Tổng quan về Blockchain và các ứng dụng

NGUYỄN CƯỜNG

Không ít người dành nhiều thập kỷ để chờ đợi một ai đó sáng chế ra một loại tiền cho các giao dịch trực tuyến. Trang web 99bitcoins.com cho biết, có nhiều công ty tuyên bố chấp nhận Bitcoin là một loại tiền tệ, như: Subway, nhà sách thuộc Viện Công nghệ Massachusetts và Bảo tàng Coastal Bend tại Victoria, Texas. Bitcoin có thể đáp ứng mong đợi là công cụ cho giao dịch trực tuyến không? Bài viết trình bày những kiến thức cơ bản về bitcoint.

Từ khóa: *tiền điện tử, bitcoint, tiền số, kinh tế số.*

1. Giới thiệu

Bitcoin là ứng dụng đầu tiên của blockchain, đây là một loại tiền tệ số dựa trên công nghệ blockchain, sử dụng cho các hoạt động thương mại trên internet cũng như chúng ta sử dụng tiền trong thế giới thực. Tiếp nối thành công của Bitcoin, người ta có thể sử dụng công nghệ blockchain trong nhiều lĩnh vực và dịch vụ khác nhau, chẳng hạn như thị trường tài chính, IOT, chuỗi cung ứng, bầu cử, điều trị và lưu trữ thuốc. Khi công nghệ blockchain được sử dụng cho các công việc hoặc dịch vụ trong cuộc sống hàng ngày, tội phạm mạng cũng có cơ hội tham gia vào các hoạt động tội phạm trên mạng. Ví dụ, các hacker thường sử dụng biện pháp DDOS để tấn công chiếm 51% số node là một vấn đề bảo mật cổ điển trong Bitcoin.

2. Khái niệm về Blockchain

Các công nghệ blockchain không chỉ là một kỹ thuật, mà còn chứa các thuật toán mật mã, toán học, thuật toán và mô hình kinh tế, kết hợp bởi mạng ngang hàng và sử dụng thuật toán phân tán để giải quyết vấn đề đồng bộ hóa cơ sở dữ liệu phân tán, đó là một kết hợp cấu trúc đa cấp(J. Garay, A. Kiayias và N. Leonardos, 2015).

Công nghệ blockchain bao gồm sáu yếu tố chính:

Phân tán (Decentralized): các tính năng cơ bản của Blockchain, có nghĩa là Blockchain không phải dựa vào node (nút) tập trung (máy chủ) nữa, dữ liệu có thể được ghi lại, lưu trữ và cập nhật phân tán.

Minh bạch (Transparent): các dữ liệu được ghi bởi hệ thống Blockchain là minh bạch tại mỗi node, minh bạch về cập nhật dữ liệu, đó là lý do tại sao Blockchain đáng tin cậy.

Mã nguồn mở (OpenSource): hầu hết hệ thống Blockchain đều mở cho mọi người xem, hồ sơ có thể được kiểm tra công khai và mọi người cũng có thể sử dụng các công nghệ Blockchain để tạo ra bất kỳ ứng dụng nào họ muốn.

Tự chủ (Autonomy): do cơ sở đồng thuận, mỗi node trên hệ thống Blockchain có thể truyền hoặc cập nhật dữ liệu một cách an toàn và không ai có thể can thiệp nó.

Không thể thay đổi (Immutable): bất kỳ ghi chép nào sẽ được giữ mãi mãi và không thể thay đổi trừ khi ai đó có thể kiểm soát hơn 51% node trong cùng một thời điểm.

Ẩn danh (Anonymity): các công nghệ Blockchain đã giải quyết vấn đề tin cậy giữa các node với nhau, do đó việc truyền dữ liệu hoặc thậm chí là giao dịch có thể được ẩn danh, chỉ cần biết địa chỉ Blockchain của đối tượng đó.

2.1. Quy trình hoạt động của Blockchain

Quy trình làm việc chính của Blockchain như sau:

(1) Nodetruyền dữ liệu sẽ ghi lại thông tin mới và phát rộng rãi lên mạng.

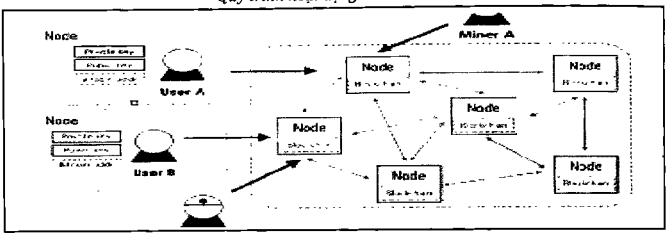
Nguyễn Cường, TS., Trường đại học Công nghệ giao thông vận tải.

(2) Node nhận được kiểm tra thông báo từ những dữ liệu mà nó nhận được, nếu tin là chính xác sau đó nó sẽ được lưu trữ vào một block (khối).

(3) Tất cả node thu nhận trong mạng thực hiện phép thuật toán chứng minh công việc (PoW) hoặc bằng chứng chứng minh (PoS) cho block.

(4) Block sẽ được lưu trữ trong chuỗi sau khi thực hiện các thuật toán đồng thuận, mỗi node trong mạng thừa nhận khối này và sẽ liên tục mở rộng chuỗi cơ bản trên khối này.

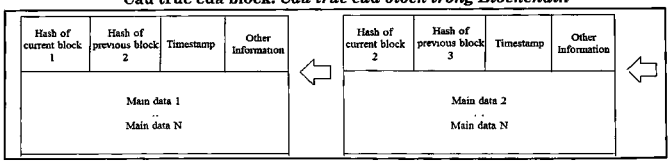
Quy trình hoạt động của Blockchain



Nguồn: Blockgeeks.com, 2107.

2.2. Cấu trúc của Blockchain

Cấu trúc của block: ***Cấu trúc của block trong Blockchain***



Nguồn: Iuon-Chang Lin và Tzu-Chun Liao, 2017.

Nói chung trong block, nó chứa dữ liệu chính, hash (một phần thông tin) của khối trước đó, hash của khối hiện tại, dấu vết về thời gian và các thông tin khác. Hình 1 cho thấy cấu trúc khối.

MainData (dữ liệu chính): tùy thuộc vào ứng dụng dịch vụ của Blockchain là gì, ví dụ: hồ sơ giao dịch, thanh toán bù trừ ngân hàng, hồ sơ hợp đồng hoặc dữ liệu IOT.

Hash (gọi là hàm băm hay hàm số toán học ánh xạ mã hóa dữ liệu có độ dài bất kỳ thành có độ dài nhất định): khi một giao dịch thực hiện, nó đã được hash đến một mã và sau đó truyền đến cho mỗi node. Bởi vì nó có thể được chứa hàng ngàn hồ sơ giao dịch trong khối của mỗi node, Blockchain được sử dụng chức năng cây Merkle để tạo ra một giá trị hash cuối cùng, đó cũng là gốc của cây Merkle. Giá trị hash cuối này sẽ được ghi vào tiêu đề block (hash của block hiện tại), bằng cách sử dụng chức năng cây Merkle, truyền dữ liệu và tài nguyên máy tính có thể được giảm rất lớn.

Timestamp (đánh dấu thời gian): là thời gian mà block được tạo ra.

OtherInformation (thông tin khác): giống như đặc tính của khối, hoặc dữ liệu khác mà người dùng xác định.

2.3. Làm thế nào để có được sự đồng thuận?

Chức năng đồng thuận là một cơ chế làm cho tất cả các nodeBlockchain có thỏa thuận trong cùng một thông báo, có thể chắc chắn rằng khối mới nhất đã được thêm vào chuỗi một cách chính xác, đảm bảo rằng thông điệp được lưu trữ bởi node là cùng một và sẽ không xảy ra "xung đột chia tách", thậm chí có thể bảo vệ khỏi các cuộc tấn công mạng.

2.4. Chứng nhận công việc (Proof of Work - PoW)

Chứng minh về công việc là một phần của dữ liệu rất khó phân biệt (tốn kém hoặc tốn nhiều thời gian) để sản xuất nhưng dễ dàng cho người khác xác minh và thỏa mãn yêu cầu nào. Việc tạo ra bằng chứng về công việc có thể là một quy trình ngẫu nhiên với xác suất thấp để đòi hỏi phải có nhiều thử nghiệm và sai sót trước khi chứng minh được công việc hợp lệ được tạo ra. Bitcoin sử dụng hệ thống chứng nhận của Hashcash.

Khi tính PoW, nó được gọi là "khai thác mỏ - mining". Mỗi khối có giá trị ngẫu nhiên được gọi là "Nonce" trong tiêu đề khối, bằng cách thay đổi giá trị nonce này, PoW phải tạo ra một giá trị làm cho giá trị Hashtiêu đề khối nhỏ hơn "Độ khó mục tiêu" mà đã được thiết lập trước nó. Độ khó có nghĩa là nó mất bao nhiêu thời gian khi node tính giá trị hash thấp hơn giá trị mục tiêu.

Để một nhóm được các thành viên tham gia mạng chấp nhận, các thợ mỏ phải hoàn thành chứng nhận về công việc bao gồm tất cả các dữ liệu trong khối. Sự phức tạp của công việc này được điều chỉnh để hạn chế tốc độ mà các khối mới có thể được tạo trong mạng 10 phút một lần. Do xác suất rất thấp của sự thành công chứng thực, điều này làm cho nó không thể đoán trước được máy tính nào trong mạng sẽ có thể tạo ra khối kế tiếp (I. Bentov, A. Gabizon và A. Mizrahi, 2014).

2.5. Chứng thực sở hữu (Proof of Stake)

Bởi vì phương pháp ProofofWork sẽ gây lãng phí nhiều điện năng và tính toán, ProofofStake không cần máy tính mạnh và đắt tiền. Với ProofofStake, tài nguyên được so sánh là lượng Bitcoin người khai thác mỏ nắm giữ - một người giữ 1% Bitcoin có thể khai mỏ được 1% "ProofofStakeblocks" (S. King và S. Nadal, 2012).

Phương pháp ProofofStake có thể giúp tăng cường bảo vệ khỏi một cuộc tấn công nguy hiểm trên mạng. Tăng cường bảo mật do 2 nguyên nhân sau:

(1) Việc thực hiện cuộc tấn công sẽ tốn kém hơn nhiều.

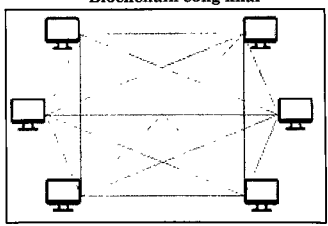
(2) Giảm bớt ý muốn tấn công. Kẻ tấn công sẽ cần phải sở hữu một phần lớn của tất cả bitcoin. Do đó, kẻ tấn công lại bị ảnh hưởng nặng nề từ cuộc tấn công của chính mình.

2.6. Phân loại Blockchain

Công nghệ Blockchain có thể được chia thành ba loại:

(1) Blockchain công khai: mọi người đều có thể kiểm tra giao dịch và xác minh nó, và cũng có thể tham gia vào tiến trình đạt được sự đồng thuận. Giống như Bitcoin và Ethereum đều là Blockchain công khai.

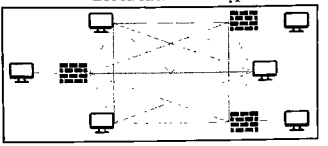
Blockchain công khai



Nguồn: Iuon-Chang Lin và Tzu-Chun Liao, 2017.

(2) Blockchain kết hợp: nghĩa là các node có thẩm quyền có thể được lựa chọn trước, thường có quan hệ đối tác như B2B, dữ liệu trong Blockchain có thể được công khai hoặc riêng tư, có thể được xem như phi tập trung một phần. Giống như Hyperledger và R3CEV là cả hai nhóm kết hợp.

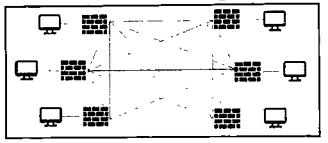
Blockchain kết hợp



Nguồn: Iuon-Chang Lin và Tzu-Chun Liao, 2017.

(3) Blockchain riêng tư: các node sẽ bị hạn chế nên phải tất cả các node có thể tham gia Blockchain này, các node có quyền quản lý nghiêm ngặt về khả năng truy cập dữ liệu.

Blockchain riêng tư



Nguồn: Iuon-Chang Lin và Tzu-Chun Liao, 2017.

Chúng ta cần Blockchain công khai vì sự thuận tiện của nó, nhưng đôi khi chúng ta có thể cần kiểm soát riêng tư như Blockchain kết hợp hoặc Blockchain riêng tư, tùy thuộc vào dịch vụ nó cung cấp hoặc nơi chúng tôi sử dụng nó.

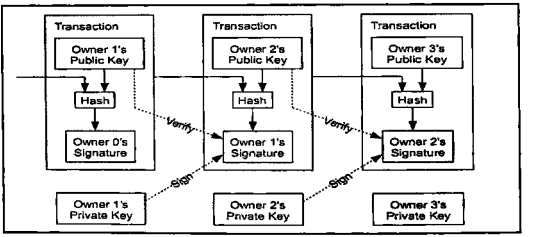
3. Ứng dụng công nghệ Blockchain

Công nghệ Blockchain có thể được sử dụng trong nhiều lĩnh vực, không chỉ trong ứng dụng tài chính, mà còn trong các ngành công nghiệp khác.

3.1. Đồng tiền kỹ thuật số: Bitcoin

Cơ cấu dữ liệu và hệ thống giao dịch của Bitcoin được xây dựng bằng công nghệ Blockchain, làm cho Bitcoin trở thành một đồng tiền số và hệ thống thanh toán trực tuyến. Bằng cách sử dụng kỹ thuật mật mã, việc chuyển tiền có thể đạt được và không cần phải dựa vào ngân hàng trung ương. Bitcoin sử dụng khóa công khai gửi và nhận Bitcoin, ghi lại giao dịch và cá nhân được ẩn danh. Quá trình xác thực giao dịch yêu cầu sức mạnh tính toán bởi máy tính của người dùng khác (máy tính đào) để có được sự đồng thuận, và sau đó ghi lại các giao dịch với mạng.

Phương thức giao dịch bằng Bitcoin

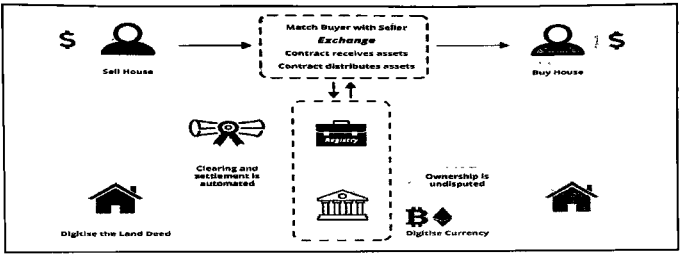


Nguồn: S. Nakamoto, 2013.

3.2. Hợp đồng thông minh: Ethereum

Hợp đồng thông minh là một hợp đồng kỹ thuật số kiểm soát tài sản số của người dùng, xây dựng quyền và nghĩa vụ của người tham gia, sẽ tự động thực hiện bằng hệ thống máy tính. Nó không chỉ là một thủ tục máy tính, nó có thể được xem như là một trong những bên tham gia hợp đồng, sẽ trả lời những gì nó nhận được và lưu trữ dữ liệu, nó cũng có thể gửi tin nhắn hoặc gửi giá trị cho ra ngoài. Hợp đồng thông minh là đáng tin cậy, có thể giữ tài sản tạm thời và sẽ làm theo thứ tự đã được lập chương trình.

Phương thức hoạt động của hợp đồng thông minh



Nguồn: Blockgeeks.com, 2107.

Ethereum là một nền tảng Blockchain mã nguồn mở kết hợp hợp đồng thông minh, cung cấp máy ảo phân tán để xử lý hợp đồng, bằng cách sử dụng đồng tiền kỹ thuật số gọi là ETH, mọi người có thể tạo ra nhiều dịch vụ, ứng dụng hoặc hợp đồng khác nhau trên nền tảng này.

3.4. Tài sản kỹ thuật số

Bitcoin tạo ra một cái gì đó độc đáo: tài sản kỹ thuật số. Trước Bitcoin, kỹ thuật số không đồng nghĩa với sự vô hạn. Mọi thứ kỹ thuật số có thể được sao chép bằng một node. có thể dễ dàng thấy về ngành công nghiệp âm nhạc và doanh số bán album nói lên câu chuyện này một cách thuyết phục.

Nhưng Bitcoin đã làm một cái gì đó mới: nó tạo ra mã kỹ thuật số không thể sao chép (uncopyable). Vì vậy, lần đầu tiên kể từ khi bit và byte được phát minh ra, có một cách để sở hữu một cái gì đó kỹ thuật số mà không thể sao chép được. Những con mèo ảo trong Crypto Kitten trên hệ thống Blockchain Etherium có giá 300 ETH (tương đương 300.000 USD) là ví dụ mới nhất về tài sản ảo.

Cho đến ngày nay, giá trị Bitcoin dựa trên công suất Blockchain của nó để ngăn ngừa in tiền quá nhiều và tạo ra các đồng tiền giả mạo. Với điều này trong tâm trí, các nhà phát triển Bitcoin và các đồng tiền mã hóa khác đã phát hành tiền kỹ thuật số lần đầu ra công chúng (ICO, ITO) có thể hoạt động như cổ phiếu trong một công ty.

3.5. Các ứng dụng khác

Vẫn còn nhiều khả năng sử dụng công nghệ Blockchain, như bảo vệ tài sản trí tuệ, truy xuất chuỗi cung ứng, giấy chứng nhận, bảo hiểm, thanh toán quốc tế, IOT, sự riêng tư của bệnh nhân trong điều trị y tế hoặc dự báo thị trường.

4. Vấn đề chia tách của Blockchain

Fork (chia tách) có liên quan đến các phiên bản thỏa thuận của node phân tán khi nâng cấp phần mềm. Đó là một vấn đề rất quan trọng bởi vì nó liên quan đến một phạm vi rộng trong Blockchain.

Khi phiên bản mới của phần mềm Blockchain được ban hành, thỏa thuận mới trong nguyên tắc đồng thuận cũng thay đổi các node. Vì vậy, các node trong mạng Blockchain có thể được chia thành hai loại, các node mới và các node cũ. Vì vậy, ở đây có 4 tình huống:

(1) Các node mới đồng ý với giao dịch của khối được gửi bởi các node cũ.

(2) Các node mới không đồng ý với giao dịch của khối được gửi bởi các node cũ.

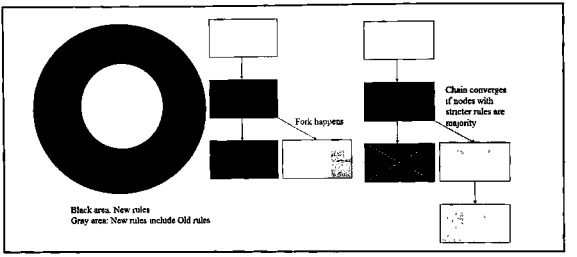
(3) Các node cũ đồng ý với giao dịch của khối được gửi bởi các node mới.

(4) Các node cũ không đồng ý với giao dịch

của khối được gửi bởi các node mới.

Bởi vì bốn trường hợp khác nhau trong việc đồng thuận, vấn đề ngã ba xảy ra, và theo bốn trường hợp này, các vấn đề Fork có thể được chia thành hai loại, HardFork và SoftFork. Ngoài việc phân biệt các node mới và các node cũ, chúng ta phải so sánh sức mạnh tính toán của các node mới với các nnode cũ, và giả sử rằng sức mạnh tính toán của các node mới là hơn 50.

Sơ đồ chia tách cứng

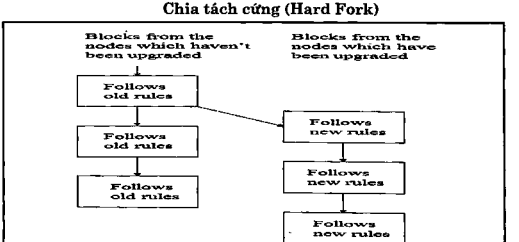


Nguồn: Iuon-Chang Lin và Tzu-Chun Liao, 2017.

- Chia tách cứng (HardFork)

HardFork là khi hệ thống đi đến một phiên bản mới hoặc thỏa thuận mới và nó không tương thích với phiên bản trước đó, các node cũ không chấp nhận với việc khai thác các node mới, do đó một chuỗi phân tách trở thành hai chuỗi. Mặc dù sức mạnh tính toán của các node mới mạnh hơn các node cũ, các node cũ vẫn tiếp tục duy trì chuỗi mà nó đang dùng.

Chia tách cứng (Hard Fork)



Nguồn: Iuon-Chang Lin và Tzu-Chun Liao, 2017.

Khi HardFork xảy ra, chúng ta phải yêu cầu tất cả các node trong mạng để cập nhật. Nếu có nhiều node cũ không cập nhật, thì chúng sẽ tiếp tục làm việc trên một chuỗi hoàn toàn khác, có nghĩa là chuỗi thông thường sẽ chia tách thành hai chuỗi.

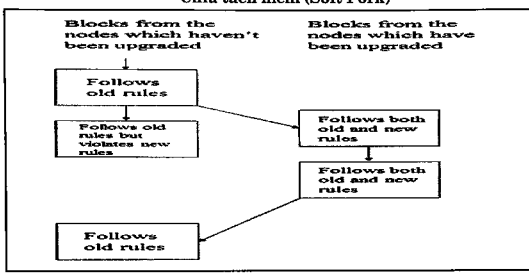
Ví dụ: Hard Fork chia tách Bitcoin thành: Bitcoin và Bitcoin Cash ngày 1-8-2017.

- Chia tách mềm (SoftFork)

SoftFork có nghĩa là khi hệ thống đi đến một phiên bản mới hoặc thỏa thuận mới và nó không tương thích với phiên bản trước

đó, các node mới không thể đồng ý với việc khai thác các node cũ. Bởi vì sức mạnh tính toán của các node mới mạnh hơn các node cũ, khối được khai thác bởi các node cũ sẽ không bao giờ được chấp nhận bởi các node mới, nhưng các node mới và các node cũ vẫn sẽ tiếp tục hoạt động trên cùng một chuỗi.

Chia tách mềm (Soft Fork)



Nguồn: Iuon-Chang Lin và Tzu-Chun Liao, 2017.

Khi SoftFork xảy ra, các node trong mạng không phải nâng cấp thỏa thuận mới vào cùng một thời điểm, nó sẽ cho phép nâng cấp dần dần. Không giống như HardFork, SoftFork sẽ chỉ có một chuỗi, nó sẽ không ảnh hưởng đến sự ổn định và hiệu quả của hệ thống khi các node nâng cấp. Tuy nhiên, SoftFork làm cho các node cũ không biết rằng các nguyên tắc đồng thuận đã bị thay đổi, trái với các nguyên tắc của tất cả các node có thể xác minh một cách chính xác một mức độ. Ví dụ: Etherium chia tách thành: Etherium và Etherium Classic.

Quá tải hệ thống

Do các hệ thống Blockchain của Bitcoin hay còn gọi là Blockchain 1.0 được thiết kế từ những năm trước 2010 bị lạc hậu với khả năng xử lý được tối đa 3 giao dịch một giây. Với đồng Bitcoin tăng giá và sự quan tâm của người dùng với tổng lượng giao dịch khoảng 18 tỷ USD một ngày đã khiến hệ thống Blockchain của Bitcoin đã đạt tới mức giới hạn làm cho thời gian xác nhận giao dịch lên tới 30 giờ, và phí giao dịch lên tới 30 USD khiến cho Bitcoin không còn thực sự là tiền tệ điện tử, mà chuyển thành dạng tài sản điện tử. Việc xuất hiện các đồng tiền điện tử mới như Etherium, Bitcoin cash... hay các đồng tiền Blockchain 2.0 đã giải quyết được các vấn đề về phí giao dịch với mức phí chỉ 0,03 đến 0,24 USD cho mọi giao dịch./.

TÀI LIỆU THAM KHẢO

1. *Blockgeeks.com.* (2107).

2. I. Bentov, A. Gabizon, & A. Mizrahi. (2014), Cryptocurrencies without proof of work,*CoRR.*

3. Iuon-Chang Lin & Tzu-Chun Liao. (2017), A Survey of Blockchain Security Issues and Challenges, *International Journal of Network Security*, 653-659.

4. J. Garay, A. Kiayias, & N. Leonardos. (2015), *The Bit coin Backbone Protocol: Analysis and Applications*, Berlin: Springer Berlin Heidelberg.

5. S. King & S. Nadal. (2012), Ppcoin: Peer-to-peer Crypto-Currency with Proof-of-Stake, *archive.org.*

6. S. Nakamoto. (2013), Bitcoin: A Peer-to-Peer Electronic Cash System, *bitcoin.org.*

7. *www.cryptokitties.co/marketplace.* (2017).

Ngày nhận bài: 5-12-2017
Ngày nhận bản sửa: 10-1-2018
Ngày duyệt đăng: 22-1-2018