# Lời dẫn (Lưu ý trước khi bắt đầu)

Thực ra, peer-to-peer, hay còn gọi là P2P đã có từ rất sớm và nếu nhìn kỹ hơn, chúng ta sẽ thấy nó rất gần gũi với đời sống hằng ngày. Trong lĩnh vực tiền điện tử, chúng ta thường xuyên nghe đến công nghệ mạng này.

P2P đóng một vai trò quan trọng trong sự phát triển của Internet. Hệ thống mạng này từng được sử dụng phổ biến nhất, đặc biệt là khi các trang web media trực tuyến như Youtube, Netflix, Spotify,… còn chưa phát triển. Ngày nay, hệ thống client-sever có phần phổ biến hơn, nhưng điều đó không có nghĩa là P2P đã biến mất. P2Pt tiếp tục được phát triển, là nền tảng then chốt của nhiều công nghệ quan trọng và hoạt động song song cùng hệ thống client-sever trong nhiều ứng dụng ở các lĩnh vực khác nhau.

Phần mềm vi phạm bản quyền và chia sẻ file đã tồn tại trước khi Internet phát triển như ngày nay, chủ yếu thông qua message board (diễn đàn trực tuyến/forum) và các trang FTP riêng. Nhưng thật là tẻ nhạt khi việc tìm kiếm file thậm chí còn lâu hơn việc tải xuống chúng. Cách phổ biến hơn để có được phần mềm là lấy một bản sao vật lý trực tiếp từ một người bạn.

Chia sẻ file P2P đã thay đổi tất cả điều đó. Nhờ phương pháp này, chúng ta có quyền truy cập trực tiếp vào dữ liệu được chia sẻ của người khác. Tất nhiên, công nghệ chia sẻ file ngang hàng không được sử dụng cho mục đích vi phạm bản quyền. Nhưng nếu thành thật mà nói, đó là lý do ban đầu mà phương pháp này được tạo ra.

Khía cạnh chia sẻ file của công nghệ P2P được đề cập khá nhiều, nhưng chắc chắn đây không phải là trường hợp sử dụng duy nhất.

Vậy peer-to-peer P2P là gì, so sánh mô hình Peer to Peer với Client Server và ưu nhược điểm của mạng ngang hàng peer-to-peer là gì.

# Tóm tắt lịch sử của các phần mềm P2P trước đây

Mạng Internet được thiết kế ban đầu như một hệ thống peer-to-peer (P2P). Trải qua thời gian, do nhu cầu sử dụng internet phát triển mạnh mẽ đã khiến cho mô hình P2P dần chuyển đổi và phát triển thành mô hình client/server. Vào đầu những năm 1960, Internet ra đời và phát triển một cách nhanh chóng. Số lượng máy client truy nhập internet gia tăng một cách chóng mặt khiến cho không gian địa chỉ IP không còn đủ để đáp ứng nhu cầu truy cập mạng của người sử dụng. Bên cạnh đó, sự phát triển của internet kéo theo nó là các yêu cầu về vấn đề bảo mật. Đó là những ngăn cản khiến cho mô hình P2P khó có thể xây dựng và phát huy được sức mạnh thực sự của nó. Mô hình client/server ra đời như một giải pháp cho các vấn đề đó.

Dường như mô hình client/server đã thể hiện như một lựa chọn đúng nhưng sự gia tăng về nhu cầu sử dụng internet một cách mạnh mẽ đã khiến các nhà phát triển phải xem xét lại vấn đề đó. Số lượng gói tin truyền đi trong mạng quá nhiều gây ra quá tải băng thông, số lượng thông tin và không gian lưu trữ tài nguyên cũng là vấn đề gặp phải của các nhà quản lý, cung cấp dịch vụ mạng. Vì vậy, chi phí cho một hệ thống server là rất cao. Và bài toán cho các vấn đề đó đã đưa những nhà phát triển mạng quay lại với mô hình mạng P2P nguyên thủy.

In May 1999, with millions more people on the Internet, Shawn Fanning introduced the music and file-sharing application called Napster.[7] Napster was the beginning of peer-to-peer networks, as we know them today, where "participating users establish a virtual network, entirely independent from the physical network, without having to obey any administrative authorities or restrictions."[7]

Đây là một cơ sở dữ liệu trung tâm chứa thông tin về tất cả các file nhạc do các thành viên nắm giữ. Bạn có thể tìm kiếm một bài hát từ máy chủ trung tâm này, nhưng để tải xuống, bạn sẽ phải thực sự kết nối với một người dùng trực tuyến khác và sao chép file từ họ. Đổi lại, một khi bạn đã có bài hát đó trong thư viện Napster của mình, nó sẽ trở thành một nguồn có sẵn cho những người khác trên mạng.

Bạn cũng có thể thêm các file của riêng mình, sau đó Napster sẽ lập chỉ mục và thêm vào cơ sở dữ liệu, sau đó sẵn sàng phân phối các file đó trên toàn thế giới. Tuy nhiên, việc triển khai bị giới hạn ở chỗ bạn chỉ có thể tải xuống từ một người. Dịch vụ có ưu điểm là tính sẵn sàng cao của các bài hát, nhưng bù lại tốc độ không quá lớn.

**<Chen hinh NAPSTER >**

Nhờ vào điều này, khái niệm về peer-to-peer đã được cả thế giới biết đến.

Napster cuối cùng đã ngừng hoạt động vào năm 2001, sau khi các mạng tương tự được tạo ra để cung cấp nhiều thứ khác, không chỉ là âm nhạc. Phim ảnh, phần mềm và hình ảnh đã có sẵn trên các mạng Morpheus, Kazaa và Gnutella (trong số đó, Limewire có lẽ là ứng dụng khách Gnutella nổi tiếng nhất).

Qua nhiều năm, nhiều giao thức và phần mềm chia sẻ file ngang hàng khác nhau đã xuất hiện và biến mất, nhưng một giao thức mở trong số đó đã được giữ lại: BitTorrent.

# Mạng ngang hàng P2P là gì?

**P2P không phải mô hình máy khách - máy chủ**

Một trang web được lưu trữ trên một máy chủ mạnh mẽ ở đâu đó trên thế giới, và cung cấp các thông tin khi máy tính hoặc điện thoại của bạn yêu cầu. Đây có thể là một phông chữ được sử dụng để hiển thị trang web chính xác, hoặc là một Linux ISO 2GB bạn muốn tải xuống. Máy chủ sẽ gửi file cho bạn. Khi người dùng tiếp theo yêu cầu, quá trình sẽ lặp lại.

Điều này thích hợp cho hoạt động của các trang web, nhưng không phù hợp lắm với việc phân phối các file có kích thước lớn. Chủ yếu là do các vấn đề về tốc độ, băng thông, chi phí và tính hợp pháp.

Tốc độ trên một máy chủ web truyền thống khá hạn chế. Sẽ tốt hơn nếu chỉ truyền một lượng nhỏ văn bản để hiển thị một trang web và một số máy chủ web được tối ưu hóa chỉ để phục vụ phần hình ảnh mà thôi. Nhưng đối với các file có kích thước lớn hơn, điều đó sẽ yêu cầu một tốc độ nhanh hơn rất nhiều trong thời gian dài và việc phải chia sẻ máy chủ với những người dùng khác. Băng thông cũng khá tốn kém. Chỉ phục vụ những hình ảnh cho một trang web thôi cũng tốn đến hàng ngàn đô la một năm.

Từ quan điểm pháp lý, việc định vị một máy chủ đơn giản là tương đối dễ dàng: Tắt máy chủ rồi truy tố chủ sở hữu. Do đó, P2P sinh ra giống như một biện pháp cứu cánh. Còn những người muốn phân phối các file có bản quyền cần một cách tốt hơn để thực hiện việc này.

**Peer-to-Peer là gì?**

Mạng ngang hàng hay còn gọi là peer-to-peer viết tắt là P2P có nghĩa là mạng đồng đẳng, một mạng máy tính mà hoạt động của nó dựa vào khả năng tính toán và băng thông của tất cả các máy tham gia chứ không tập trung vào các máy chủ trung tâm như thông thường.

Mạng máy tính P2P được xây dựng dựa trên băng thông và hiệu năng của các máy tính cá nhân trong mạng chứ không dựa trên là sự tập trung của một số lượng nhỏ các máy server. Các mạng P2P được sử dụng để kết nối các node theo các kết nối ad\_hoc (không dự tính) và rất hữu dụng cho một số mục đích như : chia sẻ file nội dung, tìm kiếm tài nguyên,...

Một mạng P2P thuần túy không có khái niệm khách/chủ (clients/servers) mà các node (peer) ngang bằng nhau thì có các chức năng như cả client và server đối với các node khác trong mạng. Mô hình này không giống với mô hình client - server, các kết nối không thường xuyên phải thông qua một server trung tâm. Một ví dụ tiêu biểu cho chia sẻ file không phải P2P là một server FTP, các chương trình client và server không giống nhau, trong đó các máy client thiết lập các yêu cầu download/upload và các máy server gửi trả lời cho các yêu cầu đó.

Không có ranh giới rõ ràng giữa một mô hình P2P và một mô hình client server. Cả hai mô hình đó có thể được tích hợp trong cùng một mạng với mục đích sử dụng khác nhau . Một vài mạng như: Napster, OpenNAP và IRC@find sử dụng cấu trúc client-server cho một vài mục đích như tìm kiếm và sử dụng cấu trúc P2P cho các mục đích khác. Các mạng khác như Gnutella hay Freenet sử dụng cấu trúc P2P cho mọi mục đích và đó là những mạng hoàn toàn P2P .

Khi một mạng P2P được thiết lập qua Internet, một máy chủ trung tâm có thể được sử dụng để lập chỉ mục các tập tin, hoặc một mạng lưới phân phối có thể được thiết lập nơi chia sẻ các tập tin được chia ra giữa tất cả người dùng trong mạng đang lưu trữ một tập tin nhất định. Thay vì chỉ đơn giản là lấy các file, peer-to-peer biến quá trình này thành “con đường hai chiều”.

Bây giờ bạn có thể đáp trả lại những người dùng khác. Trong thực tế, việc đáp trả lại này (ngày nay được gọi là "seeding") đóng vai trò rất quan trọng cho sự thành công của các mạng ngang hàng. Nếu tất cả mọi người chỉ cần tải về mà không có động thái đáp trả bất cứ điều gì cả (gọi là "leeching"), thì điều này sẽ chẳng có lợi ích gì hơn so với mô hình máy chủ - máy khách cả.

Trong mô hình máy chủ - máy khách, hiệu suất giảm xuống nếu có nhiều người dùng, vì băng thông sẽ được chia sẻ cho nhiều người dùng hơn. Trong các mạng ngang hàng, càng có nhiều người dùng thì càng làm cho mạng hiệu quả hơn. Càng nhiều người dùng tạo một file cụ thể có sẵn từ ổ cứng của họ thì người dùng mới có thể nhận file đó càng dễ dàng hơn.

Trong các mạng P2P hiện đại, tốc độ sẽ thực sự nhanh hơn khi nhiều người dùng tải xuống file. Thay vì lấy toàn bộ file từ một người dùng, bạn đang lấy các phần nhỏ hơn từ hàng trăm hoặc hàng nghìn người khác. Ngay cả khi họ chỉ có một chút băng thông trống cho bạn, việc kết hợp nhiều kết nối có nghĩa là bạn sẽ nhận được tốc độ nhanh nhất có thể. Sau đó, đến lượt bạn đóng góp để phân phối các file một lần nữa.

Trong các hình thức trước đây của mạng P2P, vẫn cần có máy chủ trung tâm để tổ chức mạng, hoạt động như một cơ sở dữ liệu chứa thông tin về người dùng và file được kết nối có sẵn trong hệ thống. Mặc dù nhiệm vụ truyền file nặng nề đã được thực hiện trực tiếp giữa những người dùng với nhau nhưng các mạng vẫn dễ bị ảnh hưởng. Đánh bại máy chủ trung tâm có nghĩa là vô hiệu hóa hoàn toàn thông tin liên lạc.

Điều này không còn tồn tại nhờ những phát triển gần đây. Ngày nay, phần mềm có thể truy vấn ngang hàng trực tiếp nếu chúng thấy một file cụ thể. Không có cách nào để đánh bại các mạng này, chúng thực sự không thể bị phá vỡ.

Emerging collaborative P2P systems are going beyond the era of peers doing similar things while sharing resources, and are looking for diverse peers that can bring in unique resources and capabilities to a virtual community thereby empowering it to engage in greater tasks beyond those that can be accomplished by individual peers, yet that are beneficial to all the peers.

# Cách thức hoạt động của mạng ngang hàng

Yêu cầu duy nhất để một máy tính tham gia vào mạng ngang hàng là kết nối Internet và phần mềm P2P. Các chương trình phần mềm P2P phổ biến bao gồm Kazaa, Limewire, BearShare, Morpheus và Acquisition. Các chương trình này kết nối với mạng P2P, như “Gnutella”, và cho phép máy tính truy cập hàng nghìn hệ thống khác trên mạng.

Sau khi kết nối với mạng, phần mềm P2P cho phép bạn tìm kiếm các tệp trên máy tính của người khác. Những người dùng khác trên mạng cũng có thể tìm kiếm tệp trên máy tính của bạn nhưng thường chỉ giới hạn trong một thư mục mà bạn đã chia sẻ.

Trong khi mạng P2P làm cho việc chia sẻ tập tin dễ dàng và thuận tiện, nó cũng dẫn đến sự sao chép phần mềm và tải nhạc bất hợp pháp. Do đó, để an toàn, bạn chỉ nên tải phần mềm và nhạc từ các trang web hợp pháp.

Đầu tiên, trước khi bước vào chi tiết cách thức hoạt động của mạng P2P, chúng ta sẽ cùng xem qua một cái nhìn khái quát nhất thông qua việc so sánh về các điểm khác nhau cơ bản giữa Mạng ngang hàng và Mạng máy khách – máy chủ:

|  |  |  |
| --- | --- | --- |
| **Cơ sở so sánh** | **Máy khách-Máy chủ** | **Ngang ngang hàng** |
| Tính chất | Tập trung – máy chủ | Phân tán – phi tập trung |
| Căn bản | Có một máy chủ cụ thể và các máy khách cụ thể được kết nối với máy chủ. | Khách hàng và máy chủ không được phân biệt; mỗi nút đều đóng vai trò là máy khách và máy chủ. |
| Dịch vụ | Yêu cầu của khách hàng về dịch vụ và máy chủ sẽ đáp ứng với dịch vụ.mà khách yêu cầu. | Mỗi nút có thể yêu cầu dịch vụ và cũng có thể cung cấp dịch vụ. |
| Tiêu điểm | Chia sẻ thông tin. | Kết nối giữa các nút mạng |
| Dữ liệu | Dữ liệu được lưu trữ trong một máy chủ tập trung. | Mỗi đồng đẳng có dữ liệu riêng của mình. |
| Máy chủ | Khi một số khách hàng yêu cầu dịch vụ đồng thời, một máy chủ có thể bị tắc nghẽn. | Vì các dịch vụ được cung cấp bởi một số máy chủ được phân phối trong hệ thống ngang hàng, nên một máy chủ không bị tắc nghẽn. |
| Chi phí | Các máy khách-máy chủ đắt tiền để thực hiện.(cần bang thông lớn) | Ngang hàng ít tốn kém để thực hiện. |
| Ổn định | Client-Server ổn định hơn và có thể mở rộng. | Peer-toPeer bị ảnh hưởng nếu số lượng đồng nghiệp tăng trong hệ thống. |

Mạng đồng đẳng bao gồm tất cả các nút mạng đại diện cho các máy tham gia và các liên kết giữa các nút mạng này. Một liên kết tồn tại giữa hai nút mạng khi một nút mạng xác định được vị trí của nút mạng kia. Dựa vào cấu trúc liên kết giữa các nút mạng trong mạng đồng đẳng ta có thể phân loại thành: có cấu trúc, không có cấu trúc và mạng lai.

## **Phân loại mạng ngang hàng**

* Mạng ngang hàng không có cấu trúc

Các nút trên mạng P2P không có cấu trúc không được tổ chức theo bất kỳ cấu trúc cụ thể nào. Những người tham gia giao tiếp ngẫu nhiên với nhau. Các hệ thống này được coi là có khả năng mạnh mẽ chống lại các các hoạt động rời bỏ của người dùng (là việc một số nút thường xuyên tham gia và rời khỏi mạng).

Mặc dù dễ xây dựng hơn, các mạng P2P không có cấu trúc có thể cần sử dụng bộ nhớ và CPU cao hơn vì các truy vấn tìm kiếm được gửi đến số lượng các đồng đẳng cao nhất có thể. Điều này có xu hướng khiến mạng tràn ngập các truy vấn, đặc biệt nếu chỉ có một số lượng nhỏ các nút cung cấp nội dung mong muốn.

* Mạng ngang hàng có cấu trúc

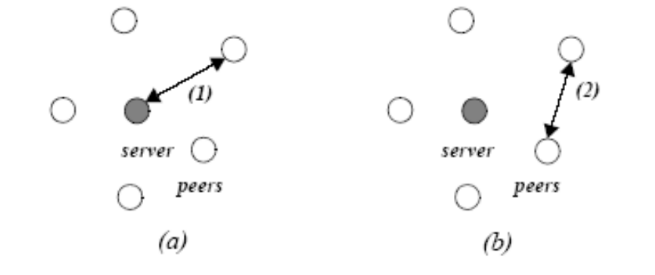
Các nút trên mạng P2P có một kiến trúc có tổ chức, cho phép các nút tìm kiếm các tệp một cách hiệu quả, ngay cả khi nội dung không có sẵn rộng rãi. Trong hầu hết các trường hợp, điều này đạt được thông qua việc sử dụng các hàm băm cho phép tra cứu cơ sở dữ liệu.

Mặc dù các mạng có cấu trúc có thể hiệu quả hơn, nhưng chúng thường thể hiện mức độ tập trung cao hơn và thường đòi hỏi chi phí thiết lập và bảo trì cao hơn. Ngoài ra, các mạng có cấu trúc kém mạnh mẽ hơn khi phải đối mặt với tỉ lệ người dùng rời bỏ mạng cao.

* Mạng ngang hàng P2P lai

Để có thể khắc phục nhược điểm của 2 cấu trúc mạng ngang hàng nêu trên, Mạng ngang hàng (Peer to Peer) lai được ra đời: kết hợp kiến trúc máy khách-máy chủ truyền thống với một số khía cạnh của kiến trúc ngang hàng. Ví dụ, mạng này có thể thiết kế một máy chủ trung tâm để tạo kết nối giữa các máy tính đồng đẳng trong mạng. So với hai kiến trúc còn lại, các mô hình lai thường thể hiện hiệu suất vận hành cao hơn. Chúng kết hợp được các ưu điểm chính của từng phương pháp, mang lại mức độ hiệu quả và phi tập trung đáng kể.

Trong mô hình này, có một máy chủ trung tâm đóng vai trò duy trì các cơ sở dữ liệu liên kết và do đó giúp các nút tìm thấy nhau dễ dàng hơn. Một ví dụ về mô hình lai có thể kể đến dịch vụ Spotify trước đây. Các mạng lai đánh đổi cấu trúc phi tập trung, bình đẳng của các nút được cung cấp trong mạng ngang hàng thuần túy với tính hiệu quả và tốc độ của nó. Sự phân cấp giúp các truy vấn và quá trình tìm kiếm dữ liệu được diễn ra hiệu quả hơn.

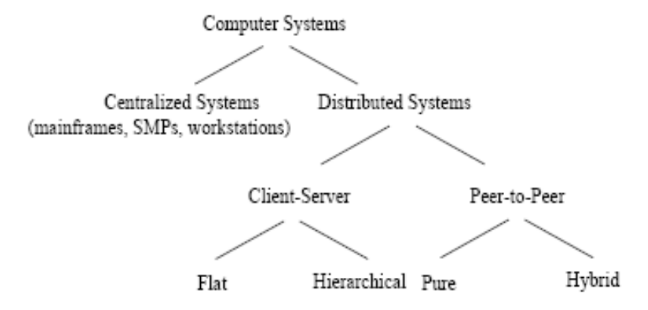


Hình 1.3.2 là một ví dụ về mô hình lai P2P. Để kết nối vào mạng P2P, đầu tiên các peer khởi tạo một liên lạc với server (1) để lưu giữ vị trí hoặc đặc điểm nhân dạng của peer, sau đó các peer liên lạc trực tiếp với nhau (2). Một vài ví dụ điển hình cho mô hình lai P2P bao gồm: Napster, Groover, Aimster, Magi, Softwax và iMesh…

Có một vài hệ thồng mạng kết hợp cả 2 mô hình thuần P2P và lai P2P để phát triển các dự án cá nhân như: Skype, KaZaa. Giải pháp đưa ra là bên cạnh việc sử dụng một server trung tâm để xác nhân các thông tin đăng nhập của peer ra còn sử dụng các peer có public IP làm các SuperPeer (SuperNode). Các SuperPeer này có thể sẽ lưu trữ một vài thông tin hoặc không, các peer khác sẽ tìm kiếm thông tin tại các SuperPeer. Tùy thuộc vào mục đích phát triển của dự án mà có thể sử dụng một trong 2 mô hình của P2P hoặc kết hợp cả 2 như một vài sự án đã nêu ở trên.

|  |  |
| --- | --- |
| **Mạng Đồng đẳng có cấu trúc** | **Mạng đồng đẳng không có cấu trúc** |
| Liên kết giữa các nút mạng | Có tổ chức, theo một thuật toán nhất định (DHT- Hàm băm phân tán) | Ngẫu nhiên, không theo quy luật nào |
| Xây dựng nút mạng | Xây dựng mỗi nút mạng sẽ chịu trách nhiệm đối với một phần dữ liệu được chia sẽ | Xây dựng từ một liên kết có sẵn trong mạng. Sau đó, thêm vào các liên kết mới của mình |
| Cách thức tìm kiếm dữ liệu | Yêu cầu tìm kiếm được áp dụng một giao thức chung nhằm xác định nút mạng chịu trách nhiệm cho dữ liệu cần tìm | Yêu cầu tìm kiếm được truyền khắp cả mạng, gửi đến tối đa nút mạng có thể. |
| Ưu điểm | Tìm kiếm các tệp một cách hiệu quả và nhanh chóng, ngay cả khi tệp đó không có sẵn rộng rãi trong mạng. | Dễ xây dựng nút mạng;  Có khả năng mạnh mẽ chống lại các hoạt động rời bõ mạng của người dùng. |
| Nhược điểm | Mức tập trung cao;  Chi phí thiết lập + bảo trì cao. | Cần dùng bộ nhớ và CPU cao hơn;  Xác suất tìm thấy các dữ liệu không phổ biến, ít được chia sẻ trên mạng sẽ là khá nhỏ. |

## **Phân loại kiến trúc mạng máy tính**

****

Tất cả các hệ thống máy tính có thể được phân thành 2 loại: Phân tán và Tập trung. Hệ thống phân tán có thể được phân ra thành 2 mô hình: client-server và P2P. Trong mô hình client-server tất cả các máy client chỉ liên lạc với một máy server đơn, hoăc có thể được phân cấp để phát triển khả năng co giãn. Trong mô hình phân cấp, server của một cấp sẽ đóng vai trò như một client của cấp cao hơn.

Trong các mạng P2P tập trung, tồn tại một chỉ mục trung tâm được duy trì ở một vị trí duy nhất cố định chứa các thông tin về vị trí của các đối tượng, và địa chỉ của các nút trong mạng… Các thành viên tham gia tìm vị trí của các tài nguyên mong muốn trong mạng bằng cách truy vấn đến máy chủ chỉ mục trung tâm. Cấu trúc Peer to Peer này không đáp ứng được quy mô mở rộng và máy chủ chỉ mục trung tâm có thể bị tấn công hoặc hỏng hóc, gián đoạn, gây ra gián đoạn hoạt động của toàn mạng.

Ngược lại với kiến trúc tập trung, các P2P có thể sử dụng cấu trúc thư mục phân tán. Trong đó tồn tại nhiều hơn một trung tâm chỉ mục tập trung. Các hệ thống này có thể phi tập trung hoàn toàn như Gnutella trong đó các nút hoạt động hoàn toàn bình đẳng, tức là đều chứa tài nguyên và cấu trúc để truy vấn trên mạng. Hoặc các hệ thống cũng có thể có kiến trúc kết hợp, trong đó một số nút trong mạng đóng vai trò duy trì các cơ sở dữ liệu chỉ mục được gọi là các nút thông báo hay các “siêu nút” nhằm phục vụ các yêu cầu tìm kiếm và truy vấn tài nguyên của các nút thông thường khác.

Các kiến trúc mạng này đều được sử dụng trong blockchain, tuỳ theo từng thiết kế về chức năng của blockchain đó. Chẳng hạn các public blockchain đa phần đều có tính chất phi tập trung và không có nút thông báo. Tuy nhiên, một số hệ thống blockchain vẫn có những nút tập trung để điều tiết dữ liệu chẳng hạn như IoTA,…

Dựa trên các cấu trúc mạng này và sự phân quyền trong blockchain, chúng ta có thể chia blockchain thành 3 loại: Blockchain công khai (Public blockchain), Blockchain riêng tư (Private blockchain) và Blockchain hợp tác (Consortium blockchain), trong đó:

* + Public blockchain: là loại Blockchain mà bất kỳ ai cũng có thể tham gia và có quyền đọc và ghi dữ liệu. Điển hình cho loại Blockchain này là các đồng tiền điện tử như Bitcoin, Ethereum… Các nút có thể tham gia hoặc rời bỏ mạng và mọi nút trên mạng là độc lập hoàn toàn, không hề có nút trung tâm kiểm soát hoặc chứa các bảng định tuyến địa chỉ (ngoài các seed node sẽ tìm hiểu ở phần tiếp theo). Việc xác thực giao dịch trên public blockchain diễn ra theo các cơ chế đồng thuận dựa trên chứng minh (chẳng hạn như Proof of Work hay Proof of Stake) và đòi hỏi sự tham gia của nhiều nút trên mạng. Hệ thống Blockchain này được đánh giá khá an toàn do chi phí cần thiết để thực hiện một vụ tấn công vào hệ thống là khá cao và cao hơn rất nhiều so với lợi ích thu được khi tấn công thành công.
  + Private blockchain: Đây là các mạng lưới blockchain mà trạng thái của nó được quyết định bởi một hoặc một số hữu hạn các thành viên tham gia. Các thành viên này được xác thực danh tính và thường biết và tin cậy lẫn nhau tuyệt đối. Các thành viên này có khả năng ghi dữ liệu và quyết định trạng thái hoạt động của blockchain. Ngoài ra, những người dùng khác chỉ được quyền đọc dữ liệu, không có quyền ghi. Private blockchain được xây dựng từ các nhóm thành viên tin cậy lẫn nhau do đó, nó thường sử dụng các cơ chế đồng thuận dựa trên kháng lỗi Byzantine với thời gian xác thực giao dịch khá nhanh (vì chỉ cần một lượng nhỏ thiết bị tham gia vào việc xác thực). Ripple là một dạng Private Blockchain, hệ thống này chỉ cần 80% các nút hoạt động ổn định là có thể tiến hành giao dịch.
  + Permissioned: Hay còn gọi là Consortium, một dạng của Private blockchain nhưng bổ sung thêm một số tính năng nhất định, kết hợp giữa “niềm tin” khi tham gia vào Public blockchain và “niềm tin tuyệt đối” khi tham gia vào Private blockchain. Khi đó các thành viên tham gia sẽ được một nhóm các thành viên khác xác minh và cấp quyền gia nhập mạng lưới. Ví dụ: Các ngân hàng hay tổ chức tài chính liên doanh sẽ sử dụng Blockchain cho riêng mình.

Như vậy cho dù là có cấu trúc hay không cấu trúc, Mạng đồng đẳng đều có những ưu và nhược điểm riêng; nhưng điểm chung ở cả 2 kiến trúc đều giúp trao đổi thông tin giữa các nút mạng mà không cần thông qua máy chủ hay cơ quan trung gian nào. Do đó, mạng này đã trở thành một kiến trúc xương sống trong giao dịch mua bán của thị trường tiền điện tử nói riêng và Blockchain nói chung.

## **Định tuyến trong mạng Peer to Peer**

Kiến trúc mạng peer to peer được thiết kế dựa trên các nút ngang hàng. Các nút này có khả năng đồng thời hoạt động như cả “máy khách” và “máy chủ”. Điều này tạo ra khó khăn hơn trong các mô hình truyền thống. Với các mô hình truyền thống, máy chủ thường có địa chỉ cố định do đó, một máy khách bất kỳ có thể dễ dàng truy vấn đến máy chủ thông qua địa chỉ IP của nó hoặc thông qua một máy chủ DNS định danh trung gian. Nhưng điều này không tồn tại trong kiến trúc mạng ngang hàng. Các nút tham gia mạng P2P này có thể tham gia hoặc rời khỏi hệ thống bất cứ lúc nào, do đó, các mạng P2P tính chất động và không ổn định cao.Trong mạng Peer to Peer có 2 vấn đề quan trọng cốt lõi đó là: làm thế nào để các nút có thể tìm thấy được nhau và làm thế nào có thể phát tán và đồng bộ hoá dữ liệu ra toàn mạng.

Để làm được điều này, các mạng peer to peer sử dụng hai cơ chế: tìm kiếm và đánh địa chỉ. Các nút và các tài nguyên trong mạng được đánh dấu bằng các địa chỉ cụ thể và thông tin về địa chỉ đó được lưu trữ tại các nút khác nhau trong mạng. Khi các nút muốn liên lạc và giao tiếp qua mạng, chúng sẽ tìm kiếm dữ liệu về các địa chỉ này và tiến hành gửi nhận thông tin với nhau. Các cơ chế đánh địa chỉ và tìm kiếm xác định cấu trúc hoạt động của mạng, cũng như tính hiệu quả của việc sử dụng các tài nguyên trong mạng.

Hầu hết các kỹ thuật tìm kiếm là dựa trên việc chuyển tiếp gói tin. Các nút khi có nhu cầu giao tiếp sẽ tạo ra các gói tin để truy vấn đến các nút khác, truy vấn này sẽ được chuyển tiếp (hoặc định tuyến) cho đến khi nó đến được nút có dữ liệu mong muốn (hoặc con trỏ tới dữ liệu mong muốn). Để chuyển tiếp được các thông điệp, mỗi nút phải giữ thông tin về một số nút “hàng xóm” khác. Thông tin của các hàng xóm này tạo thành bảng định tuyến của một nút.

Khi một nút mới khởi động, nó phải tìm kiếm các nút khác trên mạng để kết nối. Để bắt đầu quá trình này, một nút mới phải khám phá ít nhất một nút hiện có trên mạng và kết nối với nó.

Đến đây, có một câu hỏi: rõ ràng trong mạng P2P chúng ta sẽ không có cấu trúc mạng, và mỗi máy tính trên mạng đều có một địa chỉ riêng, do đó chúng ta sẽ rất khó khăn để quét qua toàn bộ mạng nhằm tìm ra được các nút hàng xóm được và do đó cũng rất khó để tìm ra được các nút khác trên mạng. Vậy thực sự trong mạng peer to peer chúng ta sẽ giải quyết vấn đề này như thế nào?

Có rất nhiều cách khác nhau để các nút có thể liên kết với mạng lưới, điều này phụ thuộc vào từng giao thức khác nhau. Nhưng về cơ bản chúng ta có thể kể đến các phương pháp như sau:

**Sử dụng một địa chỉ bên ngoài đã biết**

Các nút tham gia vào mạng có thể vào các diễn đàn, các dịch vụ web công cộng để lấy thông tin về một số địa chỉ IP của mạng lưới bên ngoài. Địa chỉ này có thể được sử dụng để thêm vào bảng định tuyến một cách thủ công.

Đối với mỗi địa chỉ này, máy khách sẽ cố gắng kết nối, gửi các yêu cầu HTTP, đọc dòng phản hồi thích hợp và phân tích địa chỉ IP từ địa chỉ đó. Nếu quá trình này thành công, địa chỉ IP được trả về, nó sẽ được quảng bá đến các nút khác mà nó được kết nối đến.

**Kết nối đến địa chỉ truy vấn đến nó (Callback Address)**

Khi một nút nhận được một kết nối đến nó từ một nút nào đó trong mạng lưới. Hai nút sẽ khởi tạo kết nối, và nút nhận được kết nối này sẽ quảng bá địa chỉ của nó đến nút yêu cầu để tạo kết nối cục bộ nếu muốn.

Sau khi gửi lại địa chỉ của mình, nút này sẽ gửi các yêu cầu đến nút Callback Address để lấy thêm danh sách các địa chỉ khác trong mạng lưới mà nút kia đang có nhằm bổ sung thêm cho bảng định tuyến của mình.

**Địa chỉ IRC**

Ngoài việc học và chia sẻ địa chỉ của chính nó, các nút còn tìm kiếm địa chỉ của các nút khác thông qua kênh IRC. Đây là một trong những cách được sử dụng trong các phiên bản Bitcoin cũ.

Sau khi một nút mã hóa địa chỉ của chính nó thành một chuỗi được sử dụng làm biệt hiệu. Nó sẽ tham gia ngẫu nhiên một kênh IRC (trong Bitcoin thì kênh này có tên giữa # bitcoin00 và # bitcoin99). Sau đó, nó sẽ ban hành một lệnh WHO, đọc các dòng khi chúng xuất hiện và giải mã địa chỉ IP của các nút khác trong kênh. Điều này được lặp đi lặp lại mãi mãi cho đến khi nút được tắt.

**Địa chỉ các nút mặc định**

Khi một nút mới tham gia vào mạng lưới, nó chưa hề biết bất cứ thông tin gì về các thành viên khác. Vậy trong trường hợp này, làm thế nào để nó có thể tìm thấy và kết nối đến các nút khác?

Về nguyên tắc, trên các mạng lưới blockchain sẽ không có các nút đặc biệt, vai trò của các nút là ngang hàng với nhau. Tuy nhiên, trên thực tế vẫn tồn tại một số nút ổn định đã hoạt động trong một thời gian dài, hoặc các nút được duy trì với một số mục đích nhất định theo thiết kế. Các nút này được gọi là các nút mầm (seed node). Các seed node được duy trì và liệt kê trong một danh sách nằm trong chính phần mềm ứng dụng blockchain hoặc trên một số cơ sở dữ liệu cố định được cung cấp. Và các nút khác khi mới tham gia vào mạng lưới có thể truy vấn và lấy danh sách địa chỉ sử dụng cho việc định tuyến của mình trong các seed node này. Mặc dù, việc kết nối này là không bắt buộc, các nút hoàn thành có thể tự chỉ định địa chỉ kết nối của các nút hàng xóm của mình như ở trên, tuy nhiến việc kết nối đến các seed node có thể giúp đơn giản hóa quá trình khởi tạo kết nối và bảng định tuyến trên các nút và giúp các nút trong mạng có thể tìm kiếm lẫn nhau một cách nhanh chóng.

Ngoài ra có những seed node được duy trì trên một số máy chủ DNS trên mạng. Để kết nối đến các seed node này và tìm kiếm các máy khác trên mạng, máy khách sẽ đưa ra các truy vấn DNS đến một danh sách các tên máy chủ dịch vụ DNS được chọn. Chẳng hạn với Bitcoin, danh sách các địa chỉ này hiện nay bao gồm:

seed.bitcoin.sipa.be

dnsseed.bluematt.me

dnsseed.bitcoin.dashjr.org

seed.bitcoinstats.com

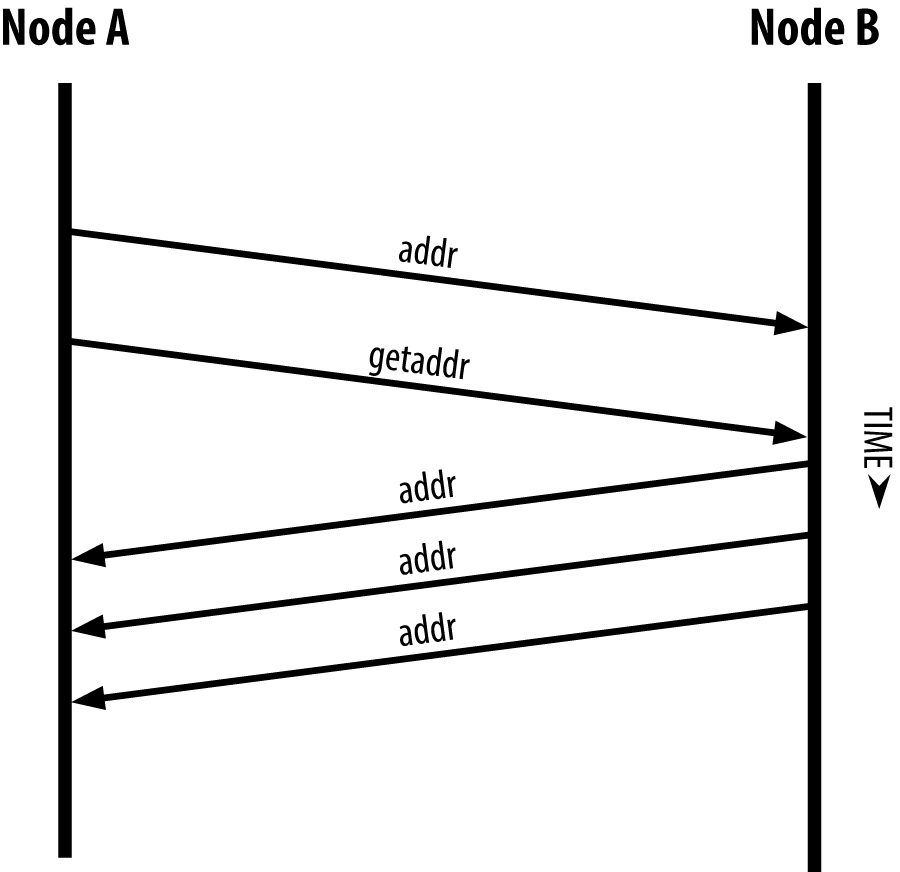
seed.bitcoin.jonasschnelli.ch

seed.btc.petertodd.org

Các phản hồi DNS có thể chứa nhiều địa chỉ IP được yêu cầu. Và các địa chỉ này có thể được thêm vào trong danh sách định tuyến của nút.

Sau khi đã tìm ra các nút liên kết, máy khách sẽ tiến hành kết nối với nó thông qua việc thiết lập các kết nối TCP. Khi thiết lập kết nối, các nút sẽ bắt đầu khởi động một giao thức bắt tay trực tiếp bằng cách truyền nhận các thông điệp để thiết lập kết nối và tìm kiếm các thông tin cần thiết. Trong Bitcoin cổng mặc định được sử dụng là 8333 hoặc một số cổng thay thế khác.

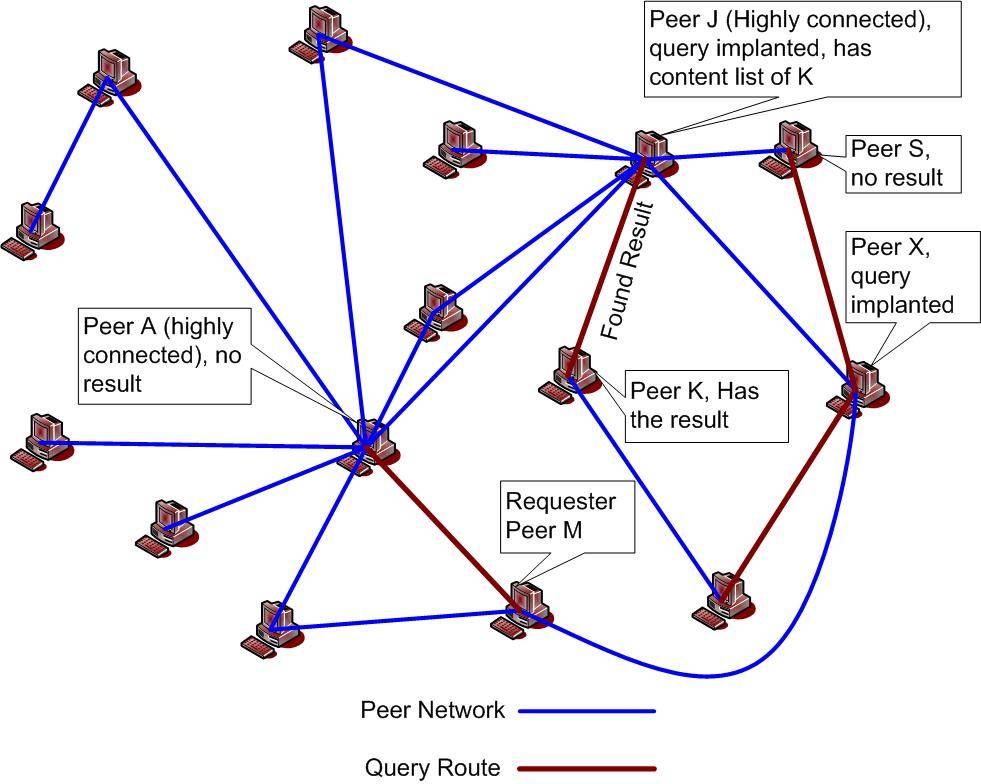
Khi một hoặc nhiều kết nối được thiết lập, nút mới sẽ gửi một thông điệp chứa địa chỉ IP của chính nó tới các nút hàng xóm. Những nút hàng xóm này sẽ lần lượt chuyển tiếp thông điệp đó tới các nút hàng xóm khác của họ. Điều này giúp cho địa chỉ của nút mới được thiết lập được quảng bá trên toàn mạng và được kết nối tốt hơn. Ngoài ra, các nút mới được kết nối có thể gửi yêu cầu truy vấn thêm địa chỉ cho các nút hàng xóm, và yêu cầu các nút này trả về một danh sách địa chỉ IP của các nút khác trên mạng. Bằng cách này, một nút có thể tìm thấy các nút khác để kết nối và quảng bá sự tồn tại của nó trên mạng để các nút khác có thể tìm thấy nó. Điều này có thể mô tả như hình dưới đây:



Nguồn: Mastering Bitcoin

Các nút trên một mạng ngang hàng có thể tham gia hoặc rời khỏi một cách ngẫu nhiên, do đó các kết nối và các bảng định tuyến không phải bao giờ cũng đáng tin cậy. Vì vậy có nút liên tục phải thực hiện khám phá các nút mới cũng như hỗ trợ các nút khác tạo lập kết nối khi chúng tham gia mạng. Để tăng hiệu quả cho quá trình này, chúng ta có một khái niệm được gọi là bootstrap. Khái niệm này giúp giảm tải băng thông và tài nguyên của mạng được sử dụng thể thiết lập kết nối. Sau khi bootstrapping, một nút sẽ ghi nhớ các kết nối ngang hàng thành công gần đây nhất của nó, để nếu được khởi động lại, nó có thể nhanh chóng thiết lập lại các kết nối với mạng ngang hàng trước đây. Nếu không ai trong số các nút cũ này phản hồi yêu cầu kết nối của nó, thì nó mới tiến hành sử dụng các seed node để khởi động lại quá trình xây dựng kết nối.

Việc tìm kiếm các tài nguyên khác trong mạng lưới Peer to Peer diễn ra tương tự, điều khác biệt duy nhất đó là các thông điệp truy vấn và phản hồi giữa các nút và công việc mà các nút cần thực hiện. Chẳng hạn muốn tìm kiếm một file được chia sẻ trên mạng P2P, một nút có thể tiến hành truy vấn đến giá trị băm của nó thông qua các bảng băm DHT được lưu trữ trên các nút theo cách tìm kiếm ở trên, các nút khi đó thay vì các địa chỉ trả về có thể trả về thông tin cụ thể về các nút chứa dữ liệu này.



Giao thức như trên được sử dụng trong mạng P2P Gnutella và hầu hết các giao thức P2P khác chẳng hạn trong Bitcoin hoặc nhiều mô hình Blockchain khác. Nó được gọi là phương pháp tìm kiếm theo chiều rộng (BFS) trên sơ đồ mạng lớp phủ có giới hạn độ sâu D. Trong phương pháp này, nút truy vấn sẽ gửi yêu cầu truy vấn tới tất cả các lân cận của nó. Mỗi hàng xóm xử lý truy vấn và trả về kết quả nếu dữ liệu được tìm thấy. Hàng xóm này sau đó chuyển tiếp yêu cầu truy vấn tới tất cả các hàng xóm của nó ngoại trừ nút truy vấn. Quy trình này tiếp tục cho đến khi đạt đến giới hạn độ sâu D. Tuy nhiên, đây không phải là phương pháp duy nhất được sử dụng để các nút có thể tìm thấy nhau và xây dựng bảng định tuyến của mình. Như có thể thấy thì phương pháp trên tạo ra một số lượng lớn các thông điệp dư thừa, trùng lặp và không có khả năng mở rộng tốt. Do đó, có rất nhiều các phương pháp khác được sử dụng trong các loại giao thức P2P khác nhằm cải tiến nó. Chẳng hạn như các phương pháp lặp sâu, bước nhảy ngẫu nhiên k-walker, BFS ngẫu nhiên sửa đổi, bước nhảy ngẫu nhiên k-walker hai cấp, tìm kiếm thông minh… Tuy nhiên, nhìn chung, trong tất cả các phương pháp này, cơ chế hoạt động luôn diễn ra tương tự như trên tức là một truy vấn được chuyển tiếp đến một tập hợp con các nút lân cận và tiếp tục được chuyển tiếp đến các hàng xóm lân cận khác, trừ một số cách cắt tỉa để tránh việc chuyển tiếp lặp lại.

Hiệu quả định tuyến thường được đo bằng số bước nhảy trên mỗi truy vấn. Trong một số hệ thống, nó cũng được đánh giá bằng cách sử dụng số lượng thông điệp cần truyền trên mỗi truy vấn. Các kỹ thuật tìm kiếm khác nhau tạo ra sự đánh đổi khác nhau giữa các đặc điểm mong muốn này. Sự phức tạp của các giao thức nảy sinh từ các ràng buộc và yêu cầu bổ sung khác nhau tùy theo từng loại mạng. Các tính năng mong muốn của thuật toán tìm kiếm trong các hệ thống P2P bao gồm các kết quả truy vấn chất lượng cao, tối thiểu hóa số nút cần truy vấn, hiệu quả định tuyến cao, cân bằng tải, khả năng phục hồi cho các lỗi trên nút và khả năng hỗ trợ các truy vấn phức tạp. Chất lượng của kết quả truy vấn phụ thuộc vào ứng dụng. Nói chung, nó được đo bằng số lượng kết quả và mức độ liên quan chẳng hạn các ràng buộc về vấn đề tính tin cậy, tính ẩn danh, tối ưu hóa độ trễ, tối ưu hóa các luồng băng thông cao của nhiều thông điệp…

Sau khi đã tìm kiếm được các nút và tài nguyên cần thiết, các ứng dụng trên mạng lưới sẽ thực hiện các yêu cầu phù hợp với yêu cầu hoạt động của mạng, chẳng hạn như tải về các file chia sẻ, phát tán kết quả tạo khối (sau khi Proof of Work hoặc một số loại bằng chứng hoạt động khác)… Các hành động này diễn ra giống hệt như các giao thức trên môi trường TCP/IP. Trên blockchain, các nút sẽ truy vấn và tiến hành giao tiếp để đồng bộ hóa dữ liệu trên mạng lưới.

# Ưu, nhược điểm của của P2P

Ưu điểm:

Trong mô hình máy chủ – máy khách, hiệu suất giảm xuống nếu có nhiều người dùng, vì băng thông sẽ được chia sẻ cho nhiều người dùng hơn. Trong các mạng ngang hàng, càng có nhiều người dùng thì càng làm cho mạng hiệu quả hơn. Càng nhiều người dùng tạo một file cụ thể có sẵn từ ổ cứng của họ thì người dùng mới có thể nhận file đó càng dễ dàng hơn. Thay vì lấy toàn bộ file từ một người dùng, bạn đang lấy các phần nhỏ hơn từ hàng trăm hoặc hàng nghìn người khác. Ngay cả khi họ chỉ có một chút băng thông trống cho bạn. Sau đó, đến lượt bạn đóng góp để phân phối các file một lần nữa.

Các mạng ngang hàng có tính bảo mật cao hơn so với kiến trúc máy khách-máy chủ truyền thống. Việc phân phối các chuỗi khối trên một số lượng lớn các nút làm cho chúng hầu như có khả năng chống lại các cuộc tấn công đã được sử dụng để tấn công nhiều hệ thống. Tương tự như vậy, vì phần lớn các nút phải đạt được sự đồng thuận trước khi dữ liệu mới được thêm vào blockchain, nên kẻ tấn công gần như không thể thay đổi dữ liệu. Điều này đặc biệt đúng đối với các mạng lớn như mạng Bitcoin.

Ngoài khả năng bảo mật, việc sử dụng kiến trúc P2P trong các blockchain tiền mã hóa cũng giúp chúng chống lại sự kiểm duyệt của các cơ quan trung ương. Khác với các tài khoản ngân hàng tiêu chuẩn, chính phủ không thể đóng băng hoặc rút sạch các ví tiền mã hóa. Ngoài ra, kiến trúc P2P cũng giúp các blockchain chống lại sự kiểm duyệt của các nền tảng nội dung và nền tảng xử lý thanh toán tư nhân. Một số nhà sáng tạo nội dung và các thương gia trực tuyến đã chấp nhận phương thức thanh toán qua tiền mã hóa như một cách để tránh bị chặn thanh toán bởi các bên thứ ba.

* Tất cả các máy khi tham gia mạng lưới đều có thể đóng góp thông tin bao gồm băng thông, dữ liệu và cả khả năng tính toán. Càng nhiều máy tham gia thì lượng thông tin cung cấp cho người dùng càng nhiều.
* Nhờ tính chất phân tán giúp các mạng khác vẫn hoạt động tốt khi một máy trong mạng lưới gặp sự cố.
* Máy tính trong hệ thống đóng vai trò như máy chủ và máy khách
* Phần mềm sử dụng dễ dàng và được tích hợp tốt
* Phần mềm có nhiều công cụ hỗ trợ người dùng và các chức năng khác nhau
* Phần mềm hỗ trợ các giao thức qua mạng như SOAP hoặc XML-RPC.

**Nhược điểm:**

* Các yêu cầu dịch vụ có thể đáp ứng tùy biến nên kết quả nhận cũng khác nhau
* Yêu cầu gửi đi sẽ không nhận được kết quả trả về vì không có gì đảm bảo một máy có thể đáp ứng được yêu cầu đó.
* Các tài nguyên sẽ biến mất vì node cung cấp tài nguyên bị ngắt kết nối bất cứ lúc nào.

Mặc dù có nhiều ưu điểm, việc sử dụng mạng P2P trên blockchain cũng có những hạn chế nhất định.

Vì sổ cái phân tán phải được cập nhật trên mỗi nút thay vì trên máy chủ trung tâm, nên việc thêm giao dịch vào blockchain đòi hỏi phải sử dụng những thuật toán phức tạp. Điều này mặc dù giúp tăng khả năng bảo mật, nhưng nó làm giảm đáng kể hiệu suất hoạt động và là một trong những trở ngại chính đến khả năng mở rộng và ứng dụng mạng rộng rãi. Tuy nhiên, các nhà mật mã học và nhà phát triển blockchain đang nghiên cứu các lựa chọn thay thế có thể được sử dụng làm giải pháp mở rộng. Các ví dụ nổi bật bao gồm các giao thức Lightning Network, Ethereum Plasma, và Mimblewimble.

Một hạn chế khác có thể xảy ra liên quan đến các cuộc tấn công có thể phát sinh trong các sự kiện chia tách chuỗi (hard fork). Vì hầu hết các blockchain là phi tập trung và có mã nguồn mở, nên các nhóm nút được tự do sao chép, sửa đổi mã và tách ra khỏi chuỗi chính để tạo thành một mạng song song mới. Việc chia tách chuỗi (hard fork) là hoàn toàn bình thường và bản thân chúng không phải là một mối đe dọa. Tuy nhiên nếu các phương thức bảo mật nhất định không được áp dụng đúng cách, cả hai chuỗi có thể dễ dàng trở thành mục tiêu của các cuộc tấn công.

Hơn nữa, bản chất phân tán của mạng P2P khiến chúng tương đối khó kiểm soát và điều tiết, không chỉ trong phân khúc blockchain. Một số ứng dụng và công ty P2P đã tham gia vào các hoạt động bất hợp pháp và vi phạm bản quyền.

# Ứng dụng của mạng ngang hàng

<lời dẫn >

* Peer to Peer Lending là gì?

Peer to Peer Lending hay còn gọi là cho vay ngang hàng. Đây là mô hình kinh doanh giữa cá nhân, doanh nghiệp với nhà đầu tư thông qua việc kết nối internet để thực hiện giao dịch vay tiền.

Đặc điểm:

* + Dựa trên nền tảng P2P nhà đầu tư có thể chọn lựa người vay
  + Tạo ra lợi nhuận cao
  + Người vay và người cho vay không cần có mối quan hệ từ trước
  + Quá trình cho vay diễn ra trực tuyến, chỉ với vài thao tác đơn giản và cực kì nhanh chóng
  + Cần có quá trình xác minh thông tin, tài khoản ngân hàng, nghề nghiệp và thu nhập của khách hàng
  + Thích hợp với những khoản vay nhỏ, vay ngắn ngày
  + Mô hình cho vay online thu hút lượng lớn người đi vay, các nhà đầu tư dễ dàng theo dõi lợi nhuận của mình từ các khoản vay
  + Đảm bảo tuân thủ quy định pháp luật và báo cáo
* Peer to Peer Payment là gì?

Peer to Peer Payment – Thanh toán ngang hàng. Đây là hình thức thanh toán trực tuyến phát triển cực nhanh khi nó có khả năng chuyển khoản trực tiếp giữa hai cá nhân với nhau. Người dùng có thể mở tài khoản của một nhà cung cấp nhằm kết nối dịch vụ với tài khoản ngân hàng. Sau đó họ sẽ gửi tiền vào tài khoản để giao dịch, thanh toán với các cá nhân khác cũng có tài khoản tại nhà cung cấp đó.

Một trong những app sử dụng ứng dụng này của P2P, đó là Metal Pay. Hệ thống Metal pay hoạt động dựa trên nền tảng blockchain – bởi vậy, chúng hoạt động trên nền tảng P2P. Ứng dụng này cho phép người dùng thanh toán hoặc chuyển tiền sử dụng đồng tiền ảo MTL – một đơn vị tiền ảo được phát triển vào năm 2017. Đặc biệt, mỗi lần thanh toán, người dùng sẽ nhận được phần thưởng là số MTL lên tới 5% giao dịch. Mục đích của hệ thống này là để phổ biến đồng tiền MTL rộng rãi tới mọi người.

* Giao dịch tiền điện tử Peer to Peer

Mạng ngang hàng có nhiều ứng dụng trong đó điển hình là giao dịch tiền điện tử P2P (giao dịch phân quyền). Đây là những giao dịch được vận hành độc quyền bởi phần mềm, cho phép những người tham gia vào thị trường có thể giao dịch trực tiếp với nhau mà không cần đến một bên thứ ba (như ngân hàng/tổ chức tài chính).

Các công ty sẽ xây dựng nền tảng giao dịch tiền điện tử P2P để giúp người dùng thực hiện giao dịch đơn giản hơn, và thu phí trên mỗi lần họ thực hiện giao dịch.

Nhờ tiền điện tử P2P mà những hạn chế trong giao dịch Bitcoin được loại bỏ. Trong giao dịch tiền điện tử, nhu cầu đổi tiền ảo thành tiền mặt ngày càng gia tăng, dẫn đến việc hỗ trợ đổi tiền ảo từ những sàn giao dịch trực tuyến như BTC China, Kraken và Bitstamp.

Tuy nhiên, những giao dịch này được điều khiển bởi các công ty thứ ba. Những công ty này đứng ra bảo lãnh cho các giao dịch, làm trọng tài khi có tranh chấp xảy ra và thu phí cho từng giao dịch nhỏ.

Nhờ giao dịch ngang hàng phân quyền P2P điều khiển bằng phần mềm, thị trường có thể loại bỏ sự tồn tại của những công ty thứ ba mà vẫn có thể giao dịch hiệu quả với nhau, thậm chí còn nhanh chóng và đơn giản hơn rất nhiều.

* Vai trò của Mạng ngang hàng trong Blockchain

Trong giai đoạn đầu của Bitcoin, Satoshi Nakamoto định nghĩa nó là một “Hệ thống tiền mặt điện tử ngang hàng” Bitcoin ban đầu được tạo ra như một dạng tiền kỹ thuật số. Nó có thể được chuyển từ người dùng này sang người dùng khác thông qua mạng ngang hàng, mạng này quản lý một cuốn sổ cái phân tán được gọi là chuỗi khối (blockchain).

Trong bối cảnh này, chính kiến trúc ngang hàng, một công nghệ trung tâm của blockchain cho phép người dùng có thể giao dịch Bitcoin và các loại tiền mã hóa khác trên toàn thế giới mà không cần đến trung gian cũng như bất kỳ máy chủ trung tâm nào. Ngoài ra, bất kỳ ai cũng có thể trở thành một nút trên mạng Bitcoin nếu họ muốn tham gia vào quá trình xác minh và xác thực các khối.

Vì vậy, không có ngân hàng nào để xử lý hoặc ghi lại các giao dịch trên mạng Bitcoin. Thay vào đó, blockchain hoạt động như một sổ cái kỹ thuật số ghi lại công khai tất cả hoạt động. Về cơ bản, mỗi nút giữ một bản sao của blockchain và so sánh nó với các nút khác để đảm bảo dữ liệu chính xác. Mạng nhanh chóng từ chối mọi hoạt động độc hại hoặc không chính xác.

Trong bối cảnh của các blockchain của tiền mã hóa, các nút có thể đảm nhận các vai trò khác nhau. Ví dụ, các nút đầy đủ là các nút giúp duy trì tính bảo mật cho mạng bằng cách xác minh các giao dịch theo các quy tắc đồng thuận của hệ thống.

Mỗi nút đầy đủ duy trì một bản sao hoàn chỉnh, cập nhật của blockchain - cho phép họ tham gia vào công việc chung để xác minh trạng thái thực của sổ cái phân tán. Tuy nhiên, điều đáng chú ý là không phải tất cả các nút xác thực đầy đủ đều là thợ đào.

Kiến trúc ngang hàng là yếu tố cốt lõi của công nghệ blockchain - nền tảng của tiền mã hóa. Có nhiều cách để phát triển và sử dụng kiến trúc ngang hàng. Bằng cách phân tán các sổ cái giao dịch trên một mạng lớn gồm nhiều nút, kiến trúc P2P cung cấp khả năng bảo mật, phi tập trung và chống kiểm duyệt.

* Giao thức BitTorrent

Được thiết kế vào năm 2001, BitTorrent là một giao thức mã nguồn mở, nơi người dùng tạo một file meta (được gọi là file torrent) chứa thông tin về bản tải xuống, mà không thực sự cung cấp dữ liệu tải xuống. Trình theo dõi (tracker) là yếu tố cần thiết để lưu trữ các file meta này, cùng với người hiện đang lưu trữ file đó. Tuy nhiên, như một giao thức mở, bất kỳ ai cũng có thể lập trình phần mềm máy khách hoặc tracker.

Vì vậy, mặc dù nó cần một tracker trung tâm để duy trì cơ sở dữ liệu của những file có sẵn, nhiều tracker khác có thể tồn tại cùng lúc. Bất kỳ file mô tả torrent nào cũng có thể đăng ký với nhiều tracker. Điều này làm cho mạng BitTorrent cực kỳ mạnh mẽ và hầu như không thể hoàn toàn bị phá hủy.

Kể từ khi ra mắt lần đầu, các cải tiến khác đã được thực hiện, nhằm cho phép người dùng tải xuống mà không cần tracker. DHT (distributed hash table - bảng băm phân tán) có nghĩa là công việc lập chỉ mục các file có sẵn có thể phân phối bởi tất cả người dùng. Magnet link không giống như vậy. Về cơ bản, Magnet link hoạt động tương tự một file torrent bình thường, với đầy đủ thông tin để máy tính có thể tải xuống một file dữ liệu từ những “peer” (có thể hiểu là nguồn tải xuống hay những người đã tải xong file dữ liệu tương tự). Tuy nhiên Magnet link không tồn tại dưới dạng một file cố định như torrent mà chỉ là một đoạn text chứa tất cả mọi thông tin.

* Các ứng dụng khác

# Lợi ích của mạng ngang hàng (P2P) trong giao dịch tiền ảo

***Chống tập trung quyền giao dịch***

Hay còn gọi là chống kiểm soát giao dịch. Những giao dịch P2P sẽ không bị kiểm soát bởi một cơ quan hay tổ chức có thẩm quyền nào, lợi ích của những người tham gia giao dịch được bảo toàn. Ngay cả khi một bộ phận của hệ thống ngừng hoạt động, phần còn lại vẫn không bị ảnh hưởng.

***Chi phí thấp***

Không phải trả tiền cho bên thứ 3 khi giao dịch vì hệ thống P2P được điều khiển bằng phần mềm.

***Bảo mật cao***

Chính phủ chưa có quyền áp đặt quy định về xác thực thông tin cá nhân đối với các giao dịch P2P, do vậy quyền riêng tư của những người tham gia giao dịch vẫn được bảo mật.

***An ninh cao***

Mạng lưới P2P không nắm giữ coin trong mỗi lượt giao dịch mà giúp các bên tham gia có thể giao dịch trực tiếp với nhau, do vậy bạn sẽ không lo bị mất tiền trong quá trình giao dịch.

Tuy nhiên, giao dịch P2P cũng còn tồn tại một số nhược điểm như thời gian giao dịch lâu và độ thanh khoản thấp.

# Tranh cãi pháp lý

Political implications (Ý nghĩa chính trị)

Intellectual property law and illegal sharing (Luật sở hữu trí tuệ và chia sẻ bất hợp pháp)

Although peer-to-peer networks can be used for legitimate purposes, rights holders have targeted peer-to-peer over the involvement with sharing copyrighted material. Peer-to-peer networking involves data transfer from one user to another without using an intermediate server. Companies developing P2P applications have been involved in numerous legal cases, primarily in the United States, primarily over issues surrounding copyright law.[46] Two major cases are Grokster vs RIAA and MGM Studios, Inc. v. Grokster, Ltd.[47] In both of the cases the file sharing technology was ruled to be legal as long as the developers had no ability to prevent the sharing of the copyrighted material.

Controversies have developed over the concern of illegitimate use of peer-to-peer networks regarding public safety and national security. When a file is downloaded through a peer-to-peer network, it is impossible to know who created the file or what users are connected to the network at a given time. Trustworthiness of sources is a potential security threat that can be seen with peer-to-peer systems.[57]

A study ordered by the European Union found that illegal downloading may lead to an increase in overall video game sales because newer games charge for extra features or levels. The paper concluded that piracy had a negative financial impact on movies, music, and literature. The study relied on self-reported data about game purchases and use of illegal download sites. Pains were taken to remove effects of false and misremembered responses.[58][59][60]

**Tính trung lập của mạng**

Các ứng dụng ngang hàng thể hiện một trong những vấn đề cốt lõi trong tranh cãi về tính trung lập của mạng . Các nhà cung cấp dịch vụ Internet ( ISP ) đã được biết đến để điều tiết lưu lượng chia sẻ tệp P2P do sử dụng băng thông cao . [61] So với trình duyệt Web, e-mail hoặc nhiều công dụng khác của Internet, nơi dữ liệu được chỉ chuyển trong khoảng thời gian ngắn và số lượng tương đối nhỏ, chia sẻ file P2P thường bao gồm việc sử dụng băng thông tương đối nặng do chuyển file đang diễn ra và bầy đàn / gói phối hợp mạng. Vào tháng 10 năm 2007, Comcast , một trong những nhà cung cấp Internet băng thông rộng lớn nhất ở Hoa Kỳ, đã bắt đầu chặn các ứng dụng P2P như BitTorrent. Lý do của họ là P2P chủ yếu được sử dụng để chia sẻ nội dung bất hợp pháp và cơ sở hạ tầng của họ không được thiết kế cho lưu lượng băng thông cao, liên tục. Các nhà phê bình chỉ ra rằng mạng P2P có các sử dụng hợp pháp và đây là một cách khác mà các nhà cung cấp lớn đang cố gắng kiểm soát việc sử dụng và nội dung trên Internet và hướng mọi người tới kiến trúc ứng dụng dựa trên máy chủ . Mô hình máy khách-máy chủ cung cấp các rào cản tài chính đối với các nhà xuất bản và cá nhân nhỏ và có thể kém hiệu quả hơn khi chia sẻ các tệp lớn. Như một phản ứng đối với việc điều chỉnh băng thông này , một số ứng dụng P2P đã bắt đầu thực hiện giao thức che giấu giao thức, chẳng hạn như mã hóa giao thức BitTorrent. Các kỹ thuật để đạt được "obfuscation giao thức" liên quan đến việc loại bỏ các thuộc tính dễ nhận dạng khác của các giao thức, chẳng hạn như chuỗi byte xác định và kích thước gói, bằng cách làm cho dữ liệu trông như thể là ngẫu nhiên. [62] Giải pháp của ISP cho băng thông cao là bộ nhớ đệm P2P , trong đó ISP lưu trữ một phần các tệp được khách hàng P2P truy cập nhiều nhất để tiết kiệm quyền truy cập vào Internet.

# Tương lai của chia sẻ file qua mạng ngang hàng

Những vụ kiện tụng liên quan tới bản quyền không kìm hãm sự phát triển của nền tảng chia sẻ file này, mà còn khiến nó phát triển hơn khi tiếp tục đưa ra các thay đổi trên hệ thống để thích nghi tình hình. Bất chấp những động thái pháp lý - điển hình là vụ kiện Hiệp hội các nhà ghi âm Mỹ (RIAA) nhằm đóng cửa Napster, hình thức chia sẻ tệp tin vẫn không hề có dấu hiệu suy giảm - ít nhất là trong thời gian trước mắt.

**Nhà cung cấp: Đi vào hoạt động ngầm**

Không lâu sau khi RIAA bắt đầu chú ý tới các dịch vụ chia sẻ file, các "nhà cung cấp" nhanh chóng thay đổi phương thức hoạt động, mà phổ biến nhất là "ém" thông tin của các khách hàng. Bản thân các động thái pháp lý cứng rắn nhằm vào Napster hay KaZaA được nhìn nhận như "đánh rắn động cỏ", thôi thúc các dịch vụ chia sẻ file đi vào hoạt động ngầm và ngày càng khó kiểm soát.

Mike, một thành viên website www.techdirt.com nhận định: "Chỉ một vài năm nữa, tôi cho rằng nhiều chúng ta sẽ phải thay đổi quan niệm đối với các dịch vụ trực tuyến tưởng như là "lầm đường, lạc lối". Trong khi đó theo nhìn nhận của nhà sáng lập dự án Freenet Ian Clarke, quyết định của RIAA chẳng khác gì "một hành động mang tính đường cùng của một ngành công nghiệp đang giẫy chết".

Cũng theo Ian Clarke, RIAA cần nhìn thấy sự ưu ái của người sử dụng dành cho các tiện ích chia sẻ file miễn phí. Bản thân RIAA "không nên coi hình thức này là một mối đe doạ mà thay vào đó là một kênh phân phối mới, có thể kiếm ra tiền".

**Không có chỗ cho những tệp tin giả mạo**

Trong nỗ lực lưu giữ sự ủng hộ của đa số người dùng và tránh "búa rìu" từ phía những công ty thu âm, ghi đĩa, chất lượng các ứng dụng, mạng chia sẻ ngang hàng sẽ ngày càng được cải thiện. Đặc biệt, cơ chế sàng lọc công khai sẽ giúp loại bỏ những tệp tin giả mạo, vô giá trị hoặc đính kèm phần mềm quảng cáo (adware), gián điệp (spyware) ra khỏi "thị trường giao dịch".

Công cụ đánh giá (rating) cũng sẽ được tích hợp ngay trên các website cung cấp. Người sử dụng có cơ hội đánh giá một cách khách quan những thông tin được đăng tải. Sau một chu trình, quản trị mạng trước sức ép của "khách hàng" sẽ phải loại bỏ những tệp tin kém chất lượng, liên tục nằm ở cuối bảng.

Cách thức chia sẻ file cũng liên tục được cải thiện bởi những công nghệ mới dành cho chia sẻ file qua mạng ngang hàng. Một trong những công nghệ hiện đang được nhắc tới nhiều nhất là Cyclic Redundancy Checking (CRC- Kiểm duyệt tính hữu dụng qua vòng xoắn). CRC xác minh gói tin được gửi đi cả ở đầu người gửi và đầu người nhận trong mạng ngang hàng. Bên cạnh CRC, không ít người sử dụng phương pháp "remailer"- gửi thông tin truy vấn của mình qua các trạm trung gian (proxy), nên dễ dàng che giấu được tung tích. Trong khi đó, các tệp tin chia sẻ trong tương lai cũng có thể sẽ được chia thành nhiều gói nhỏ không thể xác định được tung tích (untracable) để rồi sau đó lại tự động "lắp ráp" khi tới đích. Theo dõi nhằm "kết tội" tác giả gửi- nhận các gói tin kiểu này, các công ty kinh doanh có nắm bản quyền chỉ có biết "dở khóc, dở cười".

**Thu hẹp khoảng cách**

Hiệp hội mặt trận điện tử (EFF) đang vận động hướng tới hợp thức hoá hình thức chia sẻ file qua mạng ngang hàng. Môi trường mà trong đó các nghệ sĩ nhận được thù lao từ chính mạng cung cấp dịch vụ tưởng như miễn phí. Ý tưởng của EFF là "giảm thiểu tối đa khả năng bị tố cáo thông qua việc đảm bảo rằng người sử dụng được phép lưu trữ những tệp tin trong thư mục được chia sẻ, loại bỏ toàn bộ những tên tệp tin dễ "nhầm lẫn" với một ca sĩ hoặc một bài hát thuộc sở hữu của RIAA.

Ian Clarke thuộc Freenet lý giải, không lâu nữa chúng ta sẽ thay đổi cách nhìn nhận về việc chia sẻ những tệp tin MP3 qua mạng. Tuy nhiên tính cho tới thời điểm đó, vẫn đề bản quyền và tính riêng tư vẫn còn là một thách thức cần phải vượt qua.

# Kết luận

Không có gì phải bàn cãi khi nói rằng mạng P2P đã thay đổi Internet mãi mãi. Với đỉnh điểm vào năm 2006, ước tính rằng các mạng P2P chiếm hơn 70% lưu lượng truy cập trên toàn bộ Internet. Kể từ đó, việc sử dụng các mạng này đã giảm mạnh, chủ yếu là do các dịch vụ phát video trực tuyến dễ dàng truy cập như Netflix và YouTube, kết hợp với các dịch vụ phát nhạc trực tuyến như Spotify. Các mạng P2P đã lấp đầy một khoảng trống quan trọng trong lịch sử Internet khi các dịch vụ media truyền thống gặp khó khăn trong việc bắt kịp nhu cầu của người dùng.

Ngày nay, với sự phát triển vượt bậc của công nghệ thông tin, P2P không chỉ phát triển trên máy tính, mà còn được phát triển mạnh mẽ trên các thiết bị điện thoại thông minh và nhiều dạng thiết bị điện tử thông minh khác.

Kiến trúc P2P cũng là yếu tố cốt lõi của nhiều công nghệ, đặc biệt công nghệ blockchain – nền tảng của tiền mã hóa – công nghệ của tương lai, hay của giao thức BitTorrent – nền tảng chia sẻ file và đang được nhiều người sử dụng nhất thế giới.

Bổ sung

So sánh mô hình Peer to Peer và Client Server

Client Server là mô hình máy khách - máy chủ, có thể truy nhập mạng hay tài nguyên mạng từ các máy chủ. Đây là giải pháp khắc phục mạng quá tải và phá vỡ sự ngăn cách trong cấu trúc vật lý cũng như hệ điều hành khác nhau trên mạng.

So sánh giữa Peer to Peer và Client Server:

