BLOCKCHAIN - NỀN TẢNG TOÁN HỌC VÀ CÁC THUẬT TOÁN ĐỒNG THUẬN

Nguyễn Mậu Hân

Trường Đại học Khoa học, Đại học Huế

Email: nmhan@husc.edu.vn

Ngày nhận bài: 12/5/2021; ngày hoàn thành phản biện: 7/6/2021; ngày duyệt đăng: 02/11/2021

TÓM TẮT

Công nghệ blockchain không phải là một phát minh mới lạ mà là sự kết hợp giữa các lý thuyết và công nghệ đã tồn tại qua nhiều năm: lý thuyết mật mã, mạng ngang hàng và các thuật toán đồng thuận trong lý thuyết trò chơi. Vài năm gần đây, công nghệ blockchain 3.0 đã vượt khỏi biên giới của lĩnh vực tài chính – tiền tệ và thâm nhập đa dạng vào các các lĩnh vực khác nhau của đời sống xã hội. Bài báo này không trình bày một cách chi tiết về một ứng dụng nào đó trong thực tế của blockchain mà đưa ra một cách nhìn về nguồn gốc của công nghệ blockchain theo khía cạnh toán học và các thuật toán đồng thuận để hiểu hơn về bản chất của blockchain.

Từ khóa: blockchain, thuật toán đồng thuận, lý thuyết mật mã, sổ cái kế toán.

1. MỞ ĐẦU

Blockchain là một công nghệ cho phép truyền tải dữ liệu một cách an toàn dựa vào hệ thống mã hoá vô cùng phức tạp, tương tự như cuốn sổ cái kế toán của một công ty, nơi mà mọi hoạt động liên quan đến tiền bạc của công ty được giám sát một cách chặt chẽ. Blockchain được sử dụng trong việc lưu trữ thông tin trong các khối được liên kết với nhau và được mở rộng theo thời gian. Mỗi khối chứa thông tin về dữ liệu giao dịch, thời gian khởi tạo và thông tin về khối liên kết trước nó. Do các khối thông tin được quản lý bởi tất cả mọi người tham gia hệ thống nên blockchain được tạo ra để chống lại sự thay đổi dữ liệu trong hệ thống, không thể làm giả, không thể phá hủy sự liên kết giữa các khối thông tin. Khi được nhập vào trong chuỗi khối blockchain thì thông tin sẽ không thể thay đổi bởi một cá nhân nào đó và chỉ được bổ sung thêm thông tin khi có sự chấp thuận của tất cả mọi người trong hệ thống [7]. Điều này có nghĩa là nếu một phần của hệ thống blockchain bị sụp đổ thì những máy tính và nút khác sẽ tiếp tục hoạt động để bảo vệ thông tin.

Các loại công nghệ được sử dụng trong blockchain là:

Lý thuyết mật mã: Sử dụng public key trong chữ ký số và giá trị băm (hash function) để đảm bảo tính minh bạch, toàn vẹn và riêng tư.

Mạng ngang hàng: Một hệ thống mạng mà mỗi một nút trong mạng có vai trò như nhau, tự quản lý tài nguyên của mình. Một nút được xem như một client và cũng là server để lưu trữ bản sao dữ liệu [1].

Lý thuyết trò chơi: Tất cả các nút tham gia vào hệ thống đều phải tuân thủ luật chơi đồng thuận (PoW, PoS) và được thúc đẩy bởi động lực xác định trước [7].

Công nghệ blockchain đóng vai trò giống như một cuốn sổ cái ghi lại tất cả các giao dịch xảy ra trong hệ thống và có các đặc điểm chính có thể kể đến như:

Không thể làm giả: Các chuỗi blockchain gần như không thể bị phá hủy. Theo lý thuyết thì chỉ có máy tính lượng tử mới có thể can thiệp vào và giải mã chuỗi blockchain và nó chỉ bị phá hủy hoàn toàn khi Internet trên toàn cầu biến mất [6].

Tính bất biến: Dữ liệu trong blockchain gần như không thể sửa đổi được (chỉ có thể sửa đổi được bởi chính người đã tạo ra nó, nhưng phải được sự đồng thuận của các nút trên mạng) và các dữ liệu đó sẽ lưu giữ mãi mãi.

Bảo mật dữ liệu: Các thông tin, dữ liệu trong các blockchain được phân tán và độ an toàn cao, chỉ có người nắm giữ private key mới có quyền truy xuất dữ liệu đó [2].

Tính minh bạch: Có thể theo dõi được đường đi của dữ liệu trong blockchain từ địa chỉ này tới địa chỉ khác và có thể thống kê toàn bộ lịch sử trên địa chỉ đó.

Hợp đồng thông minh: Blockchain không cần bên thứ ba tham gia vào hệ thống, và nó bảo đảm rằng tất cả các bên tham gia đều biết được chi tiết hợp đồng và các điều khoản sẽ được tự động thực hiện một khi các điều kiện được bảo đảm [6].

2. PHƯƠNG PHÁP NGHIÊN CỨU

Trên cơ sở nền tảng toán học của các khối kiến thức như lý thuyết mật mã, mạng ngang hàng và lý thuyết trò chơi, phương pháp nghiên cứu được sử dụng trong bài báo là khai thác các nguồn tài liệu khác nhau về nền tảng lý thuyết và thuật toán được sử dụng trong công nghệ blockchain nhằm làm rỏ bản chất và cấu trúc chi tiết của công nghệ blockchain.

3. NỀN TẢNG TOÁN HỌC CỦA BLOCKCHAIN

Lý thuyết mật mã là khoa hoc nghiên cứu về cách viết bí mật, trong đó bản rõ được biến đổi thành bản mã, quá trình biến đổi đó được gọi là sự mã hóa. Quá trình

ngược lại biến đổi bản mã thành bản rõ được gọi là sự giải mã. Công nghệ blockchain được phát triển dựa trên hai nền tảng có nguồn gốc từ lý thuyết mật mã, đó là hàm băm và chữ ký số.

3.1 Hàm băm

Hàm băm là hàm toán học dùng để chuyển đổi một văn bản có độ dài bất kì thành một chuỗi bit có độ dài cố định. Bất kỳ nỗ lực gian lận nào để thay đổi phần nào của blockchain sẽ bị phát hiện vì giá trị băm mới sẽ không phù hợp với thông tin cũ trên blockchain. Bằng cách này, ngành khoa học mật mã (cần thiết cho việc mã hóa thông tin và mua sắm trực tuyến, ngân hàng) đã trở thành một công cụ hiệu quả để giao dịch mở.

3.1.1 Khái niệm hàm băm

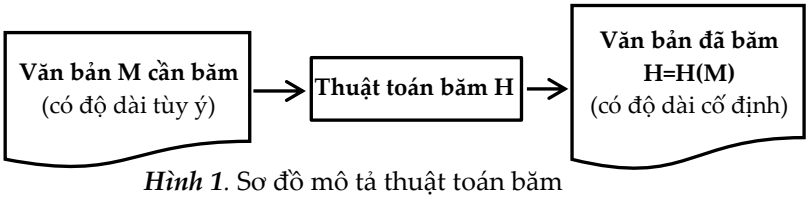
Hàm băm được định nghĩa bằng công thức: h = H(M), với M là văn bản cần băm, H là hàm băm và h là giá trị băm. Hàm băm H không có chức năng mã hóa vì khi giải mã không về được văn bản ban đầu. Giá trị băm h là một xâu bit còn được gọi là "đại diện thông điệp". Hàm băm H là hàm một chiều, theo nghĩa giá trị của hàm băm là duy nhất, và từ giá trị băm này "khó" có thể suy ngược lại được nội dung hay độ dài ban đầu của dữ liệu gốc.

Các hàm băm dòng MD: MD2, MD4, MD5 được Rivest đưa ra có kết quả đầu ra với độ dài là 128 bit. Hàm băm MD4 đưa ra vào năm 1990. Một năm sau, phiên bản mạnh MD5 cũng được đưa ra. Năm 1993, hàm băm SHA phức tạp hơn nhiều, kết quả đầu ra có độ dài 160 bit, cũng được xây dựng dựa trên các phương pháp tương tự.

3.1.2 Đặc tính của hàm băm

Hàm băm h là hàm một chiều với các đặc tính sau:

- Với văn bản đầu vào M thì chúng ta chỉ thu được giá trị băm duy nhất h=H(M).
- Nếu dữ liệu trong văn bản M bị thay đổi hay bị xóa để thành bản tin M', thì giá trị băm H(M') ≠ H(M) cho dù chỉ là một sự thay đổi nhỏ. Ví dụ chỉ cần thay đổi 1 bit dữ liệu của văn bản gốc M, thì giá trị băm H(M) của nó cũng thay đổi theo. Điều này có nghĩa là hai thông điệp khác nhau, thì giá trị băm của chúng sẽ khác nhau.



Hình 1. Sơ đồ mô tả thuật toán băm

- Nội dung của bản tin gốc "khó" có thể suy ra từ giá trị hàm băm của nó. Nghĩa là: Với thông điệp M thì "dễ" xác định được h=H(M), nhưng lại "khó" xác định ngược lại được M nếu chỉ biết giá trị băm h=H(M) (kể cả khi biết hàm băm H).

3.2 Chữ ký số

3.2.1 Giới thiệu về chữ kí số

Chữ ký nói chung là bằng chứng thể hiện người ký có chủ định khi ký vào một văn bản, làm cho người nhận văn bản biết rằng ai là người đã ký văn bản đó. Về mặt nguyên tắc chữ ký không thể sử dụng lại được, không thể sao chép sang văn bản khác, văn bản đã ký không thể thay đổi, không thể giả mạo và cũng không thể chối bỏ khi đã ký. Chữ ký có nhiều ưu điểm như dễ kiểm tra, không sao chép được, chữ ký của một người là giống nhau trên nhiều tài liệu, nhưng chỉ có giá trị trên một tài liệu cụ thể.

Chữ ký số cũng có các tính chất của chữ ký, được tạo ra bằng cách biến đổi dữ liệu sử dụng hệ mã hóa khóa công khai, người có dữ liệu ban đầu và khóa công khai của người ký thì có thể xác thực được chữ ký số vừa ký. Theo đó, mỗi người dùng sẽ sở hữu một cặp khóa gồm *khóa bí mật* và *khóa công khai*. Khóa bí mật được lưu trữ bí mật và sử dụng để ký kết các giao dịch. Các giao dịch đã ký dùng chữ ký số được phát đi trên toàn bộ mạng. Bản chất của chữ ký số là một chuỗi số gắn kết với một văn bản với một (hoặc nhiều) thực thể nguồn nào đó. Nếu văn bản thay đổi thì chữ ký số phải thay đổi theo, do đó chữ ký số đảm bảo tính toàn vẹn của văn bản được ký. Chữ ký số không thể sử dụng lại và cũng không làm giả được. Chữ ký số đảm bảo tính xác thực vì chỉ có người ký mới xác thực được chữ ký. Chữ ký số cũng xác thực đảm bảo tính không thể chối bỏ của chữ ký. Người ký không thể chối bỏ rằng không ký vào tài liệu. Chữ ký số liên quan đến hai giai đoạn: Giai đoạn tạo chữ ký số và giai đoạn xác minh.

3.2.2 Cấu tạo của chữ ký số

Sơ đồ chữ ký số là một bộ năm thành phần gồm (P, A, K, S, V), Trong đó:

- P là tập hợp hữu hạn các văn bản.
- A là tập hợp hữu hạn các chữ ký có thể được sử dụng.
- Không gian khóa K là tập hợp hữu hạn các khóa có thể sử dụng. Trong đó không gian khóa K' để tạo nên chữ ký, không gian khóa K'' kiểm tra chữ ký. Thuật toán tạo nên khóa: $K \rightarrow K' \times K''$ (K': không gian khóa bí mật, K'': không gian khóa công khai)
- S là tập các thuật toán tạo chữ ký $sig_{K'} \in S$, $sig_{K'}: P \rightarrow A$
- V là tập các thuật toán kiểm tra chữ ký $ver_{K''} \in V$, $ver_{K''}: P \times A \rightarrow \{đúng, sai\}$, thỏa mãn điều kiện sau đây đối với bất kỳ bản tin $x \in P$ và chữ ký $y \in A$.

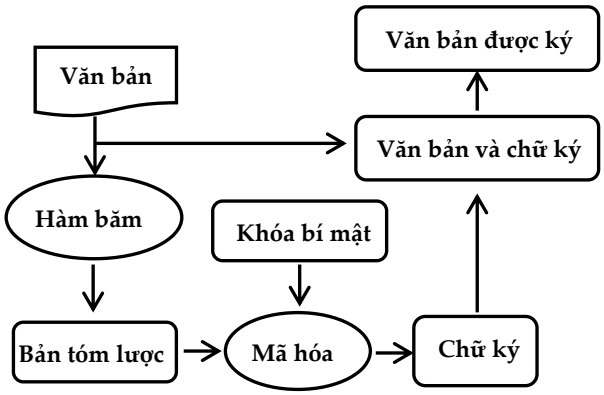
$$\forall x \in P, \forall y \in A: \quad ver_{K''}(x, y) = \begin{cases} Đúng, nếu\ y = sig_{K'}(x) \\ Sai, nếu\ y \neq\ sig_{K'}(x) \end{cases}$$

Bởi vì văn bản cần ký thường có chiều dài khá dài. Một biện pháp để ký là chia văn bản ra các đoạn nhỏ và sau đó ký lên từng đoạn và ghép lại.

3.2.3 Các giai đoạn tạo và kiểm tra chữ ký số

a. Giai đoạn tạo chữ ký số

Dùng thuật toán băm cho văn bản cần truyền đi, kết quả được một bản tóm lược, sử dụng khóa bí mật của điểm gửi để mã hóa bản tóm lược. Bản tóm lược đảm bảo 2 tính chất sau:



Hình 2. Giai đoạn tạo chữ ký số

(1) Tính duy nhất: mỗi bản khác nhau thì sẽ có một bit khác nhau, không trùng lặp và có độ dài không đổi;

(2) Tính một chiều: Từ bản tóm lược này không suy ngược lại được nội dung văn bản. Bản tóm lược này được mã hóa bằng khóa bí mật của điểm gửi và được kết hợp với văn bản, rồi gửi đến điểm nhận và bản tóm lược được mã hóa này chính là chữ ký số.

b. Giai đoạn xác minh chữ ký số

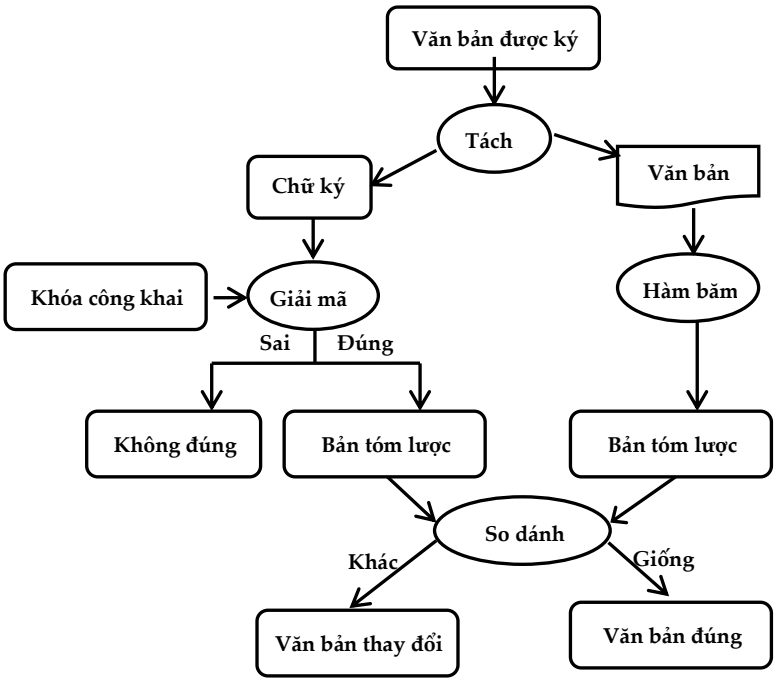
Điểm nhận sau khi nhận văn bản được ký số, quá trình tiến hành kiểm tra được thực hiện như sau:

Bước 1: Tiến hành tách văn bản và chữ ký số.

Bước 2: Lấy đoạn văn bản, đưa qua hàm băm thu được kết quả băm là bản tóm lược.

Bước 3: Giải mã chữ ký số (bản tóm lược được mã hóa bằng khóa bí mật), sử dụng khóa công khai của điểm gửi để giải mã nhận được bản tóm lược.

Bước 4: Tiến hành so sánh bản tóm lược vừa giải mã với bản tóm lược nhận được trong bước 2, nếu 2 bản này giống nhau và khóa công khai chắc chắn là do điểm gửi gửi thì kết luận: (1) văn bản nhận được là chính xác;



Hình 3*. Giai đoạn kiểm tra chữ ký số*

(2) văn bản nhận được là do chính điểm gửi gửi đi vì chỉ duy nhất điểm nhận được xác thực mới có khóa bí mật phù hợp với khóa công khai đã sử dụng để giải mã. Trường hợp 2 bản tóm lược khác nhau thì kết luận văn bản bị sửa đổi.

Chữ ký số được tạo ra bằng sự biến đổi một văn bản sử dụng hệ mã hóa khóa công khai, theo đó điểm nhận có văn bản ban đầu và khóa công khai của điểm gửi có thể xác định được.

3.2.4 Vai trò của chữ ký số trong blockchain

Hiện nay đồng tiền điện tử này có thể được sử dụng để trao đổi các sản phẩm và dịch vụ, giống như đồng đô la Mỹ (USD), Euro (EUR), đồng nhân dân tệ Trung Quốc (CNY) và các loại tiền tệ của các quốc gia khác. Do vậy chúng ta sẽ tạm lấy đồng tiền này làm đại diện để nói về nguyên lý hoạt động và vai trò của chữ ký số trong công nghệ blockchain.

Cũng giống như đô la Mỹ bản thân nó không mang giá trị, nó chỉ có giá trị bởi vì có một cộng đồng đồng ý sử dụng nó làm đơn vị giao dịch hàng hóa và dịch vụ. Để theo dõi số lượng bitcoin mà mỗi người sở hữu trong các tài khoản nhất định và theo dõi các giao dịch phát sinh từ đó thì chúng ta cần đến một cuốn sổ kế toán, trong trường hợp này nó chính là blockchain và đây thực tế là một tệp kỹ thuật số theo dõi tất cả các giao dịch bitcoin. Tệp sổ cái này không được lưu trữ trong một máy chủ trung tâm, như trong một ngân hàng hoặc trong một trung tâm dữ liệu mà ngược lại nó được phân phối trên toàn thế giới thông qua một mạng lưới các máy tính ngang hàng với vai trò lưu trữ dữ liệu và thực thi các tính toán. Mỗi máy tính này đại diện cho một "nút" của mạng lưới blockchain và mỗi nút đều có một bản sao của tệp sổ cái này.

Nếu A muốn gửi bitcoin cho B 5 bitcoin thì A sẽ phát một thông báo tới mạng lưới và cho biết số lượng bitcoin trong tài khoản của mình sẽ giảm 5 và số lượng bitcoin trong tài khoản của B sẽ tăng lên tương ứng. Mỗi nút trong mạng sau đó sẽ nhận được thông báo này và ánh xạ giao dịch được yêu cầu vào bản sao sổ cái kế toán của họ, và theo đó số dư tài khoản của cả hai bên đều được cập nhật.

Để có thể thực hiện các giao dịch trên blockchain, bạn cần một ví tiền điện tử, thực chất đây là một phần mềm sẽ cho phép lưu trữ và trao đổi các đồng bitcoin của bạn. Vì chỉ có bạn mới có thể chi tiêu các đồng bitcoin của mình do vậy mỗi chiếc ví tiền điện tử này được bảo vệ bằng một phương pháp mã hóa đặc biệt sử dụng một cặp khóa bảo mật duy nhất: khóa riêng tư (private key) và khóa công khai (public key).

Nếu một thông điệp được mã hóa bằng một khóa công khai cụ thể thì chỉ chủ sở hữu của khóa riêng tư là một cặp với khóa công khai này mới có thể giải mã và đọc nội dung thông điệp. Khi A muốn gửi bitcoin, anh ta cần phát một thông điệp được mã hóa bằng khóa riêng của ví điện tử của mình, vì thế anh ta chỉ có thể dùng bitcoin mà

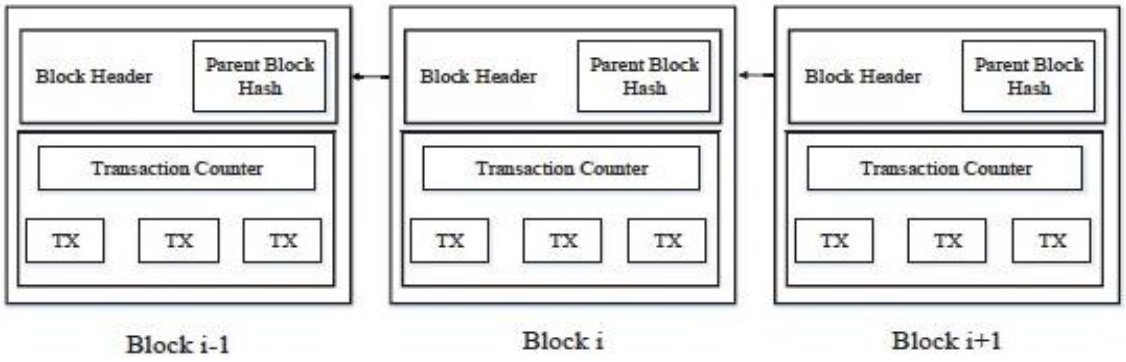
anh ta sở hữu vì A là người duy nhất biết khóa riêng tư của anh cần thiết để mở ví điện tử của mình. Mỗi nút trong mạng có thể kiểm tra chéo các yêu cầu giao dịch được gửi từ A là chính xác hay không bằng cách giải mã thông điệp yêu cầu giao dịch bằng khóa công khai của A.

Khi mã hóa một yêu cầu giao dịch bằng khóa riêng tư từ ví của bạn tức là bạn đang tạo ra một chữ ký số được các máy tính trong mạng lưới blockchain sử dụng để kiểm tra chủ thể gửi và tính xác thực của giao dịch. Chữ ký này là một chuỗi văn bản và nó là kết quả của việc kết hợp yêu cầu giao dịch và khóa riêng tư của bạn. Nếu bạn thay đổi một ký tự đơn trong thông điệp yêu cầu giao dịch này thì chữ ký điện tử sẽ thay đổi theo vì vậy không có kẻ tấn công tiềm tàng nào có thể thay đổi yêu cầu giao dịch của bạn hoặc thay đổi số lượng bitcoin mà bạn đang gửi.

4. CƠ CHẾ ĐỒNG THUẬN TRONG BLOCKCHAIN

4.1 Cấu trúc của blockchain

Blockchain có cấu trúc phi tập trung. Nghĩa là, cơ sở dữ liệu của nó không dựa vào các tổ chức thứ ba để quản lý và xác thực, không có kiểm soát trung tâm, tất cả các nút nhận được thông tin tự kiểm tra, truyền tải, và quản lý, đặt sự tin tưởng vào các nút, cho phép các nút lưu trữ các giao dịch trong một khối. Các khối được ghép nối với nhau tạo nên một chuỗi khối (blockchain). Cấu trúc phi tập chung là đặc điểm nổi bật và quan trọng nhất của blockchain [5].

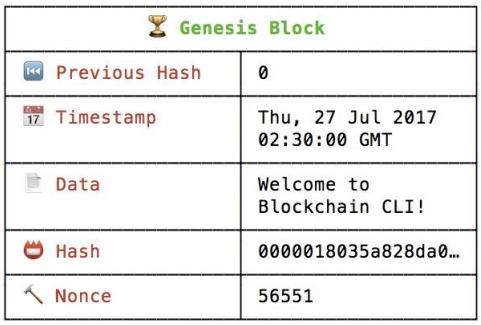


Hình 4. Cấu trúc dữ liêu của blockchain

Mỗi block trong blockchain bao gồm các thành phần sau:

- Index (Block#): Thứ tự của block (block gốc có thứ tự 0)
- Hash: Giá trị băm của block
- Previous Hash: Giá trị băm của block trước.
- Timestamp: Thời gian tạo của block;

- Data: Thông tin lưu trữ trong block;
- Nonce: Giá trị biến thiên để tìm ra giá trị băm thỏa mãn yêu cầu của mỗi blockchain;



Hình 5. Cấu trúc của block gốc

Giá trị băm (Hash) sẽ băm toàn bộ các thông tin cần thiết như timestamp, previous hash, index, data, nonce.

Khi có một block được thêm vào, block mới sẽ có giá trị "Previous Hash" là giá trị băm của block được thêm trước nó. Blockchain tìm kiếm block được thêm vào gần nhất để lấy giá trị index và previous hash. Block tiếp theo sẽ được tính như sau:

- Index: 0+1 = 1;
- Previous Hash: 0000018035a828da0… 9;
- Timestamp: thời gian block được tạo ra;
- Data: dữ liệu lưu trữ trong block;
- Hash: ??;
- Nonce: ??;

Ta cần tìm giá trị "nonce" phù hợp để có giá trị băm Hash thỏa mãn điều kiện của blockchain. Số lượng số 0 ở đầu được gọi là "difficulty".

Bằng cách lưu trữ dữ liệu trên tất cả các nút của mình, mạng blockchain loại bỏ các rủi ro đi kèm với dữ liệu được tổ chức lưu trữ tập trung. Trong mạng không có các điểm tập trung dễ bị tổn thương cho hệ thống, không có các điểm trung tâm làm cho hệ thống dừng hoạt động. Bất kỳ nút nào trong mạng khi dừng hoạt động sẽ không ảnh hưởng đến sự vận hành của hệ thống.

4.2 Nguyên lý tạo khối

Các giao dịch sau khi được gửi lên trên mạng lưới blockchain sẽ được nhóm vào các khối. Các giao dịch trong cùng một khối được coi là đã xảy ra cùng một lúc và các giao dịch chưa được thực hiện trong một khối được coi là chưa được xác nhận. Mỗi nút có thể nhóm các giao dịch với nhau thành một khối và gửi nó vào mạng lưới như một hàm ý cho các khối tiếp theo được gắn vào sau đó. Để được thêm vào blockchain, mỗi khối phải chứa một đoạn mã được tạo ra bằng hàm băm không thể đảo ngược.

Trong hệ thống phi tập trung (decentralized system), điểm mấu chốt là làm thế nào thống nhất được nội dung dữ liệu lưu trữ trên blockchain. Vì có rất nhiều nút trên hệ thống, không thể nào đảm bảo rằng tất cả các nút sẽ được cập nhật, lưu trữ dữ liệu

một cách chính xác. Cơ chế đồng thuận ra đời để đảm bảo điều này. Có thể hiểu cơ chế đồng thuận là "luật chơi" của hệ thống. Bất kỳ ai tham gia đều phải tuân theo và không thể cố tình chơi sai luật.

4.3 Thuật toán đồng thuận của Blockchain

Cơ chế đồng thuận trong blockchain có thể hiểu như cách thức mà mọi người quản lý trong hệ thống blockchain có thể đồng ý cho một giao dịch xảy ra trong hệ thống hoặc không. Dưới đây là một số cơ chế đồng thuận phổ biến trong blockchain:

- **Proof of Work (PoW)**: là cơ chế đồng thuận phổ biến nhất, được dùng trong bitcoin, Ethereum, Litecoin, Dogecoin và hầu hết các loại tiền mã hoá. Đây là cơ chế đồng thuận tiêu tốn khá nhiều điện năng. PoW là sự ghi nhận công sức bỏ ra để hoàn thành công việc. Nút nào hoàn thành công việc trước thì được quyền thêm block mới vào blockchain. Công việc ở đây là tìm một giá trị nonce bất kỳ thoả mãn điều kiện nào đó.

  Ví dụ: hash(nonce) < 0000000000000000000285a375f9d33e17…

Ở đây, hash là một hàm băm, nonce là một giá trị ngẫu nhiên được tìm ra sao cho hash(nonce) nhỏ hơn một ngưỡng nào đó.

Giá trị 0000000000000000000285a375f9d33e17… là ví dụ cho một ngưỡng nào đó.

Quá trình tìm ra giá trị nonce là một quá trình thử sai. Các nút thường sẽ bắt đầu với nonce = 0, 1, …, đến khi nào giá trị hash của nonce thoả mãn điều kiện ngưỡng.

Khi một block mới được tìm thấy, block đó sẽ được công bố trên toàn mạng để các nút khác kiểm tra. Nếu mọi tính toán, giao dịch trong block đó chính xác, các nút sẽ cập nhật vào blockchain đang lưu trữ cục bộ tại nút đó.

- **Proof of Stake (PoS)**: cơ chế đồng thuận này là một giải pháp thay thế cho PoW trong vấn đề tiết kiệm năng lượng bởi vì nó tiêu hao ít năng lượng hơn và cũng khó bị tấn công hơn. PoS phổ biến trong Decred, Peercoin và nhiều loại tiền mã hoá khác. Nhiều blockchains theo cơ chế đồng thuận PoW ngay từ đầu và đang muốn chuyển đổi dần sang PoS [10]. Ví dụ, ethereum đang có kế hoạch chuyển từ Ethash (một loại của PoW) [27] cho Casper (một loại PoS) [28].
- **Delegated Proof-of-Stake (DPoS)**: đây là cơ chế đồng thuận phổ biến trong Steemit, EOS, BitShares. Cơ chế đồng thuận này có chi phí giao dịch rẻ; có khả năng mở rộng; hiệu suất năng lượng cao. Tuy nhiên vẫn còn mang tính chất tập trung vì thuật toán này lựa chọn người đáng tin cậy để uỷ quyền với mục đích tránh rủi ro.

- **Proof of Authority (PoA)**: Đây là cơ chế đồng thuận phổ biến thường thấy trong POA.Network, Ethereum Kovan Testnet. Cơ chế đồng thuận này có hiệu suất cao, có khả năng mở rộng tốt.
- **Proof-of-Weight (PoW)**: Phổ biến trong Algorand, Filecoin. Có thể tuỳ chỉnh và khả năng mở rộng tốt. Tuy nhiên quá trình thúc đẩy việc phát triển sẽ là một thử thách lớn.
- **Ripple** [6] là một thuật toán đồng thuận sử dụng mạng con trong một mạng lớn hơn. Trong mạng, các nút được chia thành hai loại: máy chủ cho tham gia quá trình đồng thuận và máy của khách hàng chỉ tham gia trong vấn đề giao dịch tiền bạc. Mỗi máy chủ quản lý một danh sách nút duy nhất (Unique Node List-UNL). Khi cần xác định có nên đặt một giao dịch vào sổ cái hay không thì máy chủ sẽ truy vấn các nút trong UNL và nếu các thỏa thuận nhận được đạt tới 80% thì giao dịch sẽ được thực hiện và đóng gói vào sổ cái.

Tùy theo đặc trưng của Blockchain người thiết kế sẽ sử dụng thuật toán đồng thuận thích hợp. Nhờ sự mã hóa, hàm băm và cơ chế đồng thuận mà Blockchain không thể bị tấn công, sửa đổi nội dung bởi các hacker hoặc người sử dụng.

3. KẾT LUẬN

Blockchain đã cho thấy tiềm năng của nó để chuyển đổi một số hoạt động trong ngành công nghiệp truyền thống với các đặc điểm chính của nó: phi tập trung, không thể làm giả, bất biến, bảo mật dữ liệu, minh bạch và hợp đồng thông minh. Trong bài báo này, để có một cái nhìn về bản chất của blockchain chúng tôi không đi sâu về một ứng dụng blockchain trong các ngành công nghiệp cụ thể nào mà chỉ khảo sát và phân tích nền tảng toán học và các thuật toán chuyên sâu được sử dụng để tạo nên công nghệ này.

TÀI LIỆU THAM KHẢO

[1]. Nguyễn Mậu Hân (2012), *Cơ sở dữ liệu phân tán*, NXB Đại Học Huế.

[2]. Phan Đình Diệu (2002). Lý thuyết mật mã và an toàn thông tin, NXB ĐHQG Hà Nội.

[3]. Amos K. Kibet, Demeke G. Bayyou, Rosanna Esquive (2019), *Blockchain: It's structure, principles, applications and foreseen issues*, JETIR.

[4]. Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone (2019), *Blockchain Technology Overview, NIST Internal Report.*

[5]. Gates M. (2017). *Blockchain: Ultimate guide to understanding blockchain, cryptocurrencies, smart contracts and the future of money*. Wise Fox Publishings and Mark Gates.

[6]. D. Schwartz, N. Youngs, and A. Britto, "*The ripple protocol consensus algorithm*," Ripple Labs

Inc White Paper, vol. 5, 2014

[7]. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen Website, (2017), *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*

[8]. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "*Hawk: The blockchain model of cryptography and privacy-preserving smart contracts*," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.

[9]. Y. Zhang and J. Wen, "*An iot electric business model based on the protocol of bitcoin*," in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184–191.

[10]. M. Sharples and J. Domingue, "*The blockchain and kudos: A distributed system for educational record, reputation and reward*," in Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 2015, pp. 490–496.

[11]. C. Noyes, "*Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning*," arXiv preprint arXiv:1601.01405, 2016.

[12]. I. Eyal and E. G. Sirer, "*Majority is not enough: Bitcoin mining is vulnerable*," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436– 454.

[13]. "*State of blockchain q1 2016: Blockchain funding overtakes bitcoin*," 2016. http://www.coindesk.com/ state-of-blockchain-q1-2016/

[14]. S. Nakamoto, "*Bitcoin: A peer-to-peer electronic cash system*," 2008. https://bitcoin.org/bitcoin.pdf

[15]. G. W. Peters, E. Panayi, and A. Chapelle, "*Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective*," 2015, http://dx.doi.org/10.2139/ssrn. 2646618

[16]. [6] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013. [Online]. Available: https://ssrn.com/abstract=2394738.

BLOCKCHAIN - A MATHEMATICAL PLATFORM AND CONSENSUS ALGORITHMS

Nguyen Mau Han

University of Sciences, Hue University

Email: nmhan@hueuni.edu.vn

ABSTRACT

Blockchain technology is not only a new invention but also a combination of theories and technologies that have existed for many years: cryptographic theory, peer-to-peer networks and consensus algorithms in game theory. In recent years, Blockchain Technology 3.0 has transcended the boundaries of the financial - monetary field and diversified its penetration into various fields of social life. This article does not present a detailed description of a blockchain application, but gives a perspective on blockchain technology in terms of mathematical and consensus algorithms to better understand the nature of blockchain.

Keywords: blockchain, consensus algorithm, cryptography theory, ledger.

Nguyễn Mậu Hân sinh năm 1957 tại Thừa thiên Huế. Năm 1981, ông tốt nghiệp cử nhân toán tại Trường Đại học Tổng hợp Huế. Năm 1998, ông nhận bằng thạc sĩ Khoa học máy tính tại Trường Đại học Bách khoa Hà Nội. Năm 2003, ông nhận bằng tiến sĩ Khoa học Máy tính tại Viện Công nghệ Thông tin Hà Nội. Hiện ông là Phó Giáo sư, Giảng viên cao cấp tại Trường Đại học Khoa học, Đại học Huế.

Lĩnh vực nghiên cứu: Công nghệ phần mềm, Cơ sở dữ liệu, Xử lý song song và phân tán.