

SV: Hoàng Ngọc Thắng

**BÁO CÁO**

**Môn học: Thực tập viết niên luận**

*Tháng 7 - 2019*

**ĐẠI HỌC HUẾ**

**TRƯỜNG ĐẠI HỌC KHOA HỌC**

**KHOA CÔNG NGHỆ THÔNG TIN**

**Đề tài: Tìm hiểu về Blockchain và ứng dụng**

GV: Đặng Thanh Chương

**Mục lục**

[**A. Blockchain** 2](#_Toc12975205)

[**I. Giới thiệu** 2](#_Toc12975206)

[**II. Blockchain là gì** 4](#_Toc12975207)

[**1. Đặc điểm** 4](#_Toc12975208)

[**2. Cách thức Blockchain làm việc** 4](#_Toc12975209)

[**3. Một số khái niệm liên quan** 7](#_Toc12975210)

[**a. Hàm hash (băm)** 7](#_Toc12975211)

[**b. Con trỏ hash** 8](#_Toc12975212)

[**c. Cây Merkle** 8](#_Toc12975213)

[**d. Timestamp** 9](#_Toc12975214)

[**e. Cơ chế đồng thuận** 10](#_Toc12975215)

[**f. Xác định một chuỗi khối thống nhất** 10](#_Toc12975216)

[**g. Chữ kí điện tử** 13](#_Toc12975217)

[**B. Ứng dụng Blockchain vào y tế** 18](#_Toc12975218)

[**I. Bài toán đặt ra** 18](#_Toc12975219)

[**II. Sử dụng Blockchain** 18](#_Toc12975220)

[**1. Tiềm năng sử dụng** 18](#_Toc12975221)

[**a. Về quản lí hồ sơ bệnh nhân** 18](#_Toc12975222)

[**b. Về mặt nghiên cứu** 18](#_Toc12975223)

[**c. Về mặt chi phí, hiệu quả chữa bệnh** 18](#_Toc12975224)

[**2. Ví dụ thực tiễn** 18](#_Toc12975225)

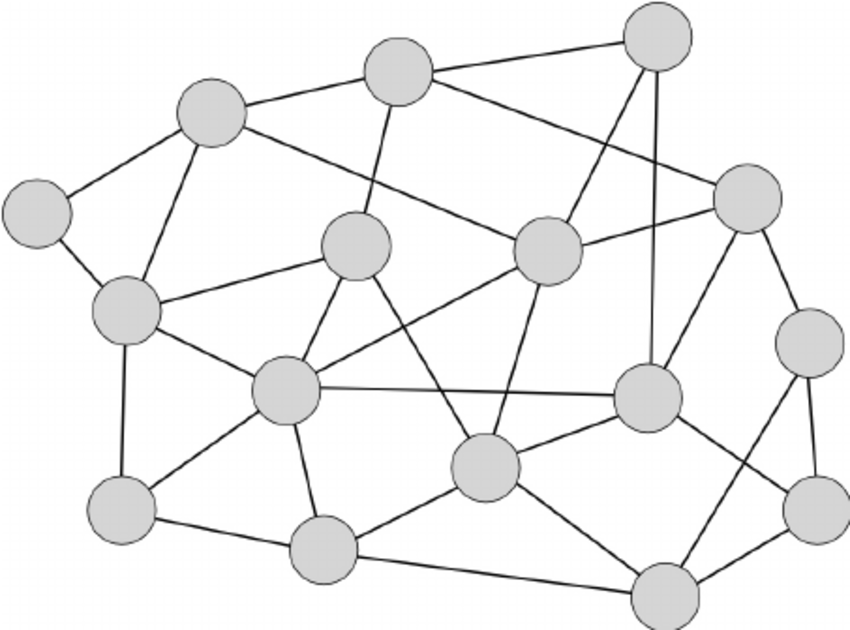
[**Tài liệu tham khảo** 22](#_Toc12975226)

# **A. Blockchain**

## **I. Giới thiệu**

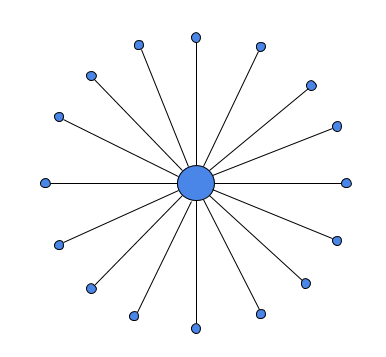
Trong thời đại hiện nay, công nghệ tài chính ngày càng phát triển, nhiều loại tiền điện tử ra đời và đi theo sau nó chính là Blockchain. Đây là một công nghệ mới hứa hẹn sẽ có nhiều phát triển và ứng dụng trong tương lai. Ở đây ta sẽ xem Blockchain hoạt động như thể nào và tại sao lại chọn Blockchain.

Mạng ngang hàng: gồm nhiều nút mạng liên kết với nhau, mỗi nút mạng có vai trò, vị trí như nhau. Độ tin cậy của mạng phụ thuộc vào độ tin cậy của các nút mạng. [1]



Hình I.1: Mạng ngang hàng

Mạng tập trung: các nút mạng cùng liên kết tới 1 nút trung tâm, nút này nắm toàn quyền quản lý, truy cập, trao đổi thông tin, cần phải có 1 lượng chi phí lớn để duy trì, đảm bảo hoạt động của nút trung tâm. [1]



Hình I.2: Mạng tập trung

Với lí do chi phí lớn như vậy cho nên các thông tin, dữ liệu cần được lưu trữ trong mạng ngang hàng. Cần có 1 giải pháp bảo mật các thông tin và Blockchain được xem như là 1 giải pháp.

## **II. Blockchain là gì**

Blockchain là công nghệ được phát minh bới Nakamoto vào năm 2008. Đây là 1 danh sách các bản ghi (hoặc được gọi là các nút) nối với nhau. Blockchain được tạo ra với mục đích là phục vụ cho hệ thống tiền điện tử bitcoin như là 1 cuốn sổ cái lưu trữ cái giao dịch 1 cách công khai

### **1. Đặc điểm**

Có 5 đặc điểm sau:

1. Tất cả các bản ghi về thông tin giao dịch trong mạng ngang hàng được lưu trong 1 cuốn sổ cái (Blockchain)

2. Tất cả thông tin được chuyển thông qua blockchain đều được mã hóa và mọi bản ghi cũng như vậy. Tức là khi 1 block được tạo ra và gắn vào chain, bản ghi đó ko thể thay đổi được

3. Blockchain sử dụng mạng ngang hàng nên mọi giao dịch ko cần phải thông qua trung gian

4. Blockchain không chỉ có thể sử dụng để chuyển tiền ảo mà còn có thể sử dụng với mọi loại bản ghi, mọi loại dữ liệu

5. Blockchain có tính phân tán [4]

Tuy có ưu điểm là vậy nhưng bên cạnh đó cũng có 1 số hạn chế về mặt công nghệ, Blockchain có giá cao hơn nhiều khi so sánh với cơ sở dữ liệu tập trung. Việc phát triển chậm hơn, mở rộng khó và chi phí bảo trì đắt đỏ.

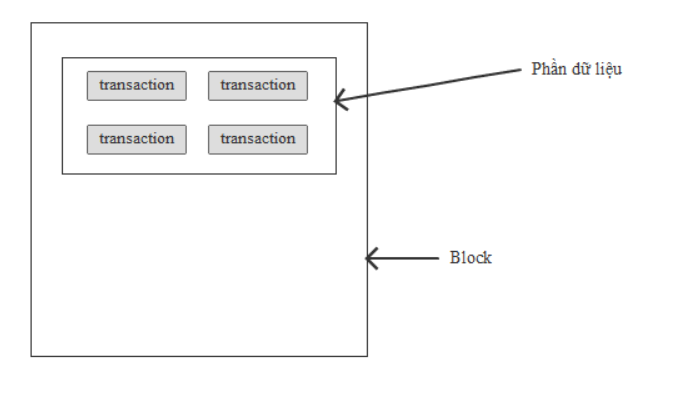
### **2. Cách thức Blockchain làm việc**

**Bước 1:** 2 bên A, B đồng ý trao đổi 1 đơn vị giá trị (có thể là mua bán, trao đổi, ở đây sẽ là trao đổi tiền ảo hoăc) để bắt đầu 1 tiến trình giao dịch (transaction)



Hình I.3: 1 giao dịch (transaction)

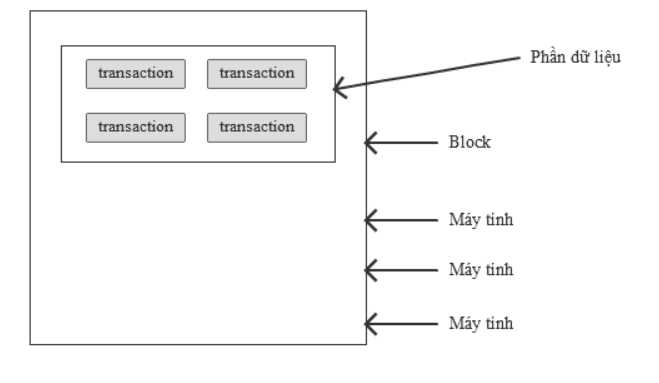
**Bước 2:** Giao dịch này sẽ được kết hợp với các giao dịch đang chờ khác để tạo thành “block”.



Hình I.4: 1 Block bao gồm các giao dịch

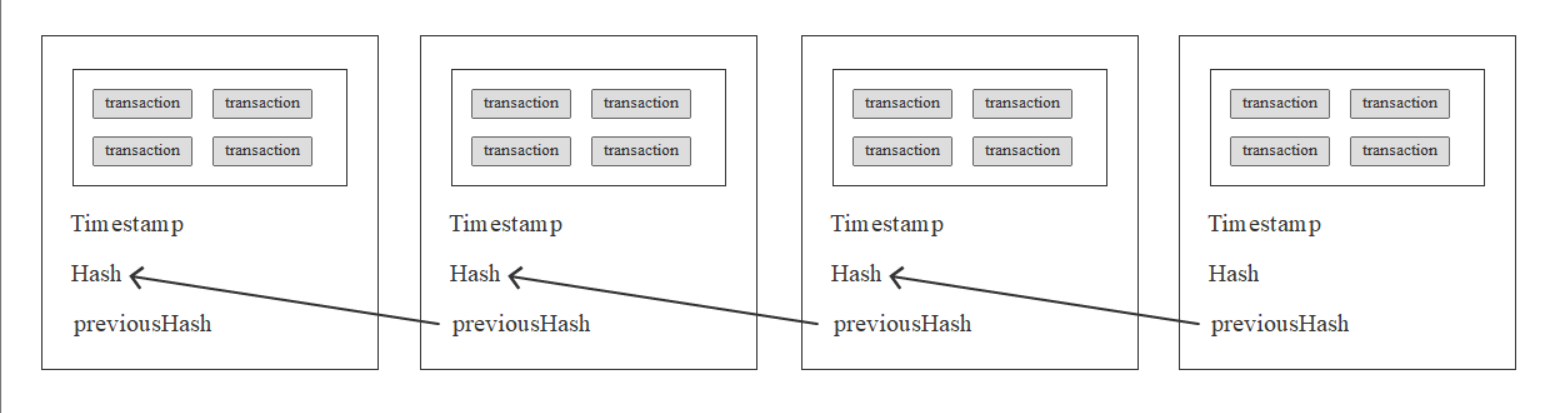
Block đang chờ này sẽ được gửi tới các máy tính tham gia trên mạng (trong thị trườn bitcoin gọi là các máy đáo tiền ảo) để đánh giá các giao dịch được chứa trong đó. Các máy tính đánh giá theo 1 kỹ thuật toán học nào đó đã được định trước.

**Bước 3:** Các giao dịch trong block được đánh giá cho tới 1 mức gọi là “đồng thuận” hoặc có hơn 50% các máy tính đánh giá đồng ý thông qua thì block được xác thực sau đó nó được gắn vào blockchain



Hình I.5: Xác minh Block bởi các máy tính

**Bước 4:** Những block này tiếp tục đợi đánh thời gian (timestamp) kèm theo 1 hóa đơn điện tử (trong trường hợp này có hóa đơn là do đang giao dịch bitcoin). Bên cạnh đó, 1 block còn giữ them 1 tham chiếu tới hàm băm (hash) của block trước. Tại blockchain tất cả các bản ghi đều không thể thay đổi được (trong trường hợp này là thông tin của các giao dịch sẽ là bản ghi).



Hình I.6: 1 Blockchain đơn giản

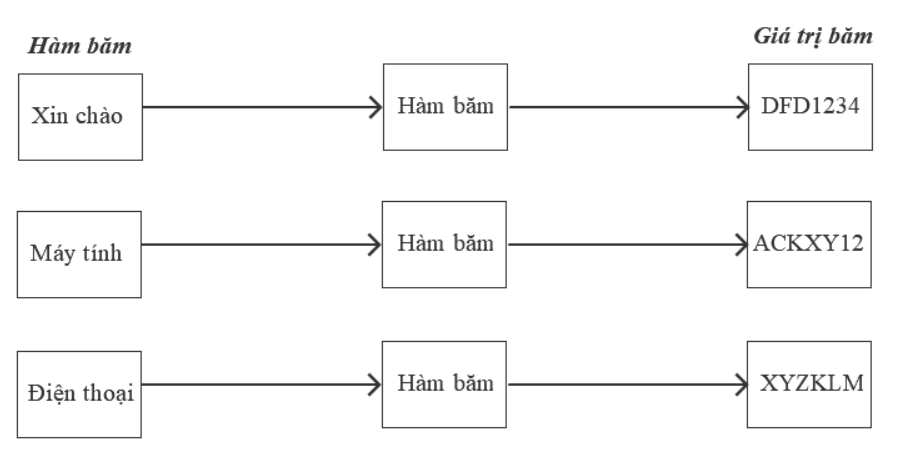
**Bước 5:** Khi giao dịch được hoàn thành thì bên B sẽ nhận được đơn vị giá trị từ bên A

### **3. Một số khái niệm liên quan**

#### **a. Hàm hash (băm)**

Đây là một hàm chuyển đổi đầu vào của các chữ cái và số thành đầu ra được mã hóa có độ dài cố định. Chuỗi đầu ra hay giá trị hash này sẽ được xem như là 1 khóa để phân biệt chuỗi đầu vào.[2]

Theo sơ đồ Blockchain ở trên ta là 1 ví dụ cho việc giá trị hash là 1 khóa.



Hình I.7: Ví dụ đơn giản về hàm Hash [2]

Hàm hash có 2 tính chất cơ bản:

- Đầu vào là 1 chuỗi ký tự có độ dài bất kỳ

- Luôn trả về chuỗi có độ dài cố định

Bên cạnh đó trong mật mã học còn sử dụng hàm băm mật mã, hàm băm mật mã thêm có 2 tính chất :

- Tính 1 chiều: Gọi ***H(x)*** là 1 hàm hash có tham số đầu vào là x. Ta có ***H(x) = y***.

Cho dù biết được y thì cũng ko thể suy ra được giá trị đầu vào của x. (Nghĩa là không thể tìm được chuỗi ban đầu từ 1 giá trị hash )

- Tính không va chạm: không va chạm là khi không thể tìm được 2 chuỗi đầu vào x và y khác nhau, nhưng lại có giá trị hash bằng nhau ***H(x) = H (y)***. (Nghĩa là không thể tìm được 2 chuỗi khác nhau nhưng có giá trị hash bằng nhau) [3]

MD5 (khi tải phần mềm từ Internet xuống máy tính) và SHA-256 (dùng trong bitcoin) là các thuật toán băm thường thấy

#### **b. Con trỏ hash**

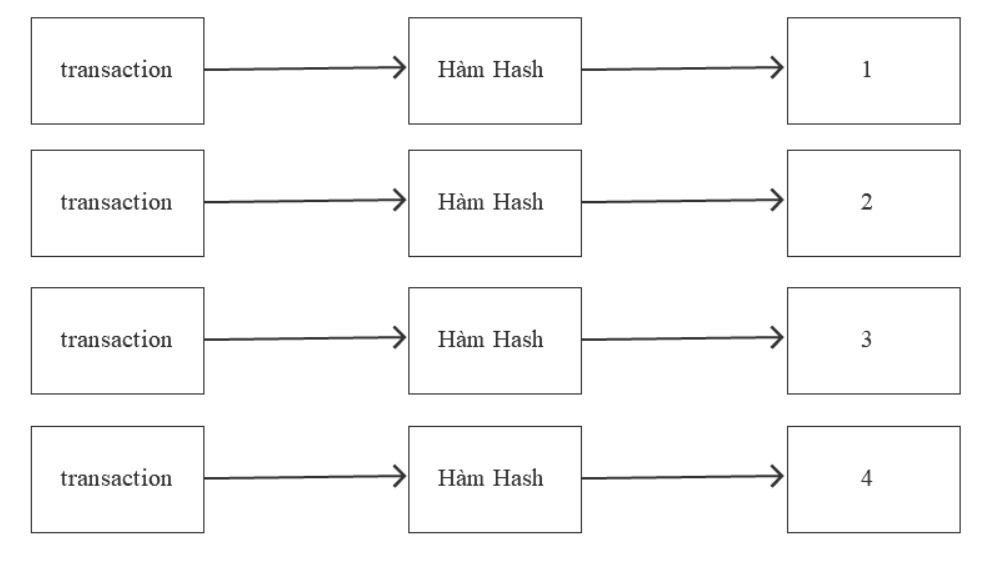
Con trỏ hash (Hash pointers) là một con trỏ thông thường ([pointers](https://en.wikipedia.org/wiki/Pointer_(computer_programming))) nhưng có kèm theo giá trị hash của nội dung được trỏ tới.

Như hình Blockchain, ta thấy được 1 block sẽ trỏ tới block trước đó, ngoài ra còn lưu thêm cả giá trị hash của khối trước (trường previousHash).

Nếu một khối bất kì có sự thay đổi, giá trị hash khối đó sẽ bị thay đổi, khối tiếp theo nó sẽ có giá trị previousHash không trùng với Hash cũ. Đây là 1 ví dụ để thấy được ý nghĩa của giá trị Hash và con trỏ Hash trong việc nhận biết dữ liệu có bị thay đổi hay không trong 1 block

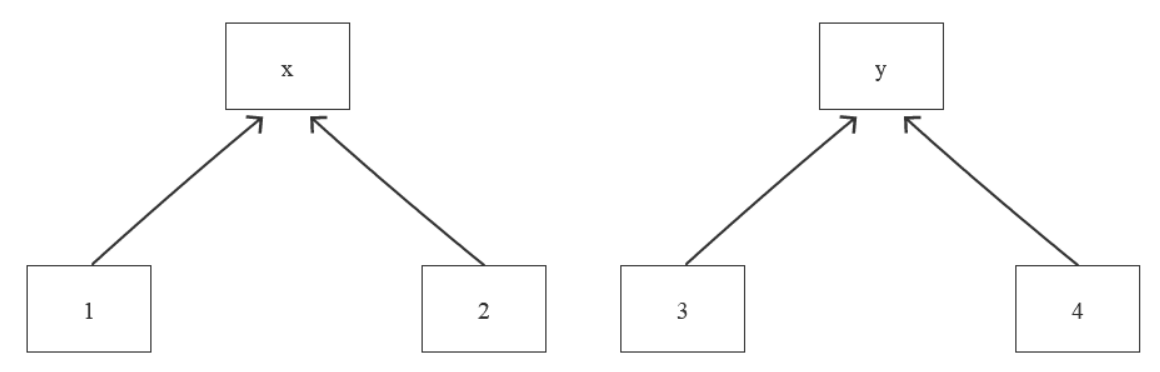
#### **c. Cây Merkle**

Giả sử ta có 4 giao dịch và sau khi đi qua hàm hash thì sẽ có các giá trị tương ứng như sau:



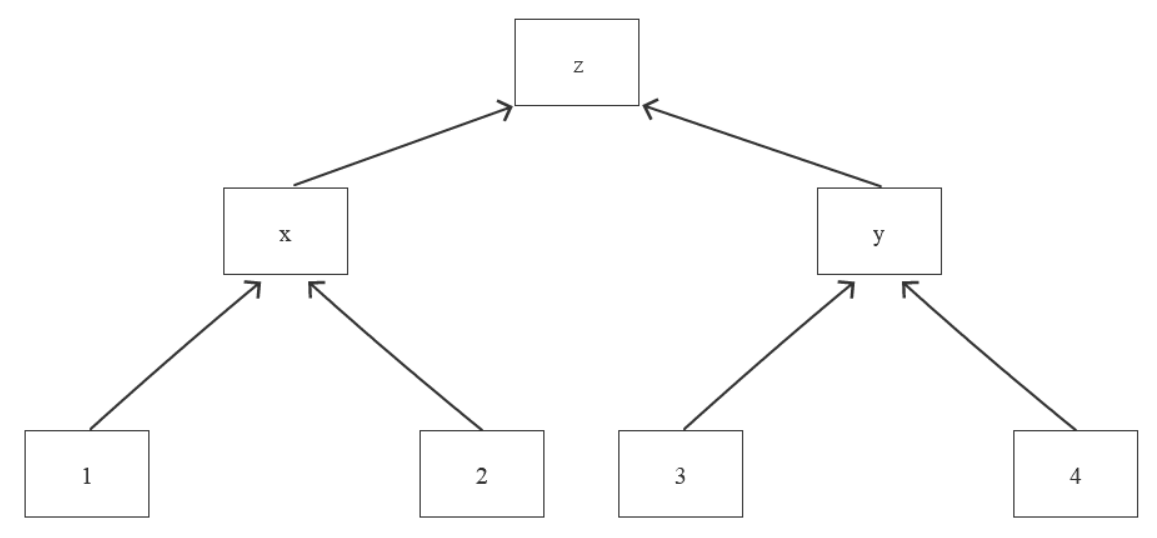
Hình I.8: Giao dịch đi qua hàm Hash

Các giá trị Hash của các giao dịch đó là 1, 2, 3, 4 tiếp tục đi qua hàm hash với công thức H=(a||b) với a,b là 2 giá trị vào, để có giá trị mới



Hình I.9: Giá trị Hash mới

Các giá trị mới này tiếp tục áp dụng công thức trên để ra 1 giá trị cuối cùng



Hình I.10 Cây Merkle hoàn chỉnh

Giá trị z này chính là giá trị của trường Hash trong block

#### **d. Timestamp**

Có 3 đặc điểm là :

- Tính phi tập trung: Mọi nút trong mạng đều có thể xác nhận timestamp xuất hiện khi nào (việc này là “đào” trong bitcoin)

- Tính bất biến: 1 khi timestamp được ghi lại thì không thể thay đổi giá trị

- Tính công khai: mọi timestamp đều là công khai mặc dù dữ liệu đã được mã hóa (ở đây là mã hóa bằng hàm Hash) [5]

Bên cạnh đó, timestap còn bao gồm 1 lượng dữ liệu trong đó, có thể là thông tin về những giao dịch, thông tin về liên lạc của 2 bên, thuật toán hash được sử dụng là gì,… [5]

#### **e. Cơ chế đồng thuận**

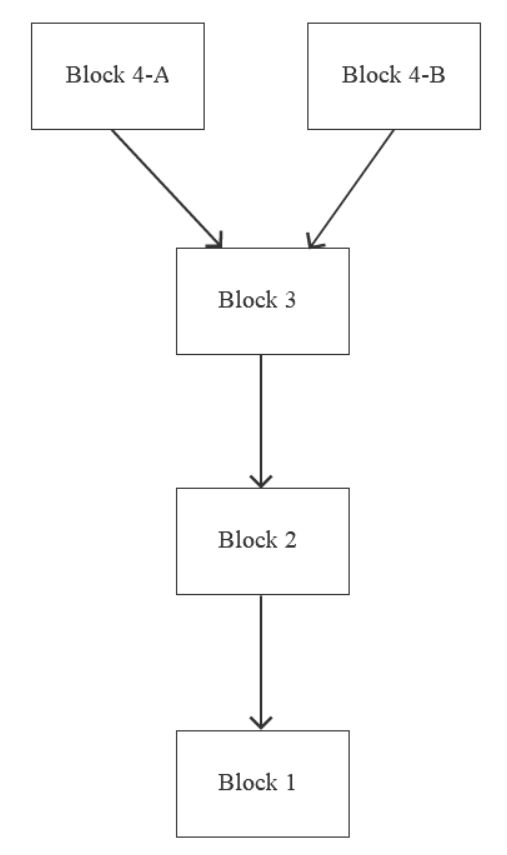
Đây chính là quá trình tìm giá trị Hash, có nhiều loại khác nhau nhưng có 2 loại tiêu biểu đó là:

- Proof of Work: sử dụng sức mạnh tài nguyên tính toán (CPU, năng lượng điện) để thực hiện giải mã thuật toán của Blockchain. Việc thực hiện giải mã này tốn rất nhiều thời gian, đặc biệt là theo thời gian, độ khó của mạng Blockchain được điều chỉnh tăng thì thời gian tạo block càng lâu.

- Proof of Authority: quá trình xác thực được thực hiện bởi những nút đó có danh tính rõ ràng, có khả năng xác nhận tính hợp lệ của các khối. cơ chế đồng thuận này cho phép thời gian tạo block nhanh hơn rất nhiều, do không phải mất thời gian chờ giải mã thuật toán

#### **f. Xác định một chuỗi khối thống nhất**

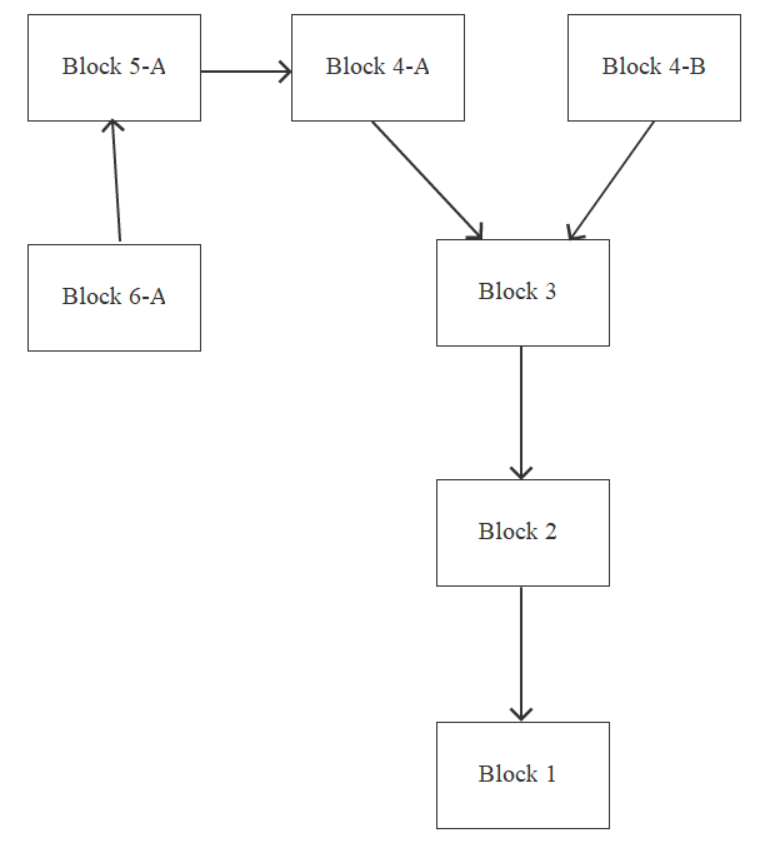
Trong blockchain, có thể tại 1 thời điểm nào đó đồng thời có 2 blockthỏa mãn được PoW, câu hỏi đặt ra là 2 block này và các block sau đó sẽ được gắn như thế nào vào blockchain. Lúc này tạm thời cả 2 block sẽ được gắn như hình



Hình I.11 Block mới đồng thời được gắn vào Blockchain

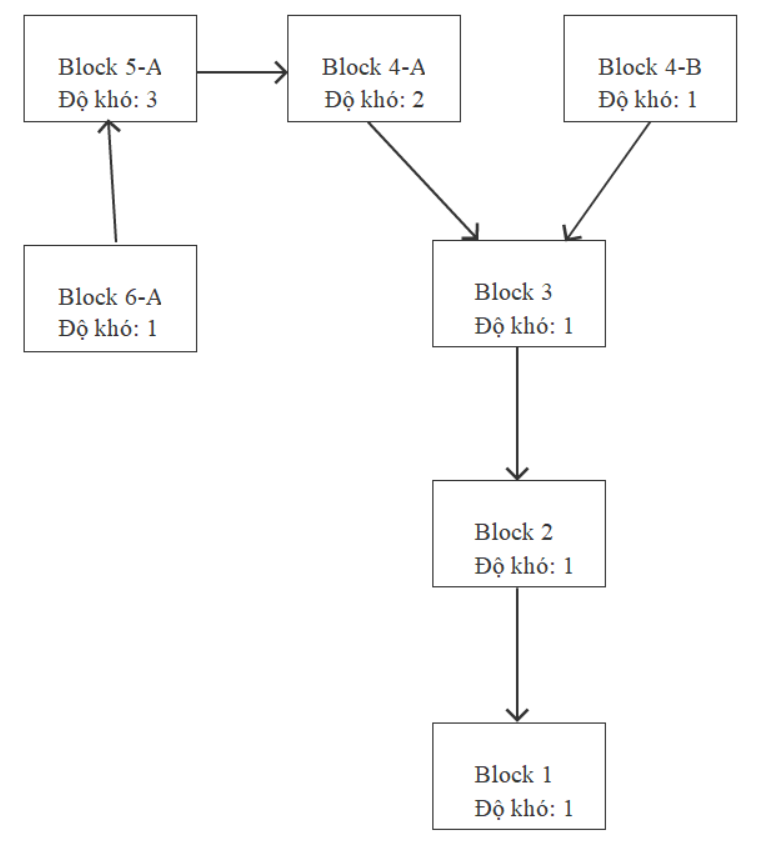
Ở đây sẽ có 2 cách để chọn để phát triển tiếp:

- Nhánh dài hơn: khi mà nhánh 4-A tạo được khối mới gắn tiếp vào trước và thông báo đến được hơn 51% nút mạng, thì tất cả block tiếp theo sẽ đi theo nhánh 4-A để đi tiếp. 4-B sẽ trở thành nhánh cụt, và giao dịch nằm trong 4-B sẽ được các nútt mạng tính toán lại Hash để tạo lại block mới gắn vào blockchain.



Hình I.12 Theo hướng nhánh dài hơn

- Nhánh có khối lượng tính toán lớn nhất: Tổng độ khó của PoW trên nhánh nào cao nhất thì phát triển tiếp theo nhánh đó. Ở đây ta thấy block 1, 2, 3 có tổng độ khó là 3. Với Block 4-A thì độ khó sẽ là 5, và 4-B độ khó là 4. Vì độ khó ở nhánh 4-A bây giờ cao nhất nên các block tiếp theo sẽ được móc nối tiếp vào block 4-A



Hình I. 13 Theo hướng nhánh có khối lượng tính toán lớn nhất

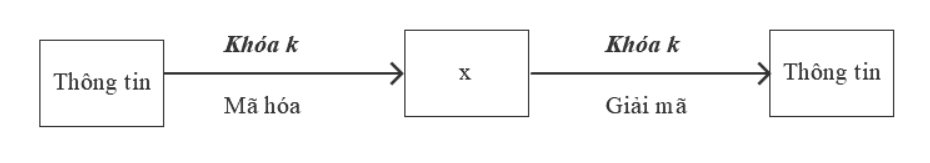
#### **g. Chữ kí điện tử**

Trước tiên, ta cần tìm hiểm xem các cơ chế sử dụng để mã hóa và giải mã thông tin, có 2 cơ chế chính

- Mã hóa đối xứng

- Mã hóa bất đối xứng

Mã hóa đối xứng là loại mã hóa và giải mã chỉ sử dụng 1 khóa (key) duy nhất

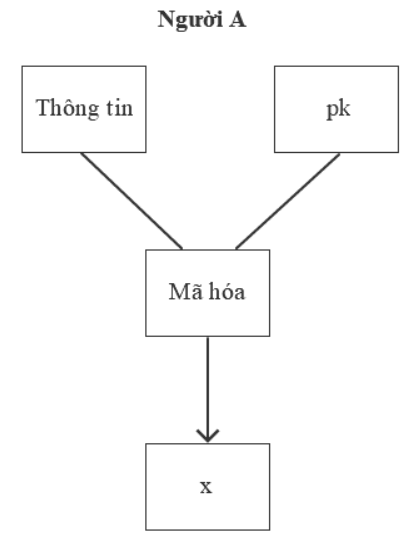


Hình I.14: Mã hóa đối xứng

Thông tin sử dụng khóa k mã hóa được giá trị x thì sau đó sử dụng lại chính khóa k đó thì mới giải mã ra được thông tin ban đầu

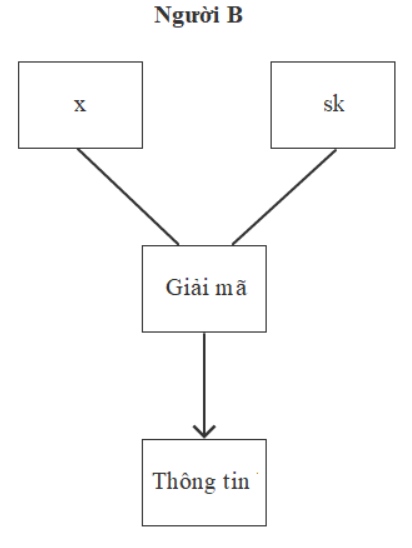
Mã hóa bất đối xứng là loại mã hóa và giải mã sử dụng 2 khóa (key) khác nhau. 1 khóa được gọi là khóa bí mật (Secret Key) kí hiệu là sk, 1 khóa được gọi là khóa công khai (Public Key) kí hiệu là pk

Ví dụ 1 người A muốn gửi thông tin của mình đi cho người B. Thông tin sẽ kết hợp với khóa công khai của B (pk của B) để được mã hóa thành đầu ra có 1 giá trị x nào đó



Hình I.15: Mã hóa thông tin với khóa công khai

Người B muốn đọc được thông tin này thì sẽ sử dụng khóa bí mật của mình (sk của B) để giải mã



Hình I.16: Giải mã thông tin với khóa bí mật

Chữ kí điện tử:

Trong quá trình gửi thông tin, có thể có một người C nào đó chen vào. Người C có thể đánh cắp thông tin, giả mạo gửi thông tin khác (vì các khóa công khai có thể biết được nhờ chia sẻ công khai). Cần có 1 cách thức để ngăn chặn việc này và chữ kí điện tử ra đời

Có 3 thuật toán được sử dụng trong chữ kí điện tử:

- Tạo khóa (Generate): ***G(key)*** tạo ra 2 khóa sp và pk như đã thấy ở trên

- Tạo chữ ký (Signature): ***S(sk, x) = y*** tạo ra 1 chữ kí có giá trị y nào đó dựa trên thông tin cần gửi đã được mã hóa là x và khóa bí mật của người đó

- Xác minh chữ kí (Verify): ***V(pk, x, y)*** với chữ ký y cùng khóa pk của người gửi có phải cùng thông tin gửi có phải là cùng 1 người gửi ban đầu hay không.

Ví dụ: Người dùng A, B đăng ký sử dụng trên 1 hệ thống blockchain, hệ thống sẽ sử dụng thuật toán ***G(key)*** tạo cặp khóa cho A và B có giá trị như sau:

- sk:

+Người A: ska123

+Người B: skb123

-pk:

+Người A: pka456

+Người B: pkb456

Người A muốn gửi thông điệp “Xin chào” tới người B thì phải qua các bước sau:

B1: Người A lấy khóa pk của B và thông điệp “Xin chào” để mã hóa thông tin gửi đi

***H( pk của b, thông tin )***

***= H( pkb456, ‘Xin chào’ )***

***= defghik123456***

B2: Hệ thống sẽ tạo 1 chữ kí điện tử cho người A

***S( sk của a, thông tin đã mã hóa )***

***= S( ska123, ‘defghik123456’ )***

***= chukicuanguoia***

B3: Thông tin được gửi đi khi tới tay người B thì sẽ được xác minh chữ kí xem người gửi ban đầu là ai

***V( pk của a, thông tin đã mã hóa, chữ kí của người A)***

***= V( ska123, ‘defghik123456’, ‘chukicuanguoia’ )***

Hệ thống sẽ trả về xem đó có phải là của người gửi ban đầu không, nếu không thì người nhận B phải cẩn thận vì có thể kẻ gian đã đột nhập vào với mục đích xấu, nếu đúng là người gửi ban đầu thì tiếp tục thực hiện B4

B4: Giải mã thông tin nhận được với khóa sk của người B là skb123

# **B. Ứng dụng Blockchain vào y tế**

## **I. Bài toán đặt ra**

Các thông tin về bệnh nhân là những thông tin riêng tư, nó ảnh hưởng tới việc điều trị, dự đoán bệnh. Thông thường các thông tin này thường được chia sẻ trong môi trường như là các bác sĩ với nhau, nhà thuốc, nghiên cứu khoa học, các công ty dược phẩm,… Nhưng người bệnh thì có thể tới nhiều trung tâm y tế khác nhau và cần phải có 1 giải pháp để giữ được lịch sử khám bệnh, bệnh trạng của người đó. Điều này sẽ rất tiện lợi khi người bệnh di chuyển qua thành phố, tỉnh, quốc gia khác.

Bên cạnh đó hiện nay đã có 1 số giải pháp cơ bản nhưng tốc độ hồi đáp còn rất chậm và thiếu đi tính bảo mật. Gửi bệnh án thông qua email là 1 ví dụ điển hình.

## **II. Sử dụng Blockchain**

### **1. Tiềm năng sử dụng**

Có 3 tiềm năng sử dụng:

#### **a. Về quản lí hồ sơ bệnh nhân**

Các trung tâm, cơ sở y tế hiện nay còn thiếu tính gắn kết. Khi 1 người đi khám thì phải tự lưu trữ toàn bộ sổ khám bệnh, bệnh án của mình. Một vài trường hợp nếu không có nhưng thông tin này khi đi khám bệnh thì bệnh nhân bắt buộc phải đi xét nghiệm gây mất thời gian và chi phí.

Giải pháp: Các trung tâm, cơ sở y tế sẽ liên kết với nhau coi như là 1 mạng. Các thông tin của bệnh nhân được xem như là các giao dịch được lưu trữ. Với mô hình thế này Blockchain sẽ quản lí các thông tin, tạo ra sự nhất quán về bệnh tình của người bệnh, tăng hiệu quả trong việc chăm sóc sức khỏe. Vì hồ sơ của bệnh nhân đã được mã hóa, không ai có thể xem được trử khi bệnh nhân cung cấp thông tin đó, tạo sự bảo mật, an toàn thông tin

#### **b. Về mặt nghiên cứu**

Do các thông tin về y tế được lưu trữ trong Blockchain không thể can thiệp, chỉnh sửa cho nên nếu Nếu bệnh nhân đồng ý cũng cấp hồ sơ bệnh án của họ các nguồn dữ liệu này đảm bảo tính tin cậy và xác thực cao.

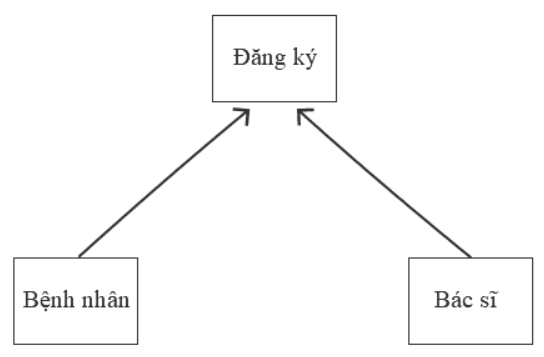
#### **c. Về mặt chi phí, hiệu quả chữa bệnh**

Vì các thông tin được lưu trữ có bệnh trạng rõ ràng, thời gian bệnh, uống thuốc, chữa bằng phương pháp nào, bác sĩ có được sự chính xác trong điều trị, bên cạnh đó tường mình về mặt chi phí khi điều trị và chi trả với các công ty bảo hiểm, nhà thuốc,…

### **2. Ví dụ thực tiễn**

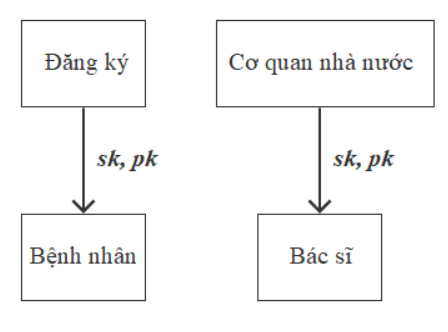
Một bệnh viện áp dụng Blockchain vào để quản lí thông tin của bệnh nhân, đây là những gợi ý cơ bản mô phỏng cách thức thực hiện

Đầu tiên người dùng phải đăng kí với hệ thống vai trò mà mình sẽ sử dụng (ở đây là bác sĩ hay là bệnh nhân).



Hình II.1: Đăng ký sử dụng dịch vụ

Sau khi đăng kí xong thì người dùng sẽ được nơi đăng kí cấp cho 1 cặp khóa (sk, pk) để mã hóa và giải mã thông tin. Riêng với bác sĩ thì cần phải có 1 cơ quan nhà nước thẩm định (thẩm định về bằng cấp, tay nghề thực tế) và cấp khóa



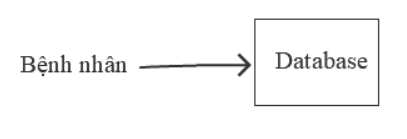
Hình II.2: Nhận khóa riêng tư và công khai

Các thông tin về bệnh nhân sẽ được lưu trong một cơ sở dữ liệu cố định ngoài Blockchain với các lí do:

- Nếu lưu quá nhiều thông tin trong Blockchain quá trình giải mã sẽ lây, không hiệu quả

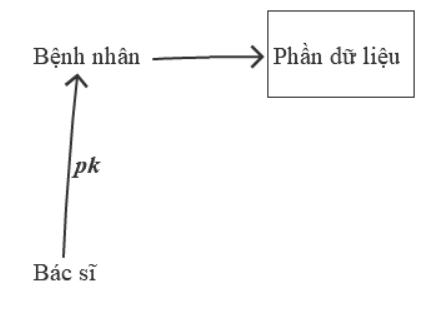
- 1 phần thông tin nào đó có thể bị lộ ra (do Timestamp lưu trữ)

- Bệnh nhân chỉ gửi các thông tin cần thiết hiện tại, không nhất thiết là toàn bộ thông tin cho bác sĩ



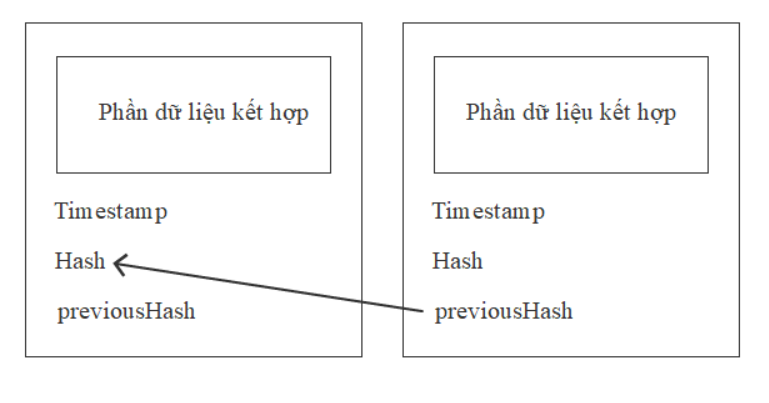
Hình II.3: Bệnh nhân nhập vào các thông tin ban đầu của mình

Khi mà bệnh nhân có nhu cầu khám bệnh, phải lấy thông tin cần thiết ra ngoài từ cơ sở dữ liệu. Bác sĩ sẽ cung cấp khóa pk của mình cho bệnh nhân, bệnh nhân sẽ gửi các thông tin cần thiết: lịch sử khám bệnh, kết quả xét nghiệm với khóa pk được nhận.



Hình II.4: Bệnh nhân gửi dữ liệu của mình cho bác sĩ

Các dữ liệu của bệnh nhân này kết hợp với dữ liệu của bệnh nhân khác tạo nên Block và theo 1 số các thao tác khác để gắn vào Blockchain



Hình II.5 Blockchain dữ liệu của bệnh nhân

Bác sĩ sau khi nhân được phần dữ liệu sẽ sử dụng sk của mình để giải mã và lấy được thông tin, sau khi đã khám bệnh, đè xuất trị liệu, cấp thuốc,.. thì cũng tương tự bệnh nhân gửi mà pk của mình cho bác sĩ, bác sĩ sử dụng pk đó kết hợp các thông tin mới rồi lại được ghép thành block chuyển vào blockchain rồi sau đó bệnh nhân giải mã với sk của mình. Thông tin mới nhận này tự động được lưu vào cơ sở dữ liệu của bệnh nhân, hoàn tất quá trình.

# **Tài liệu tham khảo**

**Tiếng Việt**

[1]: Kaopiz Software Co., Ltd. Khái niệm cơ bản về Blockchain

<https://kipalog.com/posts/Khai-niem-co-ban-ve-Blockchain>

[2]: Cơ chế hoạt động của công nghệ chuỗi khối Blockchain

http://aita.gov.vn/co-che-hoat-dong-cua-cong-nghe-chuoi-khoi-blockchain

**Tiếng Anh**

[3]: [Rafael Belchior](https://hackernoon.com/@rafaelbelchior), Blockchain For Students 101 —The Basics (Part 1)

<https://hackernoon.com/blockchain-for-students-101-the-basics-part-1-f39b8201a7d5>

[4]: Nick Grossman, The Blockchain as verified public timestamps

https://www.nickgrossman.is/2015/the-blockchain-as-time/

[5]: [Alevtina Dubovitskaya](https://www.ncbi.nlm.nih.gov/pubmed/?term=Dubovitskaya%20A%5BAuthor%5D&cauthor=true&cauthor_uid=29854130), [Zhigang Xu](https://www.ncbi.nlm.nih.gov/pubmed/?term=Xu%20Z%5BAuthor%5D&cauthor=true&cauthor_uid=29854130), [Samuel Ryu](https://www.ncbi.nlm.nih.gov/pubmed/?term=Ryu%20S%5BAuthor%5D&cauthor=true&cauthor_uid=29854130), [Michael Schumacher](https://www.ncbi.nlm.nih.gov/pubmed/?term=Schumacher%20M%5BAuthor%5D&cauthor=true&cauthor_uid=29854130), [Fusheng Wang](https://www.ncbi.nlm.nih.gov/pubmed/?term=Wang%20F%5BAuthor%5D&cauthor=true&cauthor_uid=29854130), Secure and Trustable Electronic Medical Records Sharing using Blockchain

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977675/>