BTC lưu hành giống các đồng tiền hiện nay, thì mỗi cá nhân cần phải có ứng dụng cho các giao dịch (được gọi là ví điện tử). Do đó, độ tin cậy cho BTC và ví điện tử phụ thuộc vào các giải pháp bảo mật (như hạ tầng khóa công khai PKI, mã hóa đồng cấu đầy đủ, chữ ký số ECDSA, SHA...) [14, 15, 23]. Chữ ký số ECDSA được sử dụng với mục tiêu xác thực cho các giao dịch của đồng tiền ảo. Nghĩa là, khi có sự thay đổi của block trong BTC giúp cho chủ sở hữu nhận biết được, khi đó đối tượng tấn công khó có thể tấn công vào hệ thống; (2) Cá nhân muốn thực hiện giao dịch với BTC của mình, họ phải có khóa bí mật thì mới mở được ví điện tử của mình. Khi đó, cá nhân mới có thể thực hiện được các giao dịch cần thiết với BTC của mình, bởi vì ngoài chủ sở hữu của ví điện tử thì không có ai có thể mở được ví điện tử đó.



Hình 3. Cơ chế mã hóa trong Blockchain.

Trong trường hợp xảy ra tranh chấp ở block đại diện cuối cùng trong Blockchain của BTC, tức là đã xảy ra gian lận, xác thực sẽ tiến hành xác thực lại tất cả block có mặt tham gia trong hệ thống và quá trình này mất nhiều chi phí cũng như thời gian. Quá trình tính toán với một loạt các block trước khối đại diện được tính tương đương với việc tìm ra một số lượng lớn các số ngẫu nhiên cần thiết để tìm lại được một block và đặt nó vào hệ thống

Blockchain. Điều này, cho thấy BTC được đảm bảo an toàn trước các tấn công hiện nay [15].

Giải pháp tích hợp sổ cái Blockchain cho BTC dựa trên Blockchain: Các tác giả nhận thấy, các thông tin cá nhân của chủ sở hữu cho đồng tiền ảo rất quan trọng và lưu trữ các thông tin này cần phải được đảm bảo an toàn và bảo mật. Sổ cái Blockchain là một giải pháp được sử dụng nhiều trong việc quản lý các thông tin cá nhân liên quan tới BTC. Mỗi sổ cái Blockchain được sử dụng cho đồng tiền ảo giúp cho chủ sở hữu biết được thông tin liên quan tới tài khoản của cá nhân (số dư tài khoản, thông tin các giao dịch liên quan tính tới thời điểm hiện tại và các giao dịch trước đó…).

Thông thường, mỗi sổ cái Blockchain cho BTC bao gồm số dư của từng cá nhân hoặc tài khoản là một phần của bộ hồ sơ kinh tế [24]. Ở đây, sổ cái Blockchain được sử dụng với giải pháp mã nguồn mở có sẵn trên hệ thống Blockchain. Điều này giúp các giao dịch trực tuyến cho BTC được thuận lợi hơn nhiều [25].

Giải pháp SHA (với độ dài 256 bit) giúp đảm bảo xác thực được các giao dịch và nhận dạng được có đúng là BTC đang tham gia trong hệ thống Blockchain. Chữ ký số ECDSA (với độ dài 384 bit) được thiết kế để đảm bảo rằng chữ ký của cá nhân đang được sử dụng trong hệ thống hợp pháp, nhưng điểm khác biệt khi sử dụng chữ ký số ECDSA cho đồng tiền ảo của nghiên cứu này chính là tính ẩn danh. Quá trình ký số và xác thực chữ ký số diễn ra mà chỉ có chủ sở hữu biết và không ảnh hưởng tới hệ thống. Giải pháp mã hóa đồng cấu đầy đủ được các tác giả sử dụng với mục đích mã hóa cho BTC nhằm đảm bảo tính bí mật cho đồng tiền ảo. Điều này giúp BTC được an toàn trước những cuộc tấn công có thể xảy ra trong hệ thống. BTC của các tác giả đã sử dụng các giải pháp bảo mật SHA-256 bit, chữ ký số ECDSA-384 bit và mã hóa đồng cấu đầy đủ để đảm bảo lưu trữ thông tin cá nhân liên quan tới BTC trên sổ cái Blockchain được an toàn và bảo mật đảm bảo quyền riêng tư.

Giải pháp tạo block trên BTC dựa trên Blockchain: Để đảm bảo thực hiện được giao dịch, cá nhân sẽ gửi giao dịch của mình lên hệ thống Blockchain. Khi đó, hệ thống sẽ nhóm vào các block và phân chia giao dịch thành các nhóm gồm: các giao dịch trên cùng block (xảy ra cùng thời điểm); các giao dịch chưa được thực hiện trong block (giao dịch chưa được xác nhận) [4]. Tại mỗi nút trên hệ thống có thể nhóm các giao dịch thành một block và đưa lên hệ thống như là gợi ý gắn vào các block tiếp theo trên hệ thống. Lúc này, bất kỳ người giao dịch nào cũng có thể tạo ra một block mới cho mình. Việc thêm block vào Blockchain cho BTC sẽ mất khoảng 10 phút một lần. Bởi vì, mỗi block chứa mã băm mà việc tìm được giá trị mã băm này tương đương với độ khó của bài toán tìm hàm ngược hoặc tìm va chạm của mã băm đó. Do đó, tấn công vào hệ thống thông thường có thể mất khoảng một năm với một máy tính hiện nay. Điều này cho thấy khi tạo block có giá trị mã băm đủ mạnh sẽ đảm bảo cho BTC được an toàn [14].

Khi có 2 nút cùng có lời giải thành công cho bài toán tìm ra được giá trị mã băm cùng một thời điểm và truyền các block kết quả lên hệ thống Blockchain, lúc này, cả 2 block được gửi lên hệ thống và tại mỗi nút của hệ thống sẽ xây dựng các block kế tiếp trên block nhận được trước đó. Tuy nhiên, trên hệ thống Blockchain luôn yêu cầu mỗi nút phải xây dựng trên Blockchain dài nhất khi nút nhận được từ hệ thống. Điều này cho thấy khó có thể xảy ra các trường hợp như vậy trong hệ thống Blockchain.

Với các ưu điểm về mặt bảo mật của các giải pháp SHA-256, chữ ký số ECDSA-384, mã hóa đồng cấu đầy đủ cho thấy, BTC khi được tích hợp sẽ có những ưu điểm đảm bảo an toàn hơn so với các đồng tiền ảo khác. Trong nghiên cứu này, các tác giả sử dụng giải pháp bảo mật cho BTC trên hệ thống Blockchain. BTC của các tác giả đã được tích hợp các giải pháp bảo mật (SHA-256, chữ ký số ECDSA-384, mã hóa đồng cấu đầy đủ) để đảm bảo an toàn cho block. Các kết quả đạt được trong bài báo này được các tác giả bàn luận chi tiết trong phần "kết quả và bàn luận".

Kết quả và bàn luận

Tích hợp SHA vào thuật toán đồng thuận (PoW) cho BTC

Hiện nay, có nhiều loại giao thức đồng thuận, lựa chọn giao thức đồng thuận nào cho ứng dụng sẽ tùy thuộc vào yêu cầu của ứng dụng muốn xây dựng. Trong bài báo này, các tác giả đưa ra việc xây dựng các block đến một Blockchain hoàn chỉnh và sau đó sử dụng thuật toán đồng thuận để thể hiện tính bảo mật.

Quá trình tạo block, code block để chứa dữ liệu và mã băm của block là giá trị quan trọng nhất (hình S1 phụ lục). Trong mỗi block, mã băm được tính cho toàn bộ các block, ở đây các tác giả sử dụng thuật toán SHA (độ dài 256 bit) để tính giá trị mã băm đủ mạnh và đảm bảo an toàn cho block. Thuật toán mã băm được sử dụng lấy ở Thư viện mật mã CryptoJS [26], với cú pháp lệnh như sau:

<script src="https://cdnjs.cloudflare.com/ajax/libs/crypto-js/3.1.9-1/core.min.js"></script>.

<script src="https://cdnjs.cloudflare.com/ajax/libs/crypto-js/3.1.9-1/sha256.min.js"></script>.

Sau bước này là quá trình tạo class Blockchain để chứa mảng các block (hình S2 phụ lục), class này chứa TaoMoiBlock() và KiemTraTinhToanVen(). Trong đó, TaoMoiBlock() thực hiện tính toàn bộ giá trị mã băm cho block hiện tại, sau đó lưu lại và nối với nhau bằng mã băm. Điều này được thực hiện bằng cách lấy mã băm của block cuối cùng lưu vào block hiện tại (theo biến HashTruocDo); KiemTraTinhToanVen() có tính chất tốt để sử dụng kiểm tra toàn bộ các Blockchain đang giao dịch có đảm bảo an toàn hay không. Việc kiểm tra được thực hiện bằng cách lấy toàn bộ các mã băm có trong Blockchain và so sánh các giá trị mã băm này. Quá trình so sánh các giá trị mã băm này phải đảm bảo hai tính chất (toàn vẹn và liên kết) của từng block là không bị sai mã băm. Trong trường hợp có sai lệch, nghĩa là dữ liệu đã bị chỉnh sửa trong hệ thống.

Trong class Blockchain, các tác giả dùng thuật toán đồng thuận PoW để sửa đổi file class block (hình S3 phụ lục). Chỉnh sửa này được thực hiện bằng cách tính lại toàn bộ giá trị mã băm cho khớp, quá trình đồng bộ chỉ cần vài động tác và dữ liệu được đảm bảo tính toàn vẹn ở tất cả các nút trong mạng ngang hàng. Hơn nữa, có giải pháp tốt hơn để ngăn chặn đối tượng tấn công là: thực hiện

giới hạn thời gian tính giá trị mã băm cho một Blockchain và tăng độ khó đối với thuật toán mã băm (tăng độ dài từ 128 lên thành 256 bit). Điều này làm cho đối tượng tấn công mất rất nhiều thời gian mới tìm ra mã băm của Blockchain và cũng đồng nghĩa phải sau một thời gian nhất định mới thêm được một block mới.

Trong class block, các tác giả đã thêm một biến "GiaTriTuTang" để tính mã băm với mục tiêu tăng độ khó khi mã băm bằng SHA-256 bit. Bởi vì, hàm TinhToanHash() không đổi được thiết kế trong "class block", nên để tạo ra hàm băm đơn giản trong block mà vẫn đảm bảo được độ khó (phụ thuộc vào biến this.DoKho), các tác giả đã thêm các yêu cầu đối với hàm băm (như mã băm phải bắt đầu bằng 2 hoặc 3… các số "0" liên tiếp ở đầu) mới cho phép chấp nhận hay không giá trị mã băm khi thỏa mãn yêu cầu. Hàm DaoBlock() được tạo để thực hiện lặp đi lặp lại việc "đào" mã băm cho block hiện tại, bởi vì nếu chỉ sử dụng SHA-256 (cố định giá trị input/output đối với một Blockchain) thì rất dễ bị "đào" được giá trị mã băm. Sau đó, hàm newBlock.DaoBlock(this.DoKho) giúp để thực hiện tạo mới block sẽ cần phải "đào" mới có được mã băm cho nó. Như vậy, các tác giả đã sửa lại class Blockchain cho BTC của mình bằng cách đưa vào thuật toán đồng thuận PoW với giải pháp bảo mật SHA-256 bit để tăng độ khó cho quá trình đào BTC với đối tượng tấn công (hình S4 phụ lục).

Trong giao dịch với BTC, thông thường các giao dịch không đảm bảo ẩn danh cho cá nhân, vì giao dịch có thể sử dụng địa chỉ ảo và được xác thực công khai. Do đó, bất kỳ người giao dịch nào cũng có thể liên quan tới giao dịch khác của cá nhân. Hơn nữa, khi địa chỉ giao dịch của cá nhân được liên kết với danh tính thực của cá nhân sẽ gây ra rò rỉ làm mất tất cả thông tin các giao dịch của cá nhân đó. Đây chính là những điểm làm lộ lọt thông tin cá nhân khi đang thực hiện giao dịch. Do đó, các dịch vụ trộn trong nghiên cứu này được các tác giả thiết kế trong BTC của mình để ngăn địa chỉ giao dịch của người dùng được liên kết. Kỹ thuật trộn, theo nghĩa đen đó là một sự trao đổi ngẫu nhiên tiền của người dùng với tiền của người dùng khác, do đó đối với người quan sát, quyền sở hữu tiền của họ là khó hiểu.

Hình 4. Kết quả các mã băm sau khi được đào cho BTC của nghiên cứu này.

Khi thực hiện chạy thực tế, BTC của nghiên cứu này hoạt động trên hệ thống Blockchain trong cộng đồng cho thấy các giá trị mã băm SHA-256 bit của đồng tiền ảo đã khác nhau hẳn tại các thời điểm khác nhau. Để minh chứng cho điều này, các tác giả đã thực hiện lưu lại các giá trị mã băm trong file console.log(). Hình 4 cho kết quả chi tiết khi cần kiểm tra được lưu trong file console.log() ở tab Console. Từ kết quả đạt được, các tác giả đã thiết kế 2 trong số các dịch vụ trộn kết hợp như vậy và phân tích các thuộc tính bảo mật cũng như quyền riêng tư của nó. Tuy nhiên, việc trộn không hoàn toàn đáp ứng được khả năng bảo vệ cho BTC trước các hành động tấn công như trộm cắp tiền xu. Để tăng khả năng bảo mật cho BTC, các tác giả đã sử dụng thuật toán chữ ký số ECDSA nhằm đảm bảo tính ẩn danh cho đồng tiền này.

Tích hợp chữ kỹ số ECDSA-384 làm chữ ký ẩn danh cho BTC

BTC của nghiên cứu này đã được tích hợp thuật toán chữ ký số ECDSA-384 (với độ dài 384 bit) để đánh dấu giao dịch. Mô hình chữ ký ẩn danh được sử dụng là chữ ký số ECDSA-384 đảm bảo tính riêng tư và quyền sở hữu cho đồng BTC. Một đồng tiền điện tử BTC được coi là một chuỗi các chữ ký số. Mỗi chủ sở hữu chuyển tiền tới chủ sở hữu tiếp theo bằng cách ký một mã băm của giao dịch trước và khóa công khai của chủ sở hữu sau rồi bổ sung vào cuối đồng tiền. Người thụ hưởng có thể kiểm nhận các chữ ký để xác thực chuỗi quyền sở hữu.

Chữ ký số ECDSA-384 bit được các tác giả tích hợp vào BTC để đảm bảo quyền riêng tư của đồng tiền ảo được lấy từ Thư viện mật mã CryptoJS [26]. Đầu tiên, các tác giả tạo một class để chứa giao dịch, ở đây sử dụng thuật toán đồng thuận PoW trước đó đã được tích hợp trong "class blockchain" để tạo ra một dữ liệu chứa giao dịch với đồng BTC. Lớp giao dịch (class GiaoDich) được tạo mới hoàn chỉnh chứa thông tin như địa chỉ gửi, địa chỉ nhận và giá trị. Trong "class GiaoDich", với phần định nghĩa của Blockchain đã tạo thêm 2 biến mới: "this.GiaoDichTamHoan=[]" và "this.TienThuong=100". Trong đó, "this.GiaoDichTamHoan" là mảng chứa các giao dịch chưa có mã băm; biến "this.TienThuong" được thêm để lưu giá trị mã băm tương ứng với khoản tiền thưởng có được của người đào BTC. Nghĩa là BTC của các tác giả tạo ra đã có tính khan hiếm giống với vàng, bạc hiện nay. Tạo hàm "DaoTienAo()" và hàm này sử dụng hàm "DaoBlock()" để giá trị mã băm đào được dễ dàng được thêm vào cho BTC, cải thiện được tình huống khi một block đào được không dễ thêm được vào Blockchain (hình S5 phụ lục). Với cách xây dựng như thế giúp cho người đào có thể đẩy giá trị mã băm đào từ các giao dịch đang hoãn vào Blockchain và để lần đào tiếp theo sẽ lấy được giá trị tiền thưởng tương ứng từ mã băm đào được. Việc làm này có hai tác dụng lớn là: tránh "ăn non" và khuyến khích đào BTC. Trong BTC của các tác giả là hoàn toàn có thể lấy được giá trị tiền thưởng ngay sau khi đào được. Điều này được thực hiện trong "this.GiaoDichTamHoan". Sau mỗi một lần đào được mã băm, giá trị của "this.GiaoDichTamHoan" sẽ được lưu vào chung một block và block này có thể chứa tới hàng trăm giao dịch (do lập trình viên ấn định khi viết code). Tiếp theo, sau "DaoTienAo()", xây dựng hàm TaoGiaoDich(GiaoDichMoi) cần có "GiaoDichMoi" và được đẩy vào hàm "this.GiaoDichTamHoan.push(GiaoDichMoi)".

```
KiemTraTienTrongVi(DiaChiVi) {
    let TienTrongVi = 0;

    for (const block of this.MangBlock) {

        for (const gd of block.DanhSachGiaoDich) {
            if (gd.DiaChiGui === DiaChiVi) {

                TienTrongVi -= gd.GiaTri;
            }

            if (gd.DiaChiNhan === DiaChiVi) {
                TienTrongVi += gd.GiaTri;
            }
        }
    }
    return TienTrongVi;
}
```

Hình 5. Kết quả thực hiện xây dựng mã nguồn hàm tính toán số tiền trong ví điện tử người dùng.

Cuối cùng, để đồng tiền ảo BTC của nghiên cứu này có thể hoạt động như các đồng tiền ảo khác, các tác giả đã tạo hàm tính số tiền trong ví điện tử của cá nhân (hình 5). Việc tính số tiền có trong ví điện tử của BTC được thực hiện bằng cách tính số tiền có được trong toàn bộ giao dịch bên trong Blockchain của một ví điện tử. Trong đó, ví điện tử cho BTC của các tác giả đã được tích hợp chữ ký số ECDSA-384 bit để bảo vệ cho ví điện tử. Thuật toán này được các tác giả gọi từ Thư viện mật mã CryptoJS [26] và có chỉnh sửa để đảm bảo phù hợp với các luật giao dịch điện tử hiện nay [25] giúp đảm bảo an toàn, trung thực. Điều này cho thấy, tính riêng tư của cá nhân cho BTC được đảm bảo minh bạch trong tất cả các giao dịch trực tuyến cho BTC.

Tích hợp mật mã mã hóa đồng cấu đầy đủ cho BTC dựa trên Blockchain

Để tăng tính đảm bảo an toàn cho BTC của riêng mình, các tác giả sử dụng giải pháp mã hóa BTC bằng thuật toán mã hóa đồng cấu đầy đủ. Mã hóa đồng cấu đầy đủ là hệ mật mã có độ bảo mật cao [27, 28] và các tác giả đã sử dụng hệ mật mã này từ mã nguồn (có chỉnh sửa) trong Thư viện mật mã CryptoJS [26]. Quá trình thực hiện mã hóa và giải mã bằng mã hóa đồng cấu đầy đủ và được thực hiện với thời gian ngắn [28]. Quá trình lưu trữ này gần như không làm thay đổi các thuộc tính của Blockchain. Tức là khi đã tích hợp thuật toán mã hóa đồng cấu đầy đủ cho BTC, việc thực hiện mã hóa và giải mã dữ liệu nhằm đảm bảo tính riêng tư cho BTC dựa trên Blockchain. Điều này giúp cải thiện hơn nhiều trong các giao dịch đối với các Blockchain công khai và cũng đã được các tác giả kiểm tra thông qua mã nguồn của đồng tiền Ethereum [16].

Khi các tác giả sử dụng giải pháp tích hợp mã hóa đồng cấu đầy đủ cho BTC dựa trên hệ thống Blockchain, BTC của nhóm nghiên cứu đã tăng được độ bảo mật và đảm bảo tính bí mật cho BTC mà không ảnh hưởng tới hoạt động của đồng tiền này trong các giao dịch thực tế. BTC của các tác giả đã được tích hợp các giải pháp bảo mật như mật mã mã hóa đồng cấu đầy đủ, chữ ký số ECDSA-384, SHA-256. Chính điều này đã giúp cho BTC của các tác giả đảm bảo được tính bí mật và quyền riêng tư cho nó. So với các đồng tiền ảo khác như Ethereum, BTC của chúng tôi với các giải pháp bảo mật đưa ra bước đầu còn khá đơn giản, cần cải thiện thêm các kỹ thuật để có thể ứng dụng được trong thực tế.

Kết luận

Trong nghiên cứu này, các tác giả đã phân tích quyền riêng tư dựa trên Blockchain, các kỹ thuật đảm bảo và một số giải pháp để đảm bảo quyền riêng tư cũng như tính bảo mật của nền tảng công nghệ này. Áp dụng các giải pháp mật mã (như SHA, chữ ký số ECDSA, mã hóa đồng cấu đầy đủ) để tạo ra BTC dựa trên Blockchain. Kết quả đạt được bước đầu là đã xây dựng được giải pháp mật mã cho BTC. Cụ thể, các tác giả đã tích hợp mã nguồn mật mã với các giải pháp bảo mật như mã hóa đồng cấu đầy đủ, chữ ký số ECDSA-384, SHA-256. Tuy nhiên, các giải pháp bảo mật được tích hợp cho BTC của các tác giả đưa ra còn khá đơn giản, cần cải thiện thêm các kỹ thuật để có thể ứng dụng được trong thực tế. Việc giải quyết những điểm tồn tại này cũng chính là hướng phát triển trong các nghiên cứu tương lai.

Phụ lục

index.js ×

```
/* CLASS MÔ TẢ CẤU TRÚC CỦA MỘT BLOCK */
class Block {

  constructor(NgayGioTao, DuLieu, HashTruocDo = '') {
    this.NgayGioTao = NgayGioTao;
    this.DuLieu = DuLieu;
    this.HashTruocDo = HashTruocDo;
    this.Hash = this.TinhToanHash();
  }
  TinhToanHash() {
    return CryptoJS.SHA256(this.HashTruocDo + this.NgayTao + JSON.stringify(this.DuLieu)).toString
    ();
```

Hình S1. Tạo một block.

```
class Blockchain {

    constructor() {
        this.MangBlock = [];
        this.MangBlock.push(new Block("29/11/20201", "Genesis Block", "0"));
    }

    PhanTuCuoiCung() {
        return this.MangBlock[this.MangBlock.length - 1];
    }

    TaoMoiBlock(newBlock) {
        newBlock.HashTruocDo = this.PhanTuCuoiCung().Hash;
        newBlock.Hash = newBlock.TinhToanHash();
        this.MangBlock.push(newBlock);
    }

    KiemTraTinhToanVen() {
        for (let i = 1; i < this.MangBlock.length; i++) {
            const BlockHienTai = this.MangBlock[i];
            const BlockTruocDo = this.MangBlock[i - 1];
            if (BlockHienTai.Hash !== BlockHienTai.TinhToanHash()) {
                return false;
            }
            if (BlockHienTai.HashTruocDo !== BlockTruocDo.Hash) {
                return false;
            }
        }
        return true;
    }
}
```

Hình S2. Tạo một Blockchain.

```
/* CLASS MÔ TẢ CẤU TRÚC CỦA MỘT BLOCK */

class Block {

    constructor(NgayGioTao, DuLieu, HashTruocDo = '') {
        this.NgayGioTao = NgayGioTao;
        this.DuLieu = DuLieu;
        this.HashTruocDo = HashTruocDo;
        this.Hash = this.TinhToanHash();
        this.GiaTriTuTang = 0;
    // Thêm vào giá trị tự tăng của Block
    }
    TinhToanHash() {
        return CryptoJS.SHA256(this.HashTruocDo + this.NgayTao + JSON.stringify(this.DuLieu))
        .toString();
}

DaoBlock(DoKho) {

        while (this.Hash.substring(0, DoKho) !== Array(DoKho + 1).join("0")) {
            this.GiaTriTuTang++;
            this.Hash = this.TinhToanHash();
        }
        console.log("Đã đào xong Block: " + this.Hash);
    }
}
```

Hình S3. Sử dụng thuật toán đồng thuận PoW để sửa đổi file class block.

```
class Blockchain {

    constructor() {
        this.MangBlock = [];
        this.MangBlock.push(new Block("29/11/20201", "Genesis Block", "0"));
        this.DoKho = 5;
        // Thêm độ khó cơ Blockchain
    }

    PhanTuCuoiCung() {
        return this.MangBlock[this.MangBlock.length - 1];
    }

    TaoMoiBlock(newBlock) {
        newBlock.HashTruocDo = this.PhanTuCuoiCung().Hash;
        newBlock.Hash = newBlock.TinhToanHash();
//Lúc này ta không tính toán Hash đơn thuần nữa mà phải "đào" thì mới có Hash cho Block mới.
        newBlock.DaoBlock(this.DoKho);
        this.MangBlock.push(newBlock);
    }
```

Hình S4. Sử thuật toán đồng thuận PoW để sửa đổi file class Blockchain.

```
DaoTienAo(DiaChiViNhanTienThuong) {
    let block = new Block(new Date(), this.GiaoDichTamHoan, this.PhanTuCuoiCung().Hash);

    block.DaoBlock(this.DoKho);
    this.MangBlock.push(block);


    this.GiaoDichTamHoan = [
        new GiaoDich(null, DiaChiViNhanTienThuong, this.TienThuong)
    ];

}
```

Hình S5. Hàm đào tiền ảo.

TÀI LIỆU THAM KHẢO

[1] D. Drescher (2017), *Blockchain Basics*, Apress Berkeley, CA, DOI: 10.1007/978-1-4842-2604-9.

[2] H. Sularno, E.S. Budiasih (2022), "Analisis keabsahan bitcoin sebagai mata uang virtual menurut perspektif hukum positif di indonesia", *Aliansi J. Manaj. dan Bisnis*, **17(1)**, pp.35-42.

[3] B. Hameed, et al. (2019), "A review of Blockchain based educational projects", *Int. J. Adv. Comput. Sci. Appl.*, **10(10)**, pp.491-499.

[4] D. Tapscott, A. Tapscott (2016), *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*, Portfolio, 348pp.

[5] A. Mselmi (2020), "Blockchain technology and systemic risk", *Int. J. Econ. Financ.*, **10(2)**, pp.53-60.

[6] M.B. Hoy (2017), "An introduction to the Blockchain and its implications for libraries and medicine", *Med. Ref. Serv. Qua.*, **36(3)**, pp.273-279.

[7] T.K. Mackey, G. Nayyar (2017), "A review of existing and emerging digital technologies to combat the global trade in fake medicines", *Expert Opin. Drug Saf.*, **16(5)**, pp.587-602.

[8] Q. Xia, et al. (2017), "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments", *Information*, **8(2)**, DOI: 10.3390/info8020044.

[9] S. Wang, J.P. Vergne (2017), "Buzz factor or innovation potential: What explains cryptocurrencies' returns?", *PLOS ONE*, **12(1)**, DOI: 10.1371/journal.pone.0169556.

[10] X. Yue, et al. (2016), "Healthcare data gateways: Found healthcare intelligence on Blockchain with novel privacy risk control", *J. Med. Syst.*, **40(10)**, DOI: 10.1007/s10916-016-0574-6.

[11] C. Cachin, et al. (2017), "Non-determinism in byzantine fault-tolerant replication", *Leibniz Int. Proc. Informatics*, **70**, DOI: 10.4230/LIPIcs.OPODIS.2016.24.

[12] I. Homoliak, et al. (2021), "The security reference architecture for Blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses", *IEEE Commun. Surv. Tutorials*, **23(1)**, pp.341-390.

[13] I. Homoliak, et al. (2019), "A security reference architecture for Blockchains", *2019 IEEE International Conference on Blockchain (Blockchain)*, DOI: 10.1109/Blockchain.2019.00060.

[14] R. Zhang, et al. (2019), "Security and privacy on Blockchain", *ACM Comput. Surv.*, **52(3)**, DOI: 10.1145/3316481.

[15] S. Singh, et al. (2021), "Blockchain security attacks, challenges, and solutions for the future distributed IoT network", *IEEE Access*, **9**, pp.13938-13959.

[16] https://www.intelligenthq.com/12-bitcoin-and-blockchain-thoughts-and-quotes-you-need-to-read/.

[17] https://helpex.vn/article/bao-mat-va-quyen-rieng-tu-cua-blockchain-60a5c9183c25e7505ac54f74.

[18] P. Freni, et al. (2022), "Tokenomics and Blockchain tokens: A design-oriented morphological framework", *Blockchain Res. Appl.*, **3(1)**, DOI: 10.1016/j.bcra.2022.100069.

[19] Z. Schreiber (2020), "k-Root-n: An efficient algorithm for avoiding short term double-spending alongside distributed ledger technologies such as Blockchain", *Information*, **11(2)**, DOI: 10.3390/info11020090.

[20] V.A. Thakor, et al. (2021), "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities", *IEEE Access*, **9**, pp.28177-28193.

[21] S.A. Theotokis, D. Spinellis (2004), "A survey of peer-to-peer content distribution technologies", *ACM Comput. Surv.*, **36(4)**, pp.335-371.

[22] R. Leonard (2010), *Von Neumann, Morgenstern, and The Creation of Game Theory*, Cambridge University Press, DOI: 10.1017/CBO9780511778278.

[23] R.S.A. Laboratories (2012), *PKCS #1 v2.2: RSA Cryptography Standard*, EMC Corporation Public-Key Cryptography Standards (PKCS), 63pp.

[24] H. Natarajan, et al. (2017), *Distributed Ledger Technology and Blockchain*, World Bank, DOI: 10.1596/29053.

[25] https://www.ledger.com/.

[26] https://cdnjs.cloudflare.com/ajax/libs/crypto-js/3.1.9-1/core.min.js.

[27] J. Chen, F. You (2020), "Application of homomorphic encryption in Blockchain data security", *Proceedings of the 2020 4th International Conference on Electronic Information Technology and Computer Engineering*, pp.205-209.

[28] V. Mattila, et al. (2022), "Homomorphic encryption in 5ire Blockchain", *Int. J. Soc. Sci. Manag. Rev.*, **5(2)**, DOI: 10.37602/IJSSMR.2022.5219.