

## Contents

<b>4. Kiến trúc Blockchain</b>	<b>1</b>
<b>4.1 Genesis Block</b>	<b>1</b>
4.1.1 Genesis Block là gì?	1
4.1.2 Thành phần chính của Khối khởi nguyên	1
4.1.3 Tổng quan về cách khối khởi nguyên được tạo và khai thác	2
4.1.4 Những đặc điểm của khối khởi nguyên	2
4.1.5 Tại sao cần khối khởi nguyên	2
<b>4.2 Bể nhớ (Memory Pool)</b>	<b>3</b>
4.2.1 Bể nhớ (memory pool) là gì?	3
4.2.2 Mục đích	4
4.2.3 Các cách phổ biến 1 giao dịch được đưa vào bể nhớ (memory pool)?	6
4.2.3 Cách 1 giao dịch rời khỏi bể nhớ?	7
4.2.4 Nơi Bể nhớ được lưu trữ?	8
<b>4.3 Khối ứng viên trong PoS</b>	<b>9</b>
4.3.1 Khối ứng viên là gì?	9
4.3.2 Cách tạo ra 1 khối ứng viên	11
4.2.3 Các yêu cầu đối với 1 khối ứng viên	12
<b>4.4 Các nhân tố liên quan đến phát triển blockchain</b>	<b>13</b>
<b>4.5 Vòng đời của giao dịch</b>	<b>14</b>
Các giai của giao dịch	14
Các hành động sau giao dịch	15
Các thử thách trong vòng đời của giao dịch	15
<b>5. Blockchain forks</b>	<b>16</b>
<b>Xác thực trong blockchain</b>	<b>17</b>
<b>Sự thay đổi quy tắc xác thực và các loại fork trong blockchain</b>	<b>17</b>
1. Soft Fork (Phân nhánh mềm)	18
2. hard fork	20

## 4. Kiến trúc Blockchain

### 4.1 Genesis Block

#### 4.1.1 Genesis Block là gì?

Genesis Block hay còn được gọi là khối khởi nguyên là khối đầu tiên của blockchain và chứa những đặc điểm duy nhất phân biệt nó với những khối còn lại. Nó là khối duy nhất không bắt nguồn từ khối trước nó vì không có khối nào tồn tại trước đó. Thay vào đó khối khởi nguyên được mã hóa cứng vào giao thức của blockchain như là 1 điểm bắt đầu.

#### 4.1.2 Thành phần chính của Khối khởi nguyên

1. Tiêu đề khối (Block Header): Giống như mỗi khối khác trong 1 blockchain, khối khởi nguyên có 1 tiêu đề khối bao gồm metadata chẳng hạn như phiên bản, merkle root, dấu thời gian và nonce. Tuy nhiên không giống với các khối khác nó không có previous hash.

2. Giao dịch coinbase: khối khởi nguyên bao gồm 1 giao dịch đặc biệt được gọi là giao dịch coinbase, nó là giao dịch đầu tiên của 1 blockchain

Ví dụ về khối khởi nguyên của bitcoin: 50BTC được tạo ra và nó không thể được sử dụng vì không có đầu ra hợp lệ

3. Tham số mạng: Khối khởi nguyên đặt tham số mạng đầu tiên bao gồm mục tiêu độ khó, kích thước khối lớn nhất và dấu thời gian khởi nguyên.

Ví dụ: khối khởi nguyên của bitcoin

- Độ khó: 1 (dễ nhất)
- Kích thước tối đa 1MB
- Dấu thời gian: 3/1/2009

4. Thông điệp được nhúng vào: 1 số khối khởi nguyên chứa thông điệp được người sáng tạo hoặc sáng lập blockchain đó nhúng vào.

Ví dụ: Khối khởi nguyên của bitcoin, Satoshi Nakamoto đã nhúng 1 thông điệp

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks” là tiêu đề 1 tờ báo anh đề cập đến cuộc khủng hoảng tài chính 2008-2009.

5. Giá trị băm của khối khởi nguyên: là 1 mã định danh duy nhất, được tạo ra từ nội dung của khối.

6. Phân bổ khối khởi nguyên: 1 số blockchain sử dụng khối khởi nguyên để phân bổ tài sản ban đầu.

Ví dụ: - Bitcoin: không có token nào được phân bổ sẵn trong khối khởi nguyên, toàn bộ bitcoin được khai thác theo thời gian

- Ethereum: khi ra mắt đã phân bổ 1 lượng ETH ban đầu từ khối khởi nguyên cho các nhà đầu tư.

#### 4.1.3 Tổng quan về cách khối khởi nguyên được tạo và khai thác

1. Phát triển và cấu hình: trước khi tạo ra mạng blockchain, các nhà phát triển tạo ra cấu trúc và thông số của khối khởi nguyên, nhúng các dữ liệu hoặc thông báo đặc biệt vào trong khối nguyên.
2. Tạo ra khối khởi nguyên: dữ liệu và thông số của khối khởi nguyên được mã hóa cứng vào file cấu hình hoặc file khởi nguyên. Một giá trị băm được tính toán cho toàn bộ khối bao gồm cả tiêu đề và dữ liệu được nhúng.
3. Quá trình khai thác: trong Proof Of Work giống như bitcoin, thợ đào chuẩn bị cho việc khai thác khối khởi nguyên bằng cách tải xuống phần mềm blockchain và file cấu hình. Thợ đào bắt đầu quá trình khai thác bằng cách tìm ra 1 giá trị băm hợp lệ cho target hash. Khi thợ đào tìm ra được giá trị băm hợp lệ, họ sẽ quảng bá lên mạng. Những node khác trong mạng sẽ xác minh theo các cơ chế đồng thuận được định nghĩa trong giao thức của blockchain.
4. Khởi chạy mạng: sau khi được xác minh, khối khởi nguyên được truyền đi khắp mạng, tất cả node sẽ tạo cơ sở dữ liệu của mình với dữ liệu từ khối khởi nguyên, thiết lập 1 điểm khởi đầu chung cho sổ cái blockchain. Khi khối khởi nguyên đã được thiết lập, các khối tiếp theo có thể đào và thêm vào blockchain.



#### 4.1.4 Những đặc điểm của khối khởi nguyên

- Không có khối trước đó
- Phần thưởng khối được cố định: trong 1 số mạng blockchain, khối khởi nguyên có phần thưởng khối cố định, điều này làm cho các khối tiếp theo giảm dần, được thiết kế để khuyến khích các thợ đào xác thực và xác minh các khối tiếp theo.
- Nó có giá trị băm duy nhất được mã hóa vào trong phần mềm và đảm bảo luôn là khối đầu tiên của mạng blockchain đó.
- khối khởi nguyên chứa giao dịch đặc biệt, có ý nghĩa lịch sử: đánh dấu sự khởi đầu của mạng phi tập trung và ngang hàng.
- làm cho blockchain bất biến: bất kỳ sự thay đổi trên khối khởi nguyên làm ảnh hưởng đến toàn bộ chuỗi.

#### 4.1.5 Tại sao cần khối khởi nguyên

- Khởi tạo mạng: vì nó chứa dữ liệu được mã hóa cứng là nền tảng cho các khối sau...
- Đảm bảo sự đồng thuận: dùng để thiết lập sự đồng thuận giữa các thành viên tham gia về trạng thái ban đầu của mạng.
- Cung cấp 1 điểm bắt đầu cố định: cung cấp điểm bắt đầu cố định cho blockchain, đảm bảo các khối đến sau có thể được xác minh và truy ngược về khối đầu. đảm bảo tính toàn vẹn và ngăn chặn hoạt động phá hoại.

Ví dụ về genesis block của bitcoin:



## Bitcoin Block 0

Mined on January 04, 2009 01:15:05 • [All Blocks](#)

[Satoshi](#) [Notable Block](#)

**Coinbase Message** • EThe Times 03/Jan/2009 Chancellor on brink of second bailout for banks



**Bitcoin Genesis**

On January 3rd 2009, the Bitcoin network was created when Satoshi Nakamoto (the project's mysterious creator) mined the "Genesis" block. The 50 bitcoin coinbase reward is unredeemable, as it was omitted from the transaction database. This means any attempt to spend it would be rejected by the network. Whether this was intentional or not still remains unknown.

[Read More](#)

---

### Details

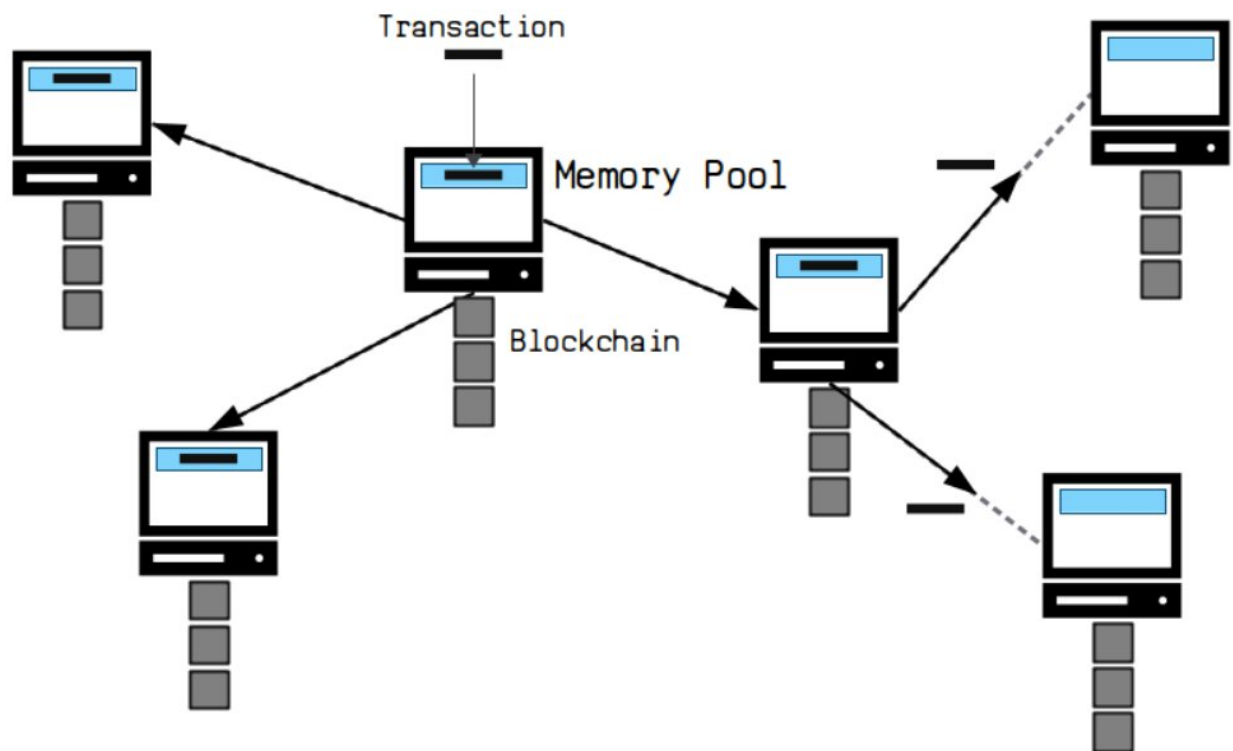
Hash	00000-ce26f 	Depth	887,784
Capacity	0.03%	Size	285
Distance	16y 2m 10d 21h 20m 55s	Version	0x1
BTC	0.0000	Merkle Root	4a-3b 
Value	\$0.00	Difficulty	1.00
Value Today	\$0.00	Nonce	2,083,236,893
Average Value	0.0000000000 BTC	Bits	486,604,799
Median Value	50.000000000 BTC	Weight	1,140 WU
Input Value	0.00 BTC	Minted	50.00 BTC
Output Value	50.00 BTC	Reward	50.000000000 BTC
Transactions	1	Mined on	01:15:05 04 thg 1, 2009
Witness Tx's	0	Height	0
Inputs	1	Confirmations	887,784
Outputs	1	Fee Range	∞-0 sat/vByte
Fees	0.000000000 BTC	Average Fee	0.000000000
Fees Kb	0.00000000 BTC	Median Fee	0.000000000
Fees kWU	0.00000000 BTC	Miner	Satoshi

## 4.2 Bể nhớ (Memory Pool)

// thiếu blockchain layer1, layer2, ...

### 4.2.1 Bể nhớ (memory pool) là gì?

Bể nhớ (Memory Pool) là nơi lưu trữ tạm thời các giao dịch chưa được xác nhận trước khi chúng được thêm vào blockchain.

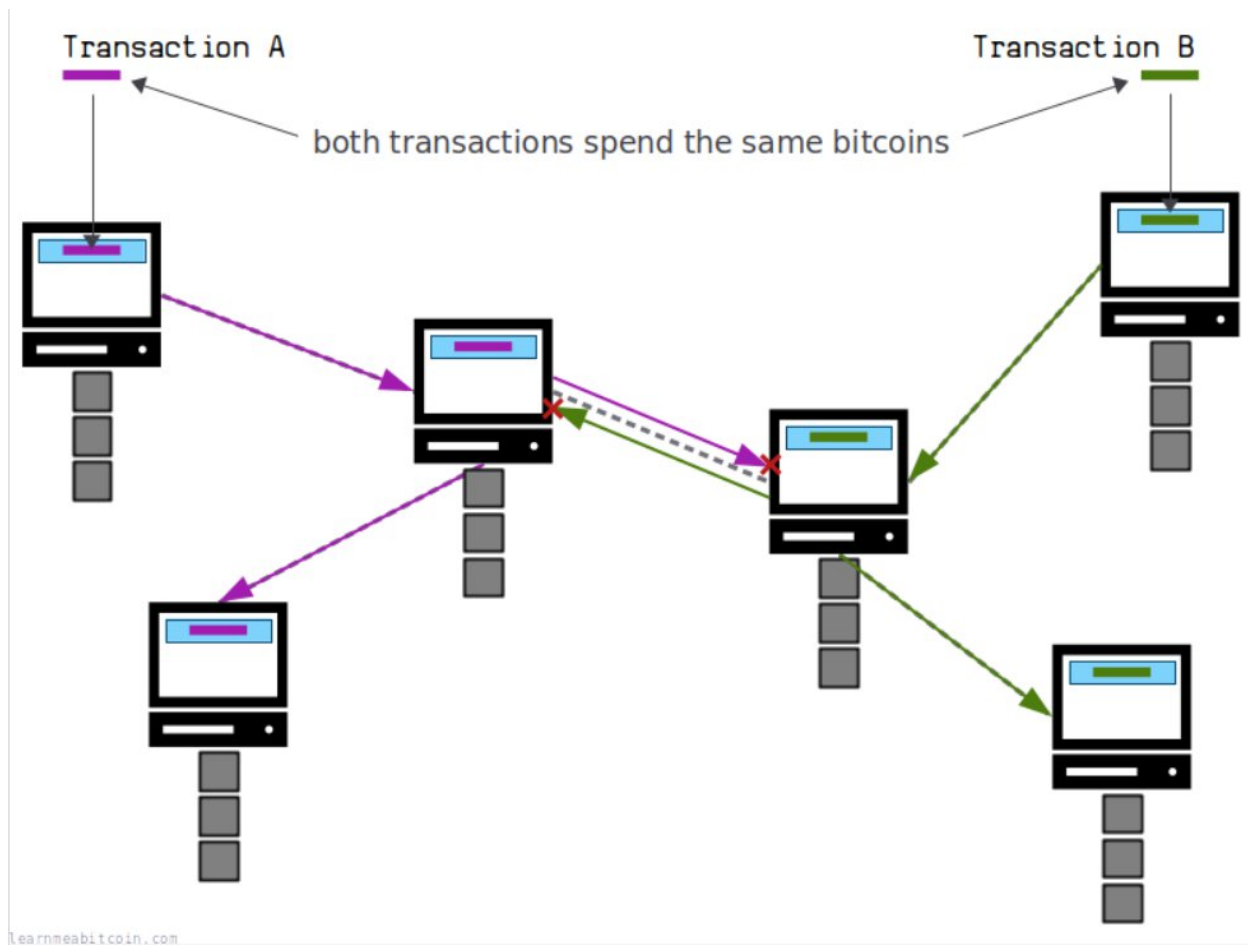


learnmeabitcoin.com

Lưu ý: Không phải tất cả các giao dịch đều đi từ bể nhớ (memory pool – nơi lưu trữ tạm thời) đến blockchain (lưu trữ vĩnh viễn)

#### 4.2.2 Mục đích

Bể nhớ (memory pool) được sử dụng để phân loại các giao dịch xung đột.



Vì không có sự xuất hiện của bên thứ 3 nên sẽ có trường hợp 1 đồng tiền mã hóa sẽ được chi tiêu nhiều lần cho các giao dịch khác nhau điều này tạo ra sự xung đột hay còn được gọi là chi tiêu kép (double spending). Như hình trên 2 giao dịch A và B chi tiêu cùng 1 lượng bitcoin cùng 1 lúc và các giao dịch này sẽ được đưa lên mạng, các node sẽ đưa nó vào bể nhớ (memory pool) và các giao dịch xung đột sẽ bị bể nhớ loại bỏ như **giao dịch A** và **giao dịch B** ở 2 node giữa từ đó xuất hiện trên mạng sẽ có các phiên bản các giao dịch xung đột cùng nhau tồn tại ở các node khác nhau.

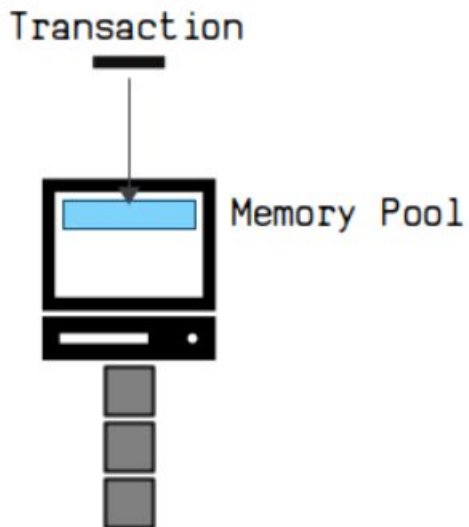
Cơ chế chọn giao dịch nào đưa vào bể nhớ thường là giao dịch nào có chi phí cao hơn.

Cách 1 trong cách giao dịch được chọn để ghi vào blockchain sử dụng bể nhớ (memory pool) là các node khai thác các giao dịch từ mem của họ và khi tìm được 1 hash hợp lệ sẽ quảng bá lên mạng, khi nhận được các khối mới này thì các node sẽ thêm nó vào blockchain và loại bỏ các giao dịch xung đột từ bể nhớ của họ.

Vì vậy bể nhớ (memory pool) có vai trò quan trọng ngăn chặn các giao dịch xung đột khỏi blockchain và cũng là lý do mọi người phải chờ đợi giao dịch được khai thác.

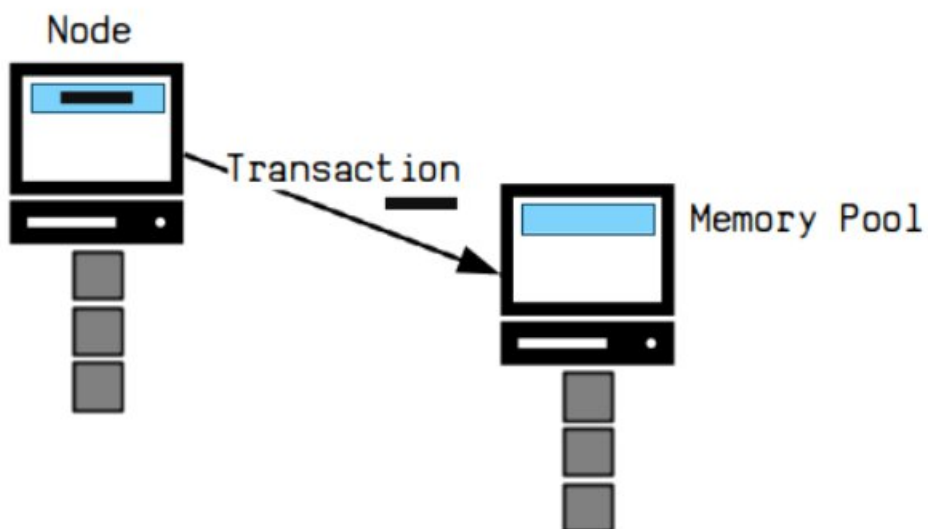
### 4.2.3 Các cách phổ biến 1 giao dịch được đưa vào bể nhớ (memory pool)?

Được chèn trực tiếp vào trong node cục bộ



Sau khi một giao dịch được node cục bộ xác thực hợp lệ, nó sẽ được thêm vào mempool và tiếp tục được quảng bá đến các node khác. Nếu một giao dịch không hợp lệ, node sẽ từ chối nó thay vì đưa vào mempool.

Nhận được từ Node khác



[learnmeabitcoin.com](http://learnmeabitcoin.com)

Một giao dịch mới có thể nhận được từ 1 node khác trên mạng. Các Node trên mạng sẽ liên tục quảng bá các giao dịch mới nhất mà họ nhận được từ các node kết nối với nó. Vì vậy nếu 1 node nhận được 1 giao

dịch mà nó chưa có thì nó sẽ thêm vào mempool . Quá trình này lặp đi lặp lại cho đến khi các node trên mạng có 1 bản sao của giao dịch mới nhất trong mempool của họ.

Lưu ý: Chỉ các giao dịch hợp lệ mới có thể thêm vào bể nhớ. Một node sẽ kiểm tra giao dịch có hợp lệ hay không trước khi thêm nó vào bể nhớ hoặc chuyển tiếp cho node nó kết nối.

### 4.2.3 Cách 1 giao dịch rời khỏi bể nhớ?

#### Được khai thác

Đây là mục tiêu của tất cả các bể nhớ giao dịch. Khi một thợ đào khai thác một khối giao dịch mới, họ sẽ phát nó đến các nút khác trên mạng. Khi một nút nhận được khối này, bất kỳ giao dịch nào trong bể nhớ của nó có trong khối đó sẽ bị xóa khỏi bể nhớ và được kết nối với khối thay thế.

Nói cách khác, các giao dịch được chuyển từ bộ nhớ tạm thời (bể nhớ) sang bộ nhớ vĩnh viễn (chuỗi khối).

#### Xung đột khai thác

Xung đột khai thác xảy ra khi một giao dịch trong mempool mâu thuẫn với một giao dịch đã được xác nhận trong một khối mới.

- Khi một nút nhận được một khối mới, nó sẽ kiểm tra xem có giao dịch nào trong mempool của nó trùng với đầu vào (inputs) của giao dịch trong khối hay không.
- Nếu có, các giao dịch đó sẽ bị loại bỏ khỏi mempool, vì chúng không còn hợp lệ (số tiền đã được sử dụng trong giao dịch trong khối).
- Điều này thường xảy ra với giao dịch chưa được xác nhận nhưng sau đó bị ghi đè bởi một giao dịch khác trong khối (ví dụ: giao dịch có phí cao hơn hoặc giao dịch thay thế).

#### Bị thay thế

Một giao dịch sẽ bị xóa khỏi bể nhớ nếu nó bị thay thế bởi một giao dịch mới có phí cao hơn.

Điều này xảy ra khi một giao dịch trong bể nhớ có cài đặt replace-by-fee (RBF), và sau đó một giao dịch mới được phát lên mạng sử dụng cùng số bitcoin nhưng với mức phí cao hơn phù hợp.

Phiên bản giao dịch mới có phí cao hơn sẽ có nhiều khả năng được đào vào chuỗi khối, vì vậy một nút sẽ loại bỏ giao dịch cũ để ưu tiên giao dịch mới.

#### Giới hạn thời gian

Mỗi node có 1 cài đặt giới hạn thời gian giữ giao dịch trong bể nhớ.

Vì vậy nếu 1 giao dịch trong bể nhớ không được khai thác trước khi hết thời gian thì node đó sẽ xóa nó ra khỏi bể nhớ.

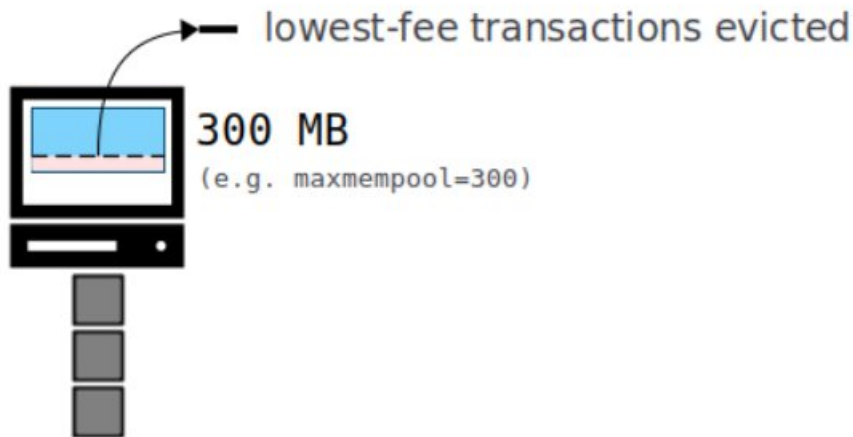
Ví dụ: bitcoin là 2 tuần

#### Giới hạn kích thước



Các giao dịch sẽ bị xóa khỏi bể nhớ của 1 node khi bể nhớ đó đạt tới 1 giới hạn nhất định. Mỗi node có khả năng đặt 1 kích thước tối đa cho bể nhớ của nó. Khi bể nhớ đạt tới 1 giới hạn thì nó sẽ xóa các giao dịch có chi phí thấp nhất để tạo không gian cho giao dịch có chi phí cao hơn. Vì vậy nếu có nhiều giao dịch trôi nổi trên mạng mà phù hợp với bể nhớ của node thì node đó sẽ giữ giao dịch có chi phí cao.

Ví dụ: giới hạn kích thước mặc định của bitcoin là 300MB



#### 4.2.4 Nơi Bể nhớ được lưu trữ?

Bể nhớ được lưu trữ trong RAM

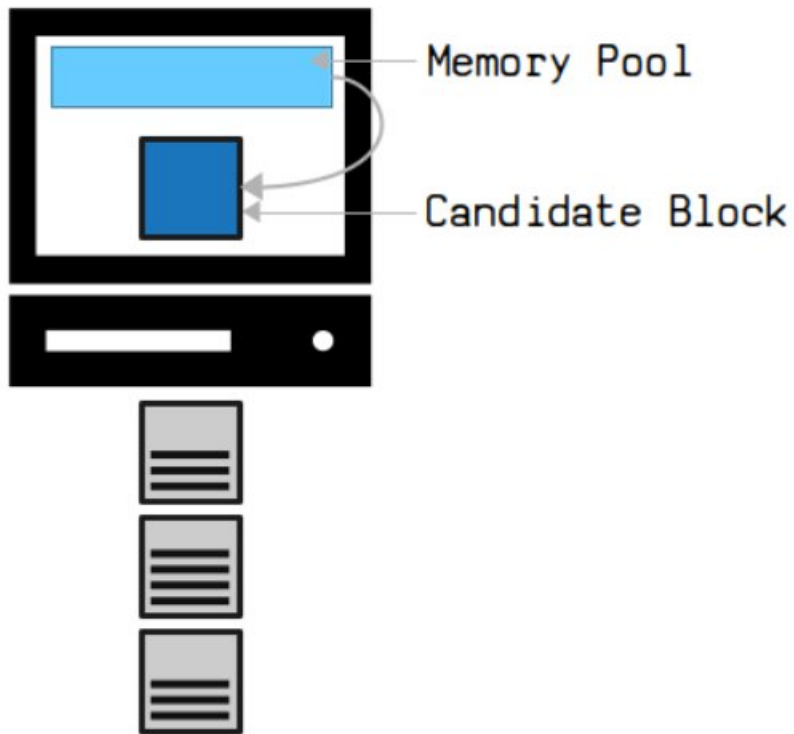
Điều này có nghĩa là giao dịch có thể được truy cập nhanh nhất có thể và cung cấp 1 số lợi ích sau:

- Xác thực giao dịch mới nhanh hơn: Mỗi giao dịch mới cần kiểm tra liệu nó có xung đột với bất kỳ giao dịch nào hiện có trong bể nhớ. Giữ giao dịch trong bể nhớ giúp xác thực và chuyển tiếp giao dịch mới nhanh hơn.
- Truyền khối mới nhanh hơn: Mỗi khối mới mà một nút nhận được cần phải được xác thực trước khi có thể ghi vào blockchain của nó và truyền tiếp đến các nút khác. Nếu hầu hết các giao dịch trong khối đã có sẵn trong bể nhớ của nút, quá trình xác thực khối sẽ diễn ra nhanh hơn (vì phần lớn giao dịch đã được xác thực trước đó)
- Tạo khối ứng viên nhanh hơn: thợ đào cần tập hợp các giao dịch từ bể nhớ khi tạo ra khối ứng viên. Nếu tất cả giao dịch trong bể nhớ được lưu trữ trong RAM, việc sắp xếp chúng để lựa chọn sẽ diễn ra nhanh hơn nhiều.

**// Mempool có trong cả PoW và PoS, nhưng quan trọng hơn trong PoW.**

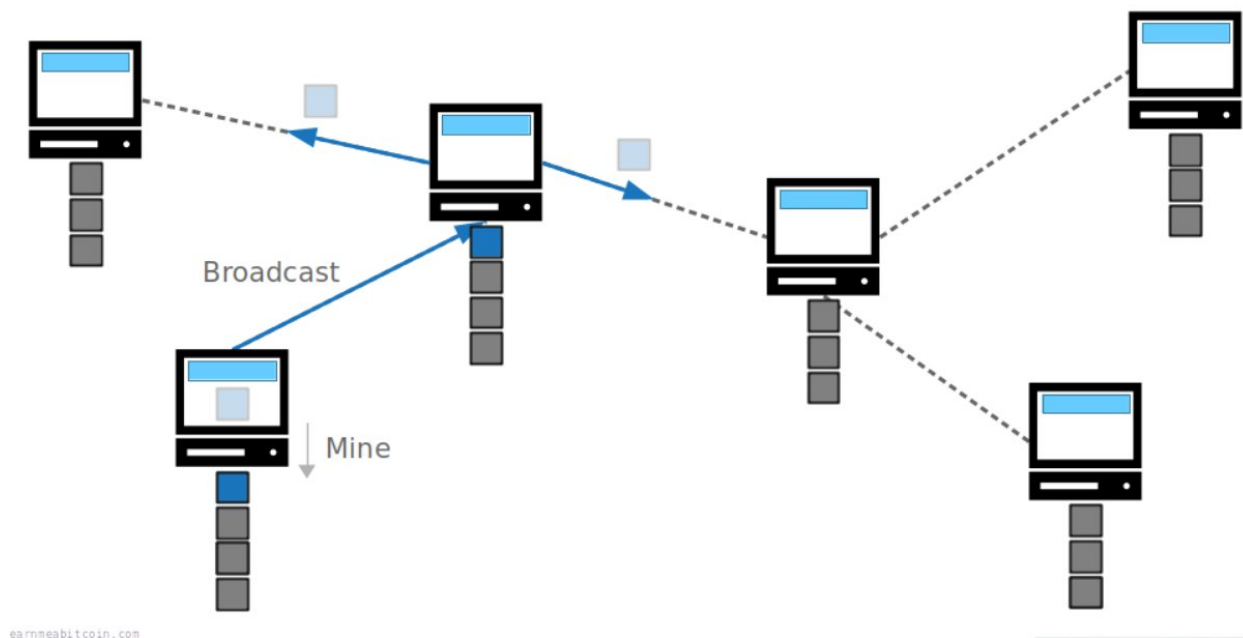
**// Candidate block chỉ tồn tại trong PoW. Trong PoS, thay vào đó có proposed block.**

### 4.3 Khối ứng viên trong PoS



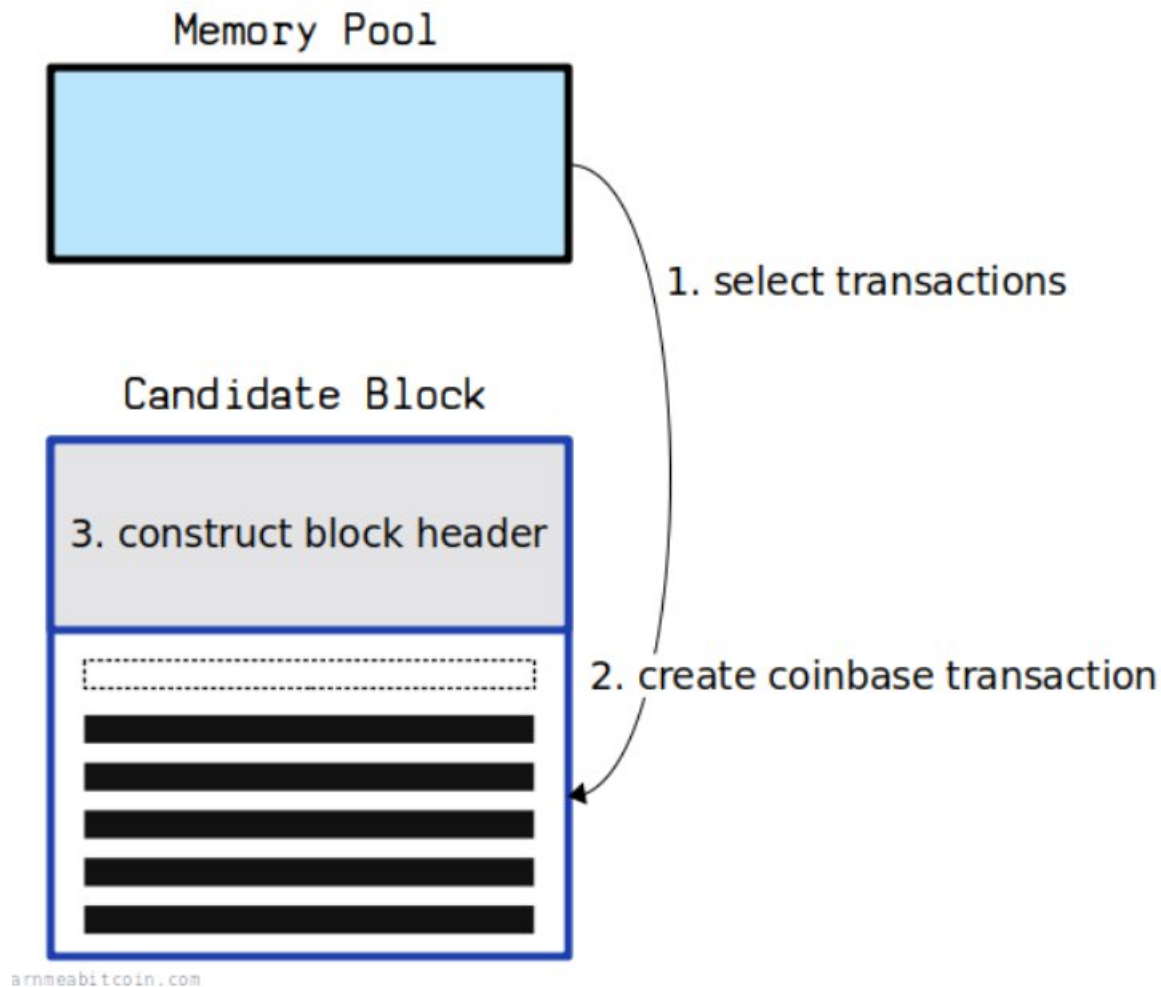
#### 4.3.1 Khối ứng viên là gì?

Khối ứng viên (candidate block) là 1 khối giao dịch mà thợ đào(miner) cố gắng để thêm vào Blockchain.



Trong quá trình khai thác, mỗi miner sẽ tập hợp các giao dịch từ bộ nhớ của họ vào trong khối ứng viên. Họ sẽ liên tục băm khối đó để nhận được giá trị băm hợp lệ (nhỏ hơn target hash). Nếu miner nhận được 1 giá trị băm hợp lệ thì khối ứng viên đó có thể thêm vào blockchain. Họ sẽ quảng bá khối ứng viên được khai thác đó đến node khác trong mạng và mỗi node sẽ xác minh và thêm nó sổ cái nếu nó hợp lệ.

### 4.3.2 Cách tạo ra 1 khối ứng viên



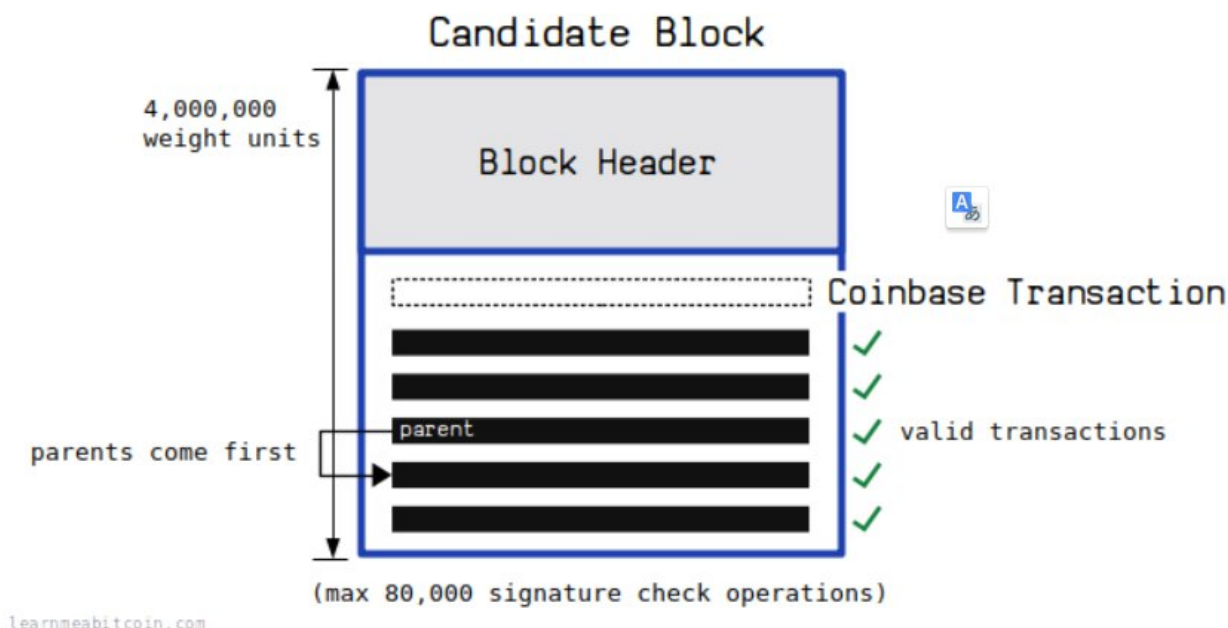
Có 3 bước cơ bản để tạo ra khối ứng viên.

1. **Lựa chọn giao dịch:** bước đầu tiên là lựa chọn giao dịch từ bể nhớ (mempool) cho khối ứng viên. Một thợ đào (miner) thông thường chọn những giao dịch có chi phí cao để tối đa hóa số tiền mà họ có thể nhận được từ phần thưởng khối.
2. **Xây dựng giao dịch Coinbase:** là giao dịch đầu tiên của 1 khối, được thợ đào sử dụng để yêu cầu phần thưởng khối.
3. **Tạo block header:** Block header là 1 lượng nhỏ metadata tóm tắt tất cả dữ liệu bên trong khối. Đây là nơi mà thợ đào (miner) sẽ bám khi họ cố gắng khai thác 1 khối ứng viên.

Hai trường quan trọng trong block header:

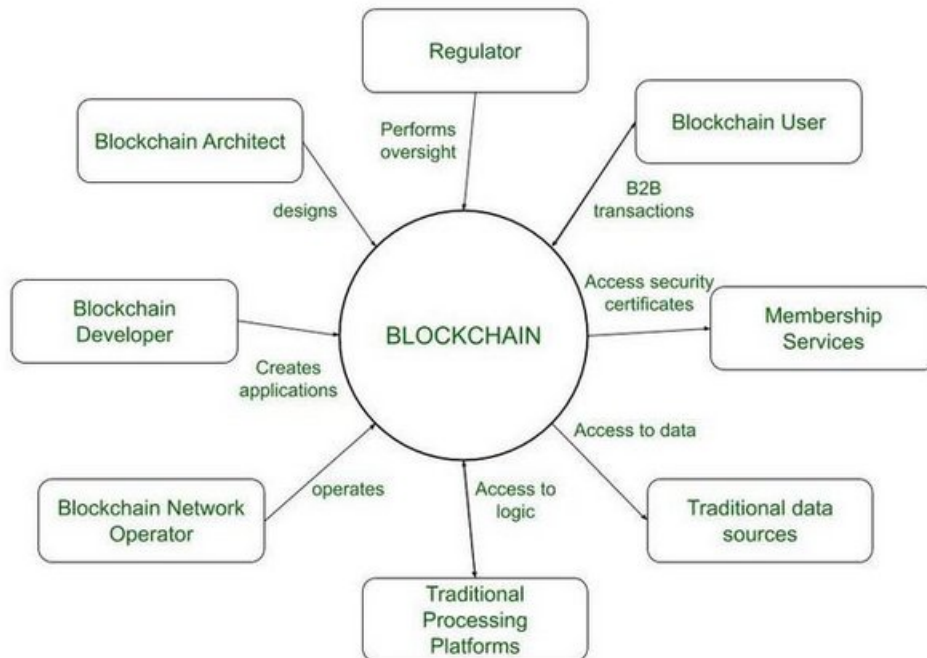
- **Khối trước đó:** trường này được sử dụng để xác định 1 khối đã tồn tại mà khối ứng viên được xây dựng trên nó. Thợ đào luôn muốn xây dựng trên đỉnh của chuỗi khối, vì họ chỉ có thể nhận phần thưởng khối nếu khối họ khai thác cuối cùng trở thành một phần của chuỗi dài nhất.
- **Merkle root:** là một dấu vân tay đại diện cho tất cả các giao dịch được đưa vào khối. Điều này quan trọng vì nó đảm bảo rằng bạn không thể thay đổi nội dung của khối mà không làm thay đổi dấu vân tay. Vì vậy, đây cũng là lý do tại sao chúng ta tạo tiêu đề khối sau khi đã chọn các giao dịch cho **khối ứng viên**.

### 4.2.3 Các yêu cầu đối với 1 khối ứng viên



1. Giao dịch Coinbase: Giao dịch đầu tiên của khối ứng viên phải là coinbase. Giao dịch này được đặt trong khối bởi vì thợ đào có thể dùng nó để yêu cầu phần thưởng khối. Điều đó có nghĩa là tất cả khối sẽ luôn luôn chứa ít nhất 1 giao dịch.
2. Giao dịch hợp lệ: tất cả giao dịch thợ đào đưa vào khối ứng viên phải hợp lệ.  
Ví dụ: mỗi giao dịch chỉ có thể chi tiêu số tiền đã tồn tại. Nếu 1 thợ đào khai thác 1 khối chứa các giao dịch không hợp lệ và quảng bá nó lên mạng, tất cả các node còn lại sẽ từ chối nó và nỗ lực khai thác khối đó là lãng phí.
3. Giao dịch cha:  
Giao dịch được xem là giao dịch cha của 1 giao dịch con thì đầu ra của giao dịch cha là đầu vào của giao dịch con.  
Cha của một giao dịch phải luôn xuất hiện trước giao dịch con.  
Ví dụ, nếu một giao dịch có tổ tiên đang nằm trong mempool, thì các tổ tiên đó phải được đưa vào trước nó trong khối ứng viên.  
Mỗi node xác thực các giao dịch trong một khối theo thứ tự từ trên xuống dưới, vì vậy nếu đưa giao dịch cha vào sau giao dịch con, thì giao dịch con đó sẽ trông như đang sử dụng đầu ra chưa tồn tại (và do đó sẽ không hợp lệ).
4. Giới hạn kích thước: kích thước giới hạn của block trong bitcoin là 4 000 000 WU với 1 WU =  $\frac{1}{4}$  byte
5. Giới hạn kiểm tra chữ ký: trong bitcoin một khối bị giới hạn tối đa 80.000 thao tác kiểm tra chữ ký. Do đó, các giao dịch mà bạn đưa vào khối ứng viên phải nằm trong giới hạn này.  
Điều này là do quá trình xác minh chữ ký tốn nhiều thời gian, vì vậy giới hạn này giúp ngăn chặn việc thợ đào tạo ra các khối có thời gian xác thực quá lâu.

## 4.4 Các nhân tố liên quan đến phát triển blockchain



### 1. Kiến trúc sư Blockchain (blockchain architect)

Kiến trúc sư Blockchain là người sẽ thiết kế cách thức xây dựng giải pháp blockchain. Họ sẽ xác định những thông tin cần được lưu trữ, các giao dịch và logic nghiệp vụ cần được nhúng vào mạng blockchain, và nhiều yếu tố khác.

### 2. Nhà phát triển blockchain (blockchain developer)

Nhà phát triển ứng dụng và hợp đồng thông minh tương tác với blockchain và được sử dụng bởi người dùng blockchain.

Nhà phát triển Blockchain là người sẽ hiện thực hóa thiết kế của kiến trúc sư bằng cách viết mã thực tế để chạy trên mạng blockchain.

### 3. Nhà vận hành mạng Blockchain (Blockchain network Operator)

Quản lý và giám sát mạng blockchain.

Mỗi phân nhánh công việc hoặc doanh nghiệp trong mạng đều có một nhà vận hành mạng blockchain. Họ cũng là người trực tiếp vận hành mạng blockchain.

Ví dụ:

Trong mạng Bitcoin (Blockchain công khai - Public Blockchain)

- Không có một thực thể duy nhất làm "nhà vận hành".
- Các thợ đào (miners) và node operators đóng vai trò duy trì mạng.
- Họ đảm bảo các giao dịch được xác thực đúng cách và đồng thuận diễn ra suôn sẻ.

Trong Blockchain riêng tư (Private Blockchain)

- Một công ty cung cấp dịch vụ tài chính sử dụng Hyperledger Fabric để xử lý giao dịch nội bộ.
- Nhà vận hành mạng là nhóm IT của công ty, chịu trách nhiệm:

- Cấp quyền truy cập cho các ngân hàng thành viên.
  - Giám sát hiệu suất mạng.
  - Thực hiện cập nhật phần mềm mà không ảnh hưởng đến giao dịch.
4. Nền tảng xử lý truyền thống (Traditional processing platform)  
 Một hệ thống máy tính hiện có có thể được blockchain sử dụng để hỗ trợ xử lý. Hệ thống này cũng có thể cần khởi tạo yêu cầu đến blockchain. Các hệ thống khác có thể gửi hoặc nhận thông tin cần thiết để xây dựng một giải pháp blockchain.
  5. Dịch vụ thành viên (Membership service)  
 Dịch vụ thành viên trong blockchain là hệ thống giúp xác thực và quản lý danh tính người dùng hoặc các thực thể tham gia vào mạng blockchain, đặc biệt là trong các mạng permissioned (có cấp phép). Những dịch vụ này đảm bảo rằng chỉ những người dùng hoặc thực thể được cấp phép mới có thể tham gia vào mạng, gửi giao dịch, và thực hiện các hành động khác.
  6. Nguồn dữ liệu truyền thống (Traditional Data Sources)  
 Một hệ thống máy tính hiện có có thể cung cấp dữ liệu để ảnh hưởng đến hành vi của hợp đồng thông minh. Chúng cũng là một phần trong giải pháp tổng thể để lưu trữ dữ liệu ngoài chuỗi.
  7. Người dùng Blockchain (blockchain user)  
 Blockchain user là người hoặc thực thể sử dụng blockchain để thực hiện giao dịch, tham gia vào các ứng dụng phân tán (DApps), hoặc tương tác với các hợp đồng thông minh. Họ có thể là người tiêu dùng cá nhân, tổ chức, hoặc bất kỳ ai sử dụng các dịch vụ và tính năng mà blockchain cung cấp. Các blockchain user cần có ví điện tử (wallet) để lưu trữ và giao dịch tiền mã hóa hoặc tham gia vào các mạng blockchain.
  8. Nhà quản lý blockchain (blockchain regulator)  
 là cơ quan giám sát và đảm bảo rằng các giao dịch và hoạt động trên mạng blockchain tuân thủ các quy định pháp lý và chính sách. Trong các blockchain permissioned, regulator có quyền đọc (read-only access) để giám sát các giao dịch và hành vi, đảm bảo chúng hợp pháp. Trong các blockchain permissionless, regulator vẫn có thể giám sát hoạt động và áp dụng các quy định về chống rửa tiền, bảo vệ người dùng, và giám sát các hành vi vi phạm pháp luật.

## 4.5 Vòng đời của giao dịch

Vòng đời của giao dịch trong blockchain đề cập đến các giai đoạn đi từ lúc nó được khởi tạo cho đến khi được lưu trữ vĩnh viễn trên blockchain.

### Các giai của giao dịch

1. Khởi tạo 1 giao dịch
  - Người dùng tạo ra 1 giao dịch bằng ví (wallet) hoặc ứng dụng.
  - Giao dịch được ký bởi khóa riêng (private key) của người gửi để đảm bảo tính xác thực
  - Giao dịch được quảng bá lên mạng blockchain.
2. Lan truyền giao dịch
  - Node nhận giao dịch và xác minh định dạng, tính hợp lệ của nó.

- Giao dịch được xác minh sẽ được thêm vào bể nhớ (mempool) và chờ đợi được khai thác bởi thợ đào (miner).
  - Mỗi node độc lập xác minh các giao dịch có đáp ứng các quy tắc (không chi tiêu kép – double spending, thực thi các quy tắc đồng bộ như chữ ký có đúng không, định dạng có đúng không, loại bỏ các giao dịch không hợp lệ) của mạng không.
3. Khai thác và xác nhận
- Quá trình khai thác: Thợ đào sẽ thêm các giao dịch lấy từ bể nhớ (mempool) vào trong khối mới bằng cách giải các bài toán mật mã (PoS)
  - Cơ chế đồng thuận: mạng sẽ đạt được sự đồng thuận về trạng thái của blockchain.
  - Thêm vào blockchain: khi khối đã được khai thác, khối được thêm vào blockchain và giao dịch trong đó được xem là đã được xác nhận
4. Giải quyết giao dịch
- Ghi vào Blockchain: Giao dịch được ghi vĩnh viễn, đảm bảo tính bất biến.
  - Tính bất biến của giao dịch: Khi đã được xác nhận, giao dịch không thể bị thay đổi hoặc xóa.
  - Phân phối phí giao dịch: Thợ đào nhận phí để xử lý giao dịch, khuyến khích họ tham gia.

#### Các hành động sau giao dịch

- Xác minh giao dịch: sau khi giao dịch được xác nhận, nó có thể được xác minh bởi bất kỳ ai sử dụng sổ cái công khai của blockchain. Người dùng có thể kiểm tra trạng thái và chi tiết của giao dịch thông qua **“block explorer”**
- Giám sát và kiểm toán: Các tổ chức có thể giám sát giao dịch để phân tích, kiểm toán và chống gian lận. Chính sự minh bạch của blockchain làm cho việc theo dõi lịch sử dễ dàng hơn.
- Trong trường hợp có sự khác biệt hoặc tranh chấp (ví dụ: cố gắng chi tiêu kép), các mạng blockchain có thể có các giao thức hoặc hợp đồng thông minh để xử lý các tình huống như vậy.  
Ví dụ: bể nhớ (mempool) loại bỏ các giao dịch xung đột do các giao dịch chi tiêu cùng 1 lượng tiền mã hóa xảy ra. Chỉ 1 giao dịch hợp lệ được đưa vào mempool.

#### Các thử thách trong vòng đời của giao dịch

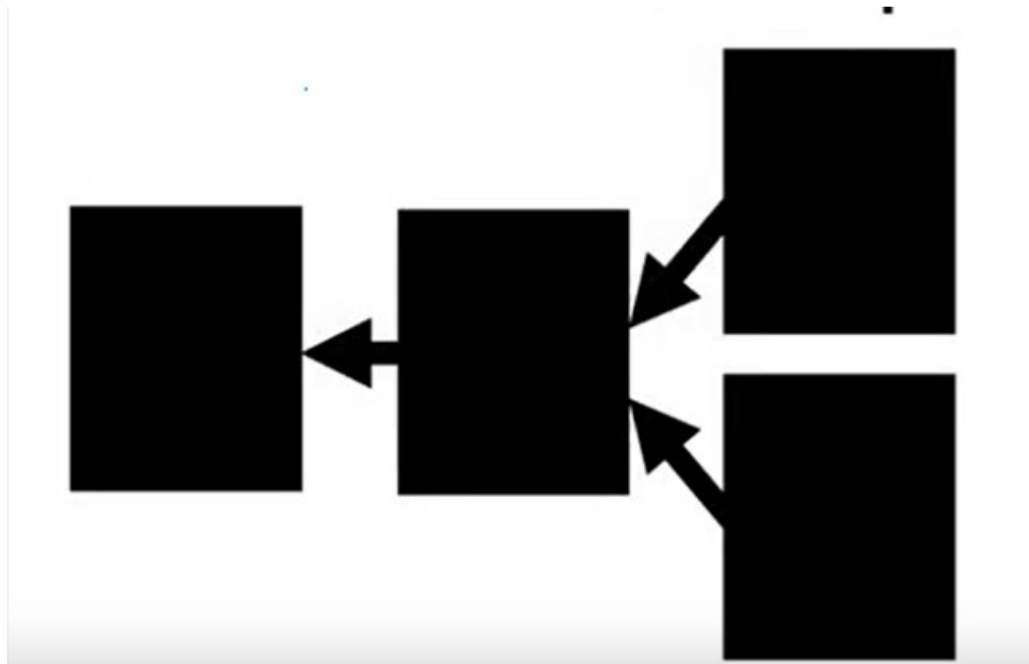
1. Tắc nghẽn mạng: Khi khối lượng giao dịch tăng lên có thể gây tắc nghẽn mạng, kết quả là thời gian xử lý lâu hơn và phí giao dịch cao hơn
2. Thông lượng bị giới hạn: Nhiều blockchain chỉ có thể xử lý được 1 số lượng giới hạn giao dịch mỗi giây, cản trở khả năng xử lý của những ứng dụng lớn
3. Chậm trễ trong xác nhận giao dịch: Giao dịch chậm trong thời điểm hoạt động của mạng cao gây khó chịu cho người dùng muốn giao dịch ngay lập tức.
4. Thời gian không nhất quán: Mỗi blockchain có thời gian xác nhận khác nhau, điều này có thể dẫn đến sự không chắc chắn về tính cuối cùng của giao dịch.
5. Tấn công 51%: trong PoS nếu có 1 thực thể kiểm soát mạng có thể thao túng giao dịch



6. Hệ sinh thái phân mảnh: Các mạng blockchain thường hoạt động độc lập, gây khó khăn trong việc chuyển tài sản hoặc dữ liệu giữa chúng một cách liền mạch
7. Thiếu tiêu chuẩn hóa: Sự thiếu thốn của các tiêu chuẩn chung trong việc tương tác cản trở sự hợp tác giữa các blockchain khác nhau.
8. Quy trình dễ xảy ra lỗi: Sai sót khi gửi giao dịch, chẳng hạn như nhập sai địa chỉ hoặc số tiền, có thể dẫn đến mất mát không thể khôi phục

## 5.Blockchain forks

Trong quá trình khai thác (mining) blockchain, có thể xảy ra trường hợp hai hoặc nhiều thợ đào khai thác thành công các khối mới gần như cùng một lúc. Khi đó, cả hai khối đều hợp lệ và cùng trở về một khối cha trước đó, dẫn đến sự phân nhánh tạm thời (fork) trong blockchain.



Phân nhánh (fork) có thể gây ra những vấn đề sau:

- Khi 1 fork xảy ra, blockchain có thể tạo 2 chuỗi riêng biệt mỗi chuỗi có lịch sử giao dịch riêng.

Ví dụ: Ethereum và Ethereum classic sau vụ hack DAO năm 2016

-Khả năng xảy ra chi tiêu kép(double spending)

Nếu 1 blockchain phân nhánh nhưng chưa có sự đồng thuận rõ ràng, 1 giao dịch có thể xuất hiện trên 2 chuỗi. Có thể kẻ tấn công lợi dụng điều này để thực hiện cùng một giao dịch hai lần (chi tiêu cùng một số tiền trên cả hai chuỗi), sẽ xảy ra chi tiêu kép.

- Hai phiên bản tiền mã hóa khác nhau
- Ví dụ. Bitcoin(BTC) và Bitcoin Cash(BCH)

Cách giải quyết Fork tạm thời: theo nguyên tắc blockchain (đặc biệt là trong Bitcoin) sau 1 khoảng thời gian các nhánh sẽ có nhiều thợ đào khai thác thêm khối và làm cho chuỗi đó dài hơn, chuỗi dài nhất (chuỗi thực hiện nhiều công việc nhất như công sức tính toán trong Proof of Work) sẽ được coi là hợp lệ. Nhánh còn lại bị loại bỏ, các block trong nhánh đó được gọi là orphaned blocks và các giao dịch bên trong chúng sẽ được khai thác tiếp nếu giao dịch đó chưa được xác nhận.

## Xác thực trong blockchain

Nguyên tắc xác thực khối (Block Validation Rules) là các tiêu chí mà full node sử dụng để kiểm tra xem một khối có hợp lệ hay không trước khi chấp nhận nó vào blockchain

Một số tiêu chí quan trọng trong xác thực khối

1. Cấu trúc khối hợp lệ
2. Block header hợp lệ
3. Các giao dịch trong khối phải hợp lệ
4. Các thuật toán đồng thuận

Ví dụ:

Proof of Work: hash của khối phải thỏa mãn 1 độ khó nhất định

Proof of Stake: phải được ký bởi Validator hợp lệ

Ví dụ về các quy tắc xác thực trong Bitcoin

- Khối < 1MB
- Giao dịch hợp lệ
- Proof of Work: khối phải thỏa mãn độ khó nhất định (nhỏ hơn target hash)
- Không có chi tiêu kép (double spends)
- Dấu thời gian của khối: đảm bảo thời gian hợp lệ
- Trỏ vào băm (hash) của khối trước đó

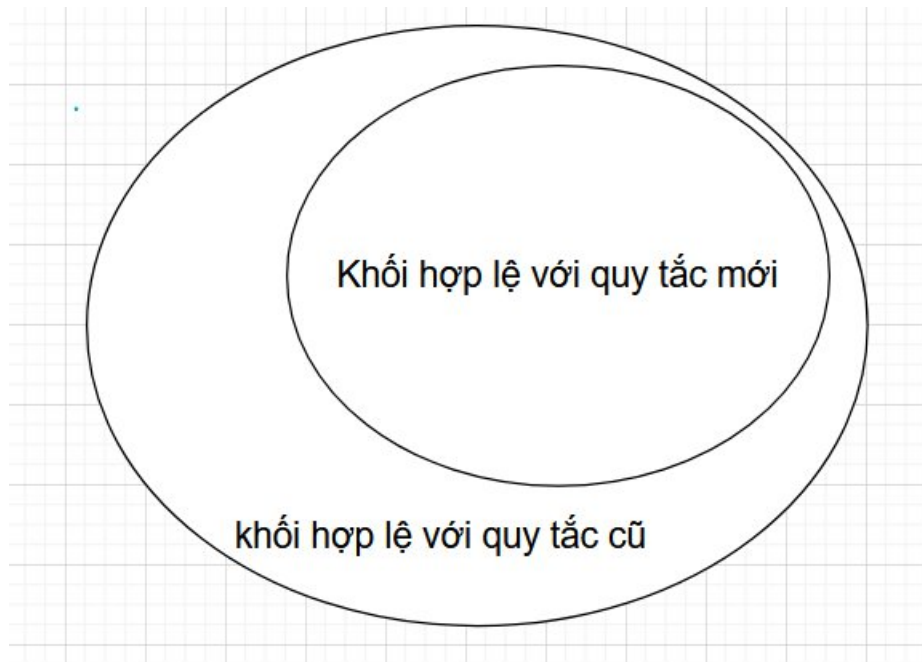
## Sự thay đổi quy tắc xác thực và các loại fork trong blockchain

Những thay đổi trong nguyên tắc xác thực có thể bao gồm:

- Fix bugs
- Vấn đề liên quan đến bảo mật
- Thêm hoặc chỉnh sửa những tính năng mới

Trong blockchain, khi các quy tắc xác thực (Validation Rules) thay đổi, có thể dẫn đến các loại fork khác nhau. Dưới đây là hai loại fork chính:

## 1. Soft Fork (Phân nhánh mềm)



Soft fork là một bản nâng cấp tương thích ngược với blockchain.

Nghĩa là các nút (node) cũ chưa cập nhật vẫn có thể nhận diện các khối (block) mới, nhưng có thể bị áp đặt một số quy tắc mới.

Soft fork hoạt động bằng cách thắt chặt các quy tắc đồng thuận hiện có, làm cho một số giao dịch trước đây hợp lệ trở nên không hợp lệ.

Ví dụ:

- thay đổi giới hạn từ 1MB xuống còn 0.5 MB (quy tắc được thắt chặt hơn)
- Cập nhật Segregated Witness (SegWit) của Bitcoin năm 2017 giúp tối ưu cách lưu trữ dữ liệu giao dịch, tăng hiệu suất

### Đặc điểm:

- Tương thích ngược: Các nút cũ vẫn có thể tương tác với blockchain được cập nhật, đảm bảo không xảy ra tách chuỗi vĩnh viễn.
- Thắt chặt các quy tắc hiện có: Soft fork thường giới thiệu các quy tắc hạn chế hơn hoặc tinh chỉnh, như giảm kích thước khối hoặc thay đổi định dạng giao dịch.
- Không Tách Chuỗi: Vì các nút cũ và mới có thể cùng tồn tại, soft fork không tạo ra các blockchain riêng biệt.
- Yêu Cầu Đồng Thuận Thấp Hơn: Soft fork chỉ cần một phần nhỏ hơn của mạng nâng cấp, giúp việc triển khai dễ dàng hơn.
- Nâng Cấp Mượt Mà: Cho phép cập nhật ít gián đoạn hơn so với hard fork, với ít vấn đề tương thích hơn.

### Thuận lợi:

- Tương thích ngược: Đảm bảo rằng các nút chạy phiên bản cũ hơn vẫn có thể tham gia vào mạng mà không cần nâng cấp.
- Giảm rủi ro phân tách chuỗi: Không có sự phân tách chuỗi vĩnh viễn, giúp cộng đồng đoàn kết và tránh các chuỗi khối cạnh tranh.
- Ít gây gián đoạn hơn: Dễ dàng triển khai và chuyển đổi mà không cần sự phối hợp lớn hoặc cập nhật tài nguyên.
- Quy tắc chặt chẽ hơn: Tăng cường bảo mật bằng cách làm cho các quy tắc nghiêm ngặt hơn mà không phá vỡ chức năng hiện có.

#### Nhược điểm:

- Phạm vi hạn chế: Soft fork bị ràng buộc bởi yêu cầu duy trì khả năng tương thích với các phiên bản cũ, giới hạn quy mô thay đổi.
- Khả năng không nhất quán: Nếu một phần lớn mạng lưới không nâng cấp, các quy tắc mới có thể không được thực thi đồng đều.
- Nhầm lẫn tạm thời: Khi các nút nâng cấp vào những thời điểm khác nhau, có thể xảy ra sự không nhất quán hoặc nhầm lẫn tạm thời trong việc xác thực giao dịch.
- Thách thức trong thực thi: Soft fork phụ thuộc vào đa số thợ đào chấp nhận cập nhật, có thể dẫn đến việc thực thi quy tắc mới không đồng đều.
- Đổi mới chậm hơn: Vì soft fork phải duy trì khả năng tương thích ngược, nó thường hạn chế các đổi mới mang tính đột phá hoặc thay đổi lớn trong giao thức.

## 2. hard fork



Hard fork là một thay đổi không tương thích ngược, nghĩa là tất cả các nút phải nâng cấp để tuân theo các quy tắc mới.

Nếu một số nút không nâng cấp, blockchain sẽ chia tách thành hai chuỗi riêng biệt.

Hard fork tạo ra hai mạng độc lập, mỗi mạng có lịch sử giao dịch và sổ dư tiền riêng.

Yêu cầu đồng thuận: yêu cầu đồng thuận đa số

Quá trình nâng cấp: Yêu cầu các nodes trong mạng nâng cấp để duy trì tính tương thích

Nguy cơ phân chia mạng: Cao có thể dẫn đến việc phân chia cộng đồng

Ví dụ:

- Ethereum vs. Ethereum Classic (ETH vs. ETC) sau vụ hack DAO.
- Bitcoin vs. Bitcoin Cash (BTC vs. BCH) do bất đồng về kích thước khối.

### **Đặc điểm:**

- Tách chuỗi vĩnh viễn: Một hard fork tạo ra hai blockchain hoạt động độc lập và tuân theo các quy tắc khác nhau
- Yêu cầu sự đồng thuận của mạng: Để thực hiện phiên bản mới, phần lớn người tham gia mạng phải đồng ý fork
- Node cũ trở nên không tương thích: Các nút không nâng cấp lên giao thức mới sẽ không thể nhận diện hoặc xác thực giao dịch hay khối mới.
- Cho phép thay đổi căn bản: Hard fork cho phép thực hiện các thay đổi lớn, như chỉnh sửa kích thước khối, thay đổi cơ chế đồng thuận hoặc áp dụng mô hình quản trị mới
- Chuỗi Nhân Bản: Người dùng có thể sở hữu token trên cả hai chuỗi (cũ và mới), tùy thuộc vào số dư của họ tại thời điểm fork

### **Thuận lợi:**

- Tự do cho những thay đổi lớn: Cho phép các nhà phát triển thực hiện những thay đổi đáng kể, chẳng hạn như cải thiện khả năng mở rộng, thêm tính năng mới hoặc sửa đổi cơ chế quản trị.
- Trao quyền lựa chọn cho cộng đồng: Nếu có bất đồng, cộng đồng có thể tách ra và theo chuỗi khối mà họ ưa thích, giúp đổi mới trên cả hai chuỗi.
- Cải thiện khả năng mở rộng: Những cải tiến lớn như tăng kích thước khối hoặc tốc độ giao dịch có thể nâng cao hiệu suất tổng thể của mạng.
- Bảo mật được nâng cao: Hard fork có thể giới thiệu các bản vá bảo mật quan trọng mà các cập nhật nhỏ khó có thể đạt được
- Con đường phát triển mới: Việc tạo ra một chuỗi mới cho phép thử nghiệm và phát triển thêm mà không ảnh hưởng đến sự ổn định của chuỗi cũ.

### **Nhược điểm:**

- Rủi ro phân tách cộng đồng: Hard fork có thể làm chia rẽ cộng đồng, dẫn đến các blockchain cạnh tranh và giảm hiệu ứng mạng.
- Vấn đề bảo mật: Người dùng có thể vô tình gửi token đến sai chuỗi, dẫn đến giao dịch trùng lặp hoặc mất tài sản.

- **Tốn nhiều tài nguyên:** Các nút cũ trở nên lỗi thời và có thể cần nâng cấp hoặc bị bỏ rơi, gây tốn kém và mất thời gian.
- **Nhằm lừa cho người dùng:** Người dùng phải quyết định chuỗi nào để ủng hộ, và có thể có sự nhầm lẫn về giá trị cũng như tính bảo mật của tài sản trên mỗi chuỗi.
- **Gián đoạn đồng thuận:** Quá trình fork yêu cầu sự phối hợp lớn trong mạng, có thể làm gián đoạn hoạt động bình thường tạm thời.

## **Tại Sao Forks Xảy Ra?**

### **1.Nâng Cấp Kỹ Thuật và Cải Tiến**

- Một số forks được tạo ra để nâng cấp bảo mật, khả năng mở rộng và hiệu suất.
- Các nhà phát triển có thể giới thiệu các tính năng mới để cải thiện hệ thống hoặc sửa lỗi bảo mật.

### **2.Bất Đồng Giữa Nhà Phát Triển và Thợ Đào**

- Các bên liên quan (nhà phát triển, thợ đào, doanh nghiệp và người dùng) có thể có ý kiến khác nhau về tương lai của blockchain.
- Nếu không đạt được sự đồng thuận, một phần của mạng có thể tách ra và tiếp tục theo quy tắc riêng.

### **3.Mâu Thuẫn Về Quản Trị và Cộng Đồng**

- Một số forks xuất phát từ tranh chấp về quản trị blockchain và quyền quyết định.
- Ví dụ: Bitcoin vs. Bitcoin Cash do bất đồng về khả năng mở rộng (tăng kích thước khối hay không).

### **4. Sự Cố Bảo Mật Và Tấn Công Hacker**

- Trong một số trường hợp, fork là cần thiết để khắc phục sự cố bảo mật hoặc phục hồi từ một cuộc tấn công.

