# BLOCKCHAIN

## BẢN CHẤT CỦA BLOCKCHAIN, BITCOIN, TIỀN ĐIỆN TỬ, HỢP ĐỒNG THÔNG MINH VÀ TƯƠNG LAI CỦA TIỀN TỆ



MARK GATES
Thành Dương *dịch*

1980 BOOKS
NHÀ XUẤT BẢN LAO ĐỘNG

# MỤC LỤC | TABLE OF CONTENTS

# Lời Nói Đầu

Thông tin trong cuốn sách này chỉ phục vụ cho mục đích tham khảo chung. Mọi nội dung trình bày trong sách không nên coi là tư vấn và khuyến nghị.

Bạn nên cân nhắc các chỉ dẫn về luật pháp, tài chính và thuế vụ của mọi thông tin trong sách này dưới góc độ hoàn cảnh và tình huống riêng của bạn.

Mặc dù cuốn sách đã được chuẩn bị kỹ lưỡng và thận trọng, nhưng nhà xuất bản không chịu trách nhiệm với bất cứ lỗi sai, thiếu sót hoặc tổn thất phát sinh do áp dụng thông tin được cung cấp trong tài liệu này.

Tác giả và đơn vị xuất bản không chịu trách nhiệm với bất cứ thiệt hại nào, vì lý do sơ suất hay không, phát sinh từ việc sử dụng hoặc lạm dụng, trực tiếp hay gián tiếp, các thông tin trong sách.

# Bảng việt hóa thuật ngữ

| Thuật ngữ Việt hóa | Thuật ngữ gốc |
|---|---|
| Băm chỉ tiêu | Target Hash |
| Bằng chứng cháy | Proof of Burn |
| Bằng chứng cổ phần | Proof of Stake (PoS) |
| Bằng chứng dung lượng | Proof of Capacity (PoC) |
| Bằng chứng hoạt động | Proof of Activity |
| Bằng chứng xử lý | Proof of Work |
| Bảo hiểm vi mô | Microinsurance |
| Blockchain cá nhân | Private Blockchain |

| | |
|---|---|
| Blockchain công khai | Public Blockchain |
| Blockchain động | Live Blockchain |
| Blockchain liên hợp | Consortium Blockchain |
| Cây Merkle gốc | Merkle Tree Root |
| Chỉ tiêu độ khó | Difficult Target |
| Chiều cao khối | Block Height |
| Chữ ký điện tử | Digital Signature |
| Chữ ký mù | Blind Signature |
| Chuỗi chính | Main Chain |
| Địa chỉ khối | Blockchain Address |
| Độ khó mạng lưới | Network Difficulty |
| Đồng thuận phân tán | Distributed Consensus |
| Giải thuật ký số hệ mật đường cong Elliptic | Elliptic Curve Digital Signature Algorithm |
| Giao dịch lặp chi | Double Spending |
| Giao dịch ngoại tuyến | Offline Transaction |

| | |
|---|---|
| Giao thức hợp đồng thông minh | Smart Contract Protocol |
| Hàm băm mật mã học | Cryptographic Hash Function |
| Khóa cá nhân | Private Key |
| Khóa công khai | Public Key |
| Khóa mật mã | Combination Lock |
| Lưu trữ đám mây | Cloud Storage |
| Mã băm | Hash |
| Mã hóa sử dụng hàm băm | Cryptographic Hash |
| Mã nguồn mở | Open Source |
| Mật mã hóa khóa công khai | Public Key Cryptography |
| Máy ảo Ethereum | Ethereum Virtual Machine |
| Mô hình ngang cấp | Peer-to-Peer (P2P) |

| | |
|---|---|
| Nhân chứng tách rời | Segregated Witness (SegWit) |
| Nhận diện kỹ thuật số | Digital Identity |
| Nhãn thời gian | Timestamp |
| Phân nhánh | Fork |
| Phần thưởng khối | Block Reward |
| Sổ cái (cấp quyền) | Ledger (Permissioned) |
| Sổ cái (không cấp quyền) | Ledger (Un-permissioned) |
| Sổ cái công khai phân tán | Distributed Public Ledger |
| Sổ cái phân tán | Distributed Ledger |
| Tấn công quá bán | 51% Attack |
| Tấn công từ chối dịch vụ | Denial of Service Attack (DoS Attack) |
| Thanh toán theo thời gian thực | Real-time Settlement |

| | |
|---|---|
| Thẻ | Token |
| Thuật toán mã hóa an toàn sử dụng hàm băm | Secure Hash Algorithm |
| Tín dụng vi mô | Microfinance |
| Ứng dụng phi tập trung | Decentralized Application (dApp) |

# Giới thiệu

*"Trên mạng Internet, không ai biết bạn là kẻ ngốc."*

**- Peter Steiner**

*"Trong Blockchain, không ai biết bạn là kho lạnh."*

**- Richard Gendal Brown**

Công nghệ Blockchain được coi là phát minh vĩ đại nhất kể từ khi xuất hiện mạng Internet.

Những người khởi xướng tuyên bố rằng công nghệ này sẽ thay đổi mọi ngành công nghiệp hiện thời và ảnh hưởng tới cuộc sống của mọi người trên hành tinh này chỉ trong vài thập kỷ.

Liệu công nghệ Blockchain thực sự là một trong những cuộc cách mạng công nghệ vĩ đại nhất trong lịch sử hay chỉ được cường điệu quá mức?

Liệu công nghệ Blockchain sẽ khiến hệ thống trái phiếu chính phủ và hoạt động ngân hàng thay đổi phương pháp xử lý thông tin hay sẽ chỉ là một giao dịch bình thường?

Có phải những người tuyên truyền về công nghệ Blockchain đã quá kích động đến mức tạo nên một loại bong bóng công nghệ khác, trong khi thực ra chỉ là một cách thức tạo dữ liệu mới?

Trong cuốn sách này, chúng ta sẽ tìm hiểu đáp án cho những câu hỏi trên, đồng thời xem xét những góc độ lập luận khác, ủng hộ và phản đối, công nghệ Blockchain.

Cuốn sách này cũng sẽ giải thích công nghệ Blockchain là gì, cách thức hoạt động và lợi ích tiềm tàng cùng những ảnh hưởng

của công nghệ này.

Dù đề cập nhiều ứng dụng tiềm năng và giá trị, cuốn sách này không nhằm mục đích quảng bá công nghệ Blockchain là giải pháp cho mọi vấn đề trong hệ thống trái phiếu chính phủ, hoạt động ngân hàng hoặc lĩnh vực công nghiệp.

Mục đích là cung cấp kiến thức đa chiều về công nghệ Blockchain cùng với lợi ích, giá trị tiềm tàng, rủi ro, bất lợi và những đồn thổi phóng đại xung quanh nó.

Cuốn sách này được viết dành cho những người bắt đầu nghiên cứu công nghệ Blockchain và đang tìm hiểu kiến thức không quá thiên về khoa học kỹ thuật của công nghệ này. Một số nội dung kỹ thuật sẽ được nhắc đến trong phần cuối sách, tuy nhiên những chi tiết thuần kỹ thuật về Blockchain không phải trọng tâm của cuốn sách.

Lần đầu tiên tìm hiểu về công nghệ Blockchain, tôi thấy rằng nhiều thông tin thuần kỹ thuật về công nghệ Blockchain được phân bổ và sắp xếp bất ổn, và không có hướng dẫn rõ ràng từ nền tảng kiến thức ngoài lĩnh vực kỹ thuật.

Tôi viết cuốn sách này vì đây chính là kiểu sách có nội dung mà, vào thời điểm lần đầu tiên tiếp cận và thử tìm hiểu về công nghệ Blockchain, tôi muốn đọc.

Tôi hy vọng bạn sẽ đọc và thấy rằng cuốn sách hữu dụng, sáng suốt và có giá trị cho kiến thức về công nghệ Blockchain của bạn.

Ghi chú:

• Cuối mỗi chương sẽ có những điểm cốt lõi tóm tắt thông tin toàn chương. Cách trình bày này thích hợp với những người ưa tổng hợp thông tin thành nhiều điểm chính yếu.

• Nếu bạn không thích hoặc không có thời gian đọc một chương nào đó, cứ thoải mái lướt tới phần tổng kết những điểm cốt lõi để biết được thông tin chính trong chương.

• Điểm cốt lõi còn hỗ trợ đắc lực cho việc ghi chú, tái xem xét hoặc tra cứu nhanh để tham khảo mà không cần đọc lại toàn chương.

• Nếu bạn đã đọc trọn vẹn chương, bạn có thể bỏ qua phần tổng kết những điểm cốt lõi vì phần này sẽ nhắc lại những thông tin bạn vừa đọc.

# Chương 1
# Blockchain là gì?

*Có sự nhầm lẫn rằng Blockchain là công nghệ duy nhất trong Bitcoin, tuy nhiên Bitcoin được tạo nên bằng cách sử dụng một chuỗi các công nghệ mật mã khác kết hợp với Blockchain.*

Nói ngắn gọn, Blockchain là một loại dữ liệu, một cách lưu trữ những hồ sơ giao dịch và giá trị.

Đáng tiếc là, định nghĩa đơn giản này không hấp dẫn mọi người và khiến họ nghĩ rằng, "Sao cơ? Toàn bộ thứ hoành tráng này chỉ là một loại dữ liệu thôi ư?"

Dù sao thì, gọi Blockchain là một loại dữ liệu mới cũng tương tự như nói thư điện tử là cách mới để gửi thư cho người khác. Dù Blockchain là một loại dữ liệu, định nghĩa này không diễn tả được đặc tính thật sự nằm trong cách thức Blockchain lưu trữ các hồ sơ giá trị và giao dịch.

Trong quá khứ, mọi tài sản giá trị hoặc các giao dịch đều được lập biên bản đưa vào kho dữ liệu, người ta dựa vào bên thứ ba như ngân hàng, chính phủ hoặc công ty để lưu trữ thông tin này. Mọi người tin tưởng rằng ngân hàng sẽ không trộm tiền của họ vì ngân hàng chịu sự quy định của chính phủ, và nếu một ngân hàng phá sản, họ hy vọng rằng chính phủ sẽ bảo đảm khoản ký gửi của họ được an toàn.

Khi chuyển tiền hoặc chi trả hàng hóa dịch vụ, người ta tin rằng các công ty phát hành thẻ tín dụng và ngân hàng sẽ chuyển một phần tiền chính xác từ tài khoản ngân hàng và tiền ký quỹ của họ tới tài khoản người bán. Người bán tin tưởng rằng công ty phát hành thẻ tín dụng sẽ thanh toán tiền cho họ và nếu xảy ra tranh chấp hoặc gian lận giao dịch, công ty phát hành thẻ tín dụng sẽ giải quyết cho họ.

Nếu người mua tại cửa hàng thanh toán bằng tiền mặt, người bán tin rằng họ có thể nhận tờ giấy bạc in số do chính phủ phát hành đó rồi tới cửa hàng khác để mua sản phẩm dịch vụ khác. Người bán cũng tin rằng nếu họ mang số tiền giấy đó tới ngân hàng, họ có thể chuyển thành tiền kỹ thuật số trong tài khoản ngân hàng và có thể sử dụng để thanh toán qua thẻ tín dụng hoặc giao dịch trực tuyến.

Mọi người cho phép các tổ chức bên ngoài này sở hữu tiền bạc và thông tin của họ. Họ tin rằng các công ty phát hành thẻ tín dụng và ngân hàng sẽ bảo đảm các thông tin chi tiết thẻ tín dụng của họ được an toàn và riêng tư. Họ tin rằng các công ty phát hành thẻ tín dụng và ngân hàng lưu trữ dữ liệu về hồ sơ số dư tài khoản và giao dịch chuẩn xác. Các ngân hàng lại tin rằng chính phủ lưu trữ dữ liệu và hồ sơ tiền giấy phát hành.

Đặt lòng tin vào các tổ chức không chỉ xuất hiện trong lĩnh vực tài chính mà còn mở rộng tới mọi lĩnh vực trong đời sống của chúng ta. Nếu bạn từng mượn sách từ thư viện, thư viện lưu trữ dữ liệu toàn bộ số sách họ có. Thư viện cũng lưu trữ dữ liệu về thành viên, mọi cuốn sách đang mượn, ngày trả sách và mọi cuốn quá hạn trả.

Thư viện còn lưu trữ dữ liệu trung tâm về thông tin cá nhân của bạn, địa chỉ nhà và những chi tiết khác. Nếu bạn không trả sách đã mượn, họ sẽ gửi giấy phạt và nếu cần, họ có thể áp dụng các biện pháp theo luật để đối phó với hành động vi phạm của bạn.

Những hồ sơ dữ liệu về thông tin cá nhân của bạn, cuốn sách bạn mượn, thói quen đọc của bạn, đều là những thông tin riêng tư được thư viện lưu trữ, và bạn tin tưởng họ sẽ không chia sẻ thông tin đó cho những người khác.

Những thông tin như vậy được tập hợp trong nhiều tổ chức dạng này mà mỗi tổ chức lại lưu trữ bản hồ sơ và hệ thống của riêng họ.

Vấn đề phổ biến xuất phát từ mọi giao dịch thường ngày là chúng ta đặt lòng tin vào các tổ chức và dữ liệu trung tâm mà họ lưu trữ để bảo quản chính xác hồ sơ của chúng ta.

Lại có một vấn đề ngầm hiểu rất phổ biến khác là chúng ta không tin tưởng lẫn nhau.

Hãy thử tưởng tượng tình huống khi thiếu tổ chức đáng tin cậy trong giao dịch.

Hãy tưởng tượng bạn sở hữu một cửa hàng và ai đó giao cho bạn mẩu giấy có viết "Tôi nợ anh 100 đô" kèm theo chữ ký của họ. Họ nói với bạn rằng nếu bạn mang mẩu giấy đó tới cửa hàng khác, bạn có thể dùng để mua sản phẩm giá 100 đô tại đó.

**Bạn có tin họ không?**

Đáp án có lẽ là không, nhưng đó chính là điều chúng ta đang làm mỗi ngày với tiền giấy. Một tờ tiền 100 đô chỉ là một tờ giấy với dòng "Tôi nợ anh 100 đô" kèm xác nhận từ chính phủ. Bạn chấp nhận và sử dụng tiền giấy gần như hằng ngày và tin tưởng rằng các

cửa hàng sẽ chấp nhận, rồi họ lại tin tưởng những người bán khác cũng chấp nhận và cứ thế tiếp diễn.

Còn Blockchain mang đến tiềm năng to lớn tại những quốc gia mà người ta không tin vào ngân hàng, tổ chức, chính phủ, tiền tệ hoặc người khác.

Ngay cả ở Mỹ nơi hệ thống tài chính ổn định và phát triển nhất thế giới, nhiều tổ chức tài chính to lớn cũng phá sản trong cuộc Đại Khủng hoảng Tài chính. Các công ty tài chính hàng trăm năm tuổi sụp đổ gần như trong một đêm kéo theo tiền gửi cả đời của nhiều người bị mất trắng.

Năm 2015, tại Hy Lạp, một quốc gia đã phát triển và một thành viên của khối liên minh EU, các ngân hàng đóng băng toàn bộ tài khoản ký gửi và chỉ cho phép chủ tài khoản rút khoảng 70 đô mỗi ngày từ các máy rút tiền tự động.

Có lựa chọn nào dành cho người gửi tiền ngoài các công ty và ngân hàng đáng tin cậy mà họ đang đặt lòng tin? Giấu toàn bộ tiền mặt dưới đệm gối? Nếu ai đó phát hiện ra khoản tiết kiệm giấu trong nhà, bạn sẽ có nguy cơ bị trộm mất; nếu nhà của bạn bắt lửa, bạn có nguy cơ mất toàn bộ tiền vì vụ cháy.

Nếu ngân hàng có thể bị phá sản và chính phủ có thể đóng băng các khoản rút tiền từ ngân hàng tại Mỹ cũng như châu Âu, vậy làm sao những người sống ở các quốc gia kém phát triển, kém ổn định hơn có thể tin tưởng vào ngân hàng và chính phủ của họ?

Đáp án đơn giản là họ không thể tin vào những tổ chức đó.

**Vấn Đề Niềm Tin Và Blockchain**

Có hàng tỷ người trên thế giới đang sống tại các quốc gia nơi chính phủ được chế độ độc tài quân sự điều hành, chính phủ sở

hữu các ngân hàng và lấy trộm hoặc tịch thu tiền từ các tài khoản, đồng tiền địa phương không được nhiều cửa hàng chấp nhận, tội phạm tràn lan và không có hệ thống luật định để bảo vệ mọi người và tài sản của họ.

Có nhiều quốc gia nơi mà dù bạn có thể tin rằng ngân hàng sẽ không đánh cắp tiền của bạn hoặc bị phá sản, tiền gửi của bạn cũng được chính phủ giám sát cẩn thận, và họ có thể bắt giữ, tống giam hoặc xử phạt bạn vì những giao dịch của bạn.

Trong ví dụ về thư viện kể trên, chia sẻ thông tin với dữ liệu trung tâm có vẻ vô hại với bạn. Bạn có thể mượn từ thư viện cuốn sách mà chính phủ nước sở tại không chấp thuận, chẳng hạn như *Beginners guide to overthrowing a military dictatorship* (Tạm dịch: *Hướng dẫn nhập môn lật đổ chế độ độc tài*) hoặc cuốn 1984 của George Orwell. Chính phủ sở tại có thể quy kết thói quen đọc sách của bạn là bước chuẩn bị cho một mưu đồ tương lai rồi bắt giữ bạn hoặc tệ hơn.

Tại những nước này, nơi thiếu vắng lòng tin vào các công ty và chính phủ, các giao dịch rất rủi ro và khó khăn. Nếu người ta gửi tiền vào ngân hàng, họ phải đối mặt với nguy cơ bị ngân hàng hoặc chính phủ đánh cắp. Đối với những khoản mua sắm lớn như mua nhà cửa, họ có thể buộc phải tiết kiệm bằng tiền mặt, vàng, ngọc hoặc kim loại quý để dành cho khoản chi tiêu lớn này, chấp nhận rủi ro rằng tiền có thể bị đánh cắp hoặc hủy hoại do một vụ cháy.

Sau tất cả rủi ro này, nếu ai đó tiết kiệm đủ tiền cho các khoản mua sắm lớn như mua nhà cửa, họ vẫn phải đối mặt với rủi ro rằng người bán sẽ lừa trộm tiền của họ và không giao cho họ quyền sở hữu ngôi nhà. Hệ thống pháp luật không phải lúc nào cũng đủ vững

chắc để đòi lại quyền sử dụng hoặc tố cáo hành vi trộm cắp. Nếu giao dịch mua sắm thanh toán bằng tiền mặt hoặc vàng chứ không phải giao dịch điện tử, sẽ không có bằng chứng chứng minh giao dịch đã diễn ra.

Cơ sở dữ liệu trung tâm và các tổ chức hoạt động chỉ khi tồn tại niềm tin vào hệ thống pháp lý, luật định, chính phủ, tài chính và con người. Dù mọi yếu tố trên đều đáng tin cậy, niềm tin đôi khi vẫn bị phản bội vì người ta bị mất tiền bạc và tài sản.

Một cơ sở dữ liệu trung tâm được xây dựng trên Blockchain, loại bỏ sự cần thiết của các cơ sở dữ liệu và tổ chức trung tâm. Mọi cá nhân trong Blockchain có thể quan sát và kiểm nhận giao dịch, giúp đảm bảo tính minh bạch và độ tin cậy.

Niềm tin là cốt lõi của Blockchain, tạo nên hệ thống tín nhiệm giữa các cá nhân mà không cần tổ chức trung gian liên quan đến giao dịch.

Blockchain cho phép mọi người giao dịch mọi giá trị. Trong ví dụ thư viện trên thì đó là những cuốn sách, nhưng cũng có thể là bất động sản, cổ phần, tài liệu điện tử và gần như mọi thứ khác.

**Sự Khác Biệt Giữa Blockchain Và Bitcoin**

Chú ý đầu tiên về Blockchain là nó nằm trong phạm vi mã nguồn của Bitcoin, về cơ bản Blockchain đầu tiên được hình thành khi Bitcoin được tạo ra. Lịch sử của Bitcoin và Blockchain sẽ được trình bày trong chương sau, vì thế trong chương này chúng ta sẽ không đi vào chi tiết.

Blockchain là một trong những công nghệ cơ sở của Bitcoin. Có sự nhầm lẫn rằng Blockchain là công nghệ duy nhất trong Bitcoin,

tuy nhiên Bitcoin được tạo nên bằng cách sử dụng một chuỗi các công nghệ mật mã khác kết hợp với Blockchain.

Bitcoin là đồng tiền ảo, chủ yếu được dùng để thanh toán. Đó là một cách ứng dụng công nghệ Blockchain, tuy nhiên Blockchain có thể sử dụng để lưu trữ và chuyển giao mọi giá trị, không chỉ các giao dịch tài chính.

Các hệ thống xây dựng trên nền tảng Blockchain đang được sử dụng cho nhiều hoạt động đa dạng trên khắp các lĩnh vực công nghiệp khác nhau bao gồm nhận diện kỹ thuật số, mạng xã hội, bầu cử, lưu trữ dữ liệu trực tuyến, ứng dụng phi tập trung và nhiều lĩnh vực khác sẽ được trình bày trong phần sau cuốn sách. Có vẻ hệ thống xây dựng trên nền tảng Blockchain sở hữu tiềm năng vô tận đang được nhiều công ty và chính phủ khai thác.

Bitcoin, ngược lại, chỉ được sử dụng để thanh toán điện tử. Mặc dù Bitcoin ngày càng trở nên nổi tiếng vì giá trị của nó ngày càng tăng cao, đồng tiền này chủ yếu được thiết kế như một hình thức thanh toán.

Trong chương sau, chúng ta sẽ đi sâu vào chi tiết kèm các ví dụ về việc Blockchain hoạt động chính xác như thế nào.

**Điểm Cốt Lõi:**

• Blockchain giống cơ sở dữ liệu, là một hình thức lưu trữ hồ sơ giá trị và giao dịch. Gần như mọi thứ đều có thể được lưu trữ trên Blockchain.

• Đa phần các giao dịch ngày nay giữa mọi người đều đòi hỏi một đơn vị trung gian đáng tin cậy, có khả năng bảo mật và tạo điều kiện để giao dịch thuận lợi như ngân hàng và các tổ chức tài chính.

• Công nghệ Blockchain loại bỏ sự cần thiết của một đơn vị trung gian, cho phép mọi người giao dịch trực tiếp với nhau.

• Hàng tỷ người trên thế giới sống ở những quốc gia nơi mà họ không thể đặt lòng tin vào các đơn vị trung gian như ngân hàng, chính phủ và hệ thống pháp luật trong việc thực hiện giao dịch cũng như lưu trữ chính xác hồ sơ. Blockchain đặc biệt hữu dụng trong những trường hợp này vì có thể cung cấp độ tin cậy và đảm bảo cho mọi người khi họ giao dịch với nhau.

• Bitcoin là một hệ thống xây dựng trên nền tảng Blockchain. Blockchain không phải là hệ thống xây dựng trên nền tảng Bitcoin.

• Bitcoin chủ yếu được sử dụng để thanh toán. Hệ thống xây dựng trên nền tảng Blockchain có khả năng ứng dụng rộng rãi để chuyển giao mọi loại giá trị.

# Chương 2
# Blockchain hoạt động như thế nào

*Chú ý: Chương này là bản hướng dẫn tổng quan và không nặng về lý thuyết cho biết cách thức hoạt động của Blockchain.*

*Để tìm hiểu thêm hướng dẫn có tính kỹ thuật hơn về cách thức hoạt động của Blockchain, vui lòng đọc mười chương cuối cuốn sách có nhan đề Technical Guide to the Blockchain (tạm dịch: Hướng dẫn kỹ thuật về Blockchain).*

Trong chương trước, bạn đã được giới thiệu về công nghệ Blockchain kèm giới thiệu rất ngắn gọn rằng công nghệ này có thể được sử dụng để thay thế các đơn vị trung gian trong giao dịch như thế nào. Trong chương này, chúng ta sẽ đi sâu vào chi tiết và các ví dụ về cách thức hoạt động của Blockchain.

Quay lại ví dụ về thư viện trong chương trước, bạn sẽ thấy thư viện là đơn vị trung gian lưu trữ cơ sở dữ liệu trung tâm của người mượn sách.

Nếu ai đó đã mượn cuốn sách mà bạn muốn mượn, bạn có thể yêu cầu thư viện thông báo cho bạn biết khi nào cuốn sách được trả về, nhưng thư viện sẽ không cung cấp cho bạn thông tin về người đang mượn cuốn sách đó.

Người mượn cuốn sách đó có thể ở ngay phố nhà bạn, gần thư viện hơn, tuy nhiên bạn không thể đến nhà họ để hỏi xem bạn có thể mượn cuốn sách từ họ không. Thư viện lưu trữ cơ sở dữ liệu trung

tâm tất cả các thông tin sách được mượn, nhưng không chia sẻ cho các thành viên.

Bây giờ, hãy tưởng tượng một thư viện chung nơi bạn có thể đóng góp sách cho người khác mượn. Bạn có thể có nhiều sách mà người khác muốn mượn; ngược lại, người khác có nhiều sách bạn muốn mượn.

Trong ví dụ về thư viện chung, mọi người có thể tham gia và khi họ mượn sách, họ cũng có thể cho người khác mượn sách mà không cần phải mang trả lại thư viện hay chủ sở hữu cuốn sách.

Bạn sẽ lưu trữ hồ sơ những người mượn sách, cuốn nào của họ và ai là chủ sở hữu của cuốn sách như thế nào?

Hồ sơ bạn cần lưu trữ không chỉ là sách của bạn mà còn là sách của những người khác trong thư viện chung. Bạn cần ghi một hồ sơ hiện có của mọi người trong thư viện, chủ sở hữu, sách đang cho mượn và ai đang mượn.

Bạn có thể phân công một người trong nhóm ghi chép hồ sơ, nếu không bạn có thể áp dụng mô hình cơ sở dữ liệu trung tâm và thư viện thông thường.

Cách này có vẻ khá phức tạp nên đến lúc này, bạn có thể đang tự hỏi bản thân rằng tại sao mình lại chọn tham gia thư viện chung này trong khi mình chỉ cần lấy sách từ Kindle.

Đây là tình huống mà những lợi thế của công nghệ Blockchain thực sự vượt lên các cơ sở dữ liệu truyền thống.

Blockchain có thể cung cấp một cơ sở dữ liệu phân tán, phi tập trung toàn bộ sách trong thư viện.

Với cơ sở dữ liệu phi tập trung, mọi người trong thư viện có thể truy cập hồ sơ. Họ sẽ thấy tất cả sách trong thư viện, chủ sở hữu

ban đầu, người đang mượn sách, họ còn biết liệu họ có tiếp tục cho mượn cuốn sách đó nữa không.

Mỗi lần một cuốn sách trong thư viện chung được ai đó mượn, tất cả hồ sơ sách trong cơ sở dữ liệu mà mọi người truy cập đều sẽ được cập nhật. Không cần đến tổ chức hoặc cơ sở dữ liệu trung tâm để thực hiện hoạt động này, mọi người tự ghi chép dữ liệu.

Bạn có thể điều hành một thư viện mà không cần tổ chức bên ngoài hoặc cơ sở dữ liệu trung tâm vận hành.

**Tại Sao Lại Gọi Là Blockchain**

Trong ví dụ về thư viện, mỗi khi một cuốn sách được mượn đi, một giao dịch sẽ được khởi tạo. Có rất nhiều giao dịch diễn ra cùng lúc, vì thế những giao dịch này sẽ được tập hợp lại rồi đưa vào một khối mới.

Khối mới này được đưa vào "phía trên" khối trước đó bằng cách thêm chỉ dẫn đến khối trước đó, liên kết chúng với nhau.

Chẳng hạn:

Khối 10 liên kết với khối 9

Khối 9 liên kết với khối 8

Khối 8 liên kết với khối 7 v.v…

Bằng cách liên kết các khối này lại với nhau, một chuỗi (chain) các khối (block) được tạo ra, vì thế có tên là "Blockchain". Mỗi khối mới đều chỉ dẫn tới khối trước đó, khối đó lại dẫn tới khối trước nữa, và cứ thế ngược về thời điểm bắt đầu.

Trong ví dụ thư viện, bất cứ ai cũng có thể tới khối mới nhất trong chuỗi. Họ có thể xem xét mọi cuốn sách đang được mượn và ai đang mượn. Sau đó, họ có thể quan sát các giao dịch trong khối

trước đó, xem ai đã mượn sách trước họ, cứ như thế ngược về khối khởi đầu xem ai là chủ sở hữu.

Không tồn tại tổ chức hoặc cơ sở dữ liệu trung tâm, nếu một người muốn thông báo họ là chủ sở hữu ban đầu của cuốn sách, ta có thể đi từ khối giao dịch mới nhất về khối giao dịch đầu tiên, còn gọi là "khối nguyên thủy".

**Thay Đổi Giao Dịch Và Khối Sau Khi Thêm**

Các khối được thêm vào chuỗi sẽ không thể bị can thiệp hoặc sửa đổi, các khối sẽ được bổ sung vĩnh viễn vào Blockchain. Vì mỗi khối liên kết với khối trước đó, nếu một ai đó muốn gian lận bằng cách thay đổi một giao dịch, họ sẽ phải thay đổi toàn bộ các khối trước và sau khối đó.

Mạng lưới Bitcoin ước tính rằng sau khi 6 khối được bổ sung vào trên một khối, sẽ không thể thay đổi bất kỳ một giao dịch nào trong khối đó vì không đủ công suất tính toán cần thiết để thực hiện thay đổi.

Nếu một giao dịch diễn ra trong khối số 10, thì ngay khi Blockchain đạt tới khối số 16, sẽ không thể thay đổi các giao dịch trong khối 10.

Số các khối trên của một giao dịch cũng có thể được coi là các xác nhận, một số công ty sẽ chờ đủ 6 xác nhận trước khi chấp thuận một thanh toán để đảm bảo rằng giao dịch trong Blockchain sẽ không bị thay đổi.

**Giao Dịch Lặp Chi**

Để hiểu một vấn đề khác mà Blockchain phải xử lý, hãy xem xét ví dụ thư viện trong hoàn cảnh ai đó muốn lợi dụng cơ chế thư viện chung bằng cách lấy trộm sách.

Mỗi khi một cuốn sách được mượn đi, một giao dịch chờ xử lý xuất hiện, giao dịch này được gửi tới mọi người trong mạng lưới để kiểm nhận và bổ sung vào Blockchain. Người tập hợp giao dịch đó với những giao dịch chờ xử lý khác rồi bổ sung một khối giao dịch hợp lệ vào chuỗi sẽ nhận được phần thưởng.

Khối giao dịch mới được bổ sung vào chuỗi nên cơ sở dữ liệu của mọi người được cập nhật một hồ sơ giao dịch.

Mọi người trong mạng lưới có thể thấy ai sở hữu mỗi khối và người họ mượn sách. Vì mọi người biết ai sở hữu mỗi khối, toàn bộ mạng lưới có thể thấy liệu có ai không trả sách hoặc tình huống đang diễn ra tại mọi thời điểm.

**Trao Đổi Giá Trị Trong Blockchain**

Chúng ta hãy thêm một yếu tố vào thư viện chung này, mỗi khi ai đó mượn một cuốn sách, họ trả cho người họ mượn sách một đồng "bookcoin".

Giả định rằng một người có thể chỉ cho người khác mượn sách để kiếm lợi nhuận, họ sẽ phải trả 1 bookcoin nếu mượn sách và nhận được 1 bookcoin khi cho mượn sách. Để kiếm lợi nhuận, họ sẽ cần cho mượn sách nhiều hơn số sách họ mượn.

Sam Lén Lút tham gia thư viện chung. Anh ta tham gia bất chấp các thành viên khác nghi ngờ rằng anh ta sẽ làm gì đó vụng trộm lén lút.

Dù sao thì, Sam Lén Lút vẫn đóng góp cuốn Romeo và Juliet vào thư viện, ai đó mượn cuốn sách này trong thư viện nên anh ta nhận được 1 bookcoin.

Vốn là một người hay vụng trộm, anh ta nảy ra kế hoạch thử nghiệm mượn nhiều sách hơn khả năng chi trả bookcoin của anh ta.

Sam Lén Lút mượn cuốn 1984 của David. Sau đó, Sam Lét Lút nhanh chóng đi mượn cuốn Hamlet của Sally.

Hai giao dịch đồng thời được tạo ra trong mạng lưới. Giao dịch đầu tiên được truyền tới mọi người trong mạng lưới để công nhận hành động cho mượn cuốn 1984 và rằng Sam Lén Lút phải trả 1 bookcoin cho David vì đã mượn cuốn đó.

Giao dịch này được mọi người trong mạng lưới chấp nhận là hợp lệ và họ thêm vào một khối mới, khối này cũng được bổ sung vào Blockchain:

Sam Lén Lút mượn 1984 từ David

Sam Lén Lút trả 1 bookcoin cho David

Sau khi giao dịch này thông qua, mạng lưới nhận được giao dịch tiếp theo cần công nhận:

Sam Lén Lút mượn Hamlet từ Sally

Sam Lén Lút trả 1 bookcoin cho Sally

Mạng lưới kiểm tra số dư bookcoin của Sam Lén Lút và phát hiện ra anh ta chỉ có 1 bookcoin, và anh ta đang cố gắng tạo ra bản sao chép đồng tiền này để thử đánh lừa mạng lưới.

Vì mạng lưới mở và mọi người đều có một bản hồ sơ, họ có thể truy nguyên toàn bộ giao dịch. Họ có thể thấy thời điểm nào Sam Lén Lút nhận được 1 bookcoin vì cho mượn sách của mình để số dư tài khoản bookcoin của anh ta bằng 1.

Anh ta không có 2 bookcoin để trả và mọi người trong mạng lưới có thể thấy rõ điều đó. Phần lớn mọi người trong mạng lưới đồng thuận rằng giao dịch này không hợp lệ. Họ không cho phép anh ta mượn cuốn sách thứ hai và hoạt động thanh toán này bị gắn nhãn

không hợp lệ. Giao dịch này bị từ chối và không được bổ sung vào Blockchain.

**Đồng Thuận Phân Tán**

Trong ví dụ kể trên, đại đa số thành viên trong mạng lưới cần đồng thuận rằng một giao dịch hợp lệ để giao dịch diễn ra, khái niệm này được gọi là Đồng Thuận Phân Tán.

Sẽ không có khả năng toàn bộ thành viên trong hệ thống đồng thuận vì sẽ có những người trong hệ thống cố gắng thực hiện giao dịch lặp chi, đánh lừa hệ thống bằng cách cố gắng công nhận giao dịch ảo hợp lệ.

Đối với nhiều Blockchain, ngưỡng đồng thuận là hơn 50%, nếu có trên 50% thành viên trong mạng lưới đồng thuận rằng một giao dịch hợp lệ, giao dịch đó được công nhận là hợp lệ.

Đây là cách thức thông thường mà Blockchain phi tập trung hoạt động để công nhận các giao dịch và quản lý mạng lưới. Thay vì một bộ phận chịu trách nhiệm công nhận toàn bộ các giao dịch và duy trì độ chính xác của cơ sở dữ liệu, nhiệm vụ này được chia sẻ với cả mạng lưới. Tất cả các thành viên kết nối với mạng lưới đều có quyền lên tiếng nhận định một giao dịch có nên được chấp nhận vào chuỗi hay không.

Rủi ro và nguy hiểm tiềm tàng khi hơn 50% thành viên trong mạng lưới chấp nhận một giao dịch không hợp lệ sẽ được thảo luận trong phần sau cuốn sách.

**Khai Thác**

Bạn có thể đã được nghe thuật ngữ "khai thác" khi thảo luận về Bitcoin và nhiều loại tiền ảo khác.

Các yêu cầu giao dịch được truyền tới mọi máy tính trong mạng lưới để kiểm nhận và gộp vào Blockchain.

Để kiểm nhận một giao dịch và đưa vào Blockchain, các máy tính trong mạng lưới phải giải được mảnh ghép liên quan đến khối kế tiếp để được đưa vào Blockchain.

Máy tính đầu tiên tìm ra đúng mảnh ghép có thể thêm một giao dịch vào một khối, sau đó thêm khối giao dịch đó vào Blockchain.

Vì xử lý thành công mảnh ghép trước tiên, họ nhận được một phần thưởng, thường được trả bằng tiền ảo hoặc mã xác nhận dùng trong mạng lưới đó.

Quá trình này được gọi là khai thác, vì giống như khai thác nhiều khoản giá trị nhỏ từ một khối.

**Bằng Chứng Xử Lý**

Những thợ đào (miner)[1] xử lý mảnh ghép và thêm khối hợp lệ vào mạng lưới được thưởng vì đóng góp vào công suất tính toán, điện năng và nhiều nguồn lực khác cho mạng lưới, từ đó giúp mạng lưới duy trì hoạt động.

*[1] Thợ đào (miner) là những người tham gia khai thác trong Blockchain.*

Mảnh ghép họ xử lý được gọi là Bằng Chứng Xử Lý. Đây là mảnh ghép toán học rất khó giải đáp nhưng rất dễ xác minh thành quả sau khi xử lý xong.

Hãy coi đó là khóa mật mã. Để thêm một khối mới vào chuỗi và nhận được phần thưởng, bạn phải tìm ra mật mã cho khóa.

Bạn chỉ có thể tìm ra mật mã cho khóa này bằng cách ước đoán các số. Mọi người trong mạng lưới phỏng đoán ngẫu nhiên số khóa

mật mã. Người đầu tiên tìm ra mã số sẽ nhận được một phần thưởng và có thể thêm một khối vào Blockchain.

Ngay khi mật mã của khóa được giải, những người khác trong mạng lưới có thể dễ dàng đưa mã số đó vào khóa để xác nhận rằng mã số mở được khóa.

Hành động này được coi là bằng chứng chứng tỏ rằng công suất tính toán, điện năng, thời gian và nguồn lực đã được đóng góp vào mạng lưới. Phần thưởng là một bù đắp cho giá trị đóng góp những nguồn lực trên vào hoạt động của Blockchain.

Bằng Chứng Xử Lý đòi hỏi công suất tính toán lớn và còn nhiều cách thức được sử dụng để vận hành Blockchain sẽ được thảo luận trong những phần sau.

**Tổng Kết Cách Thức Hoạt Động Của Blockchain**

Chúng ta đã thảo luận cách thức mạng Blockchain được sử dụng để thiết lập một cơ sở dữ liệu nhằm mục đích thay thế một thư viện hay một tổ chức trung tâm.

Đối với nhiều người, hiệu quả của việc thay thế một cơ sở dữ liệu thư viện có lẽ không quan trọng trong thời điểm hiện nay vì hầu hết mọi hoạt động đều là kỹ thuật số. Dù vậy, những cuốn sách cũng có thể được thay thế bằng gần như mọi loại giá trị khác.

Nếu chúng ta thay thế sách bằng quyền sở hữu tài sản trong ví dụ trên, chúng ta thấy quyền sở hữu một tài sản có thể được chuyển giao và quản lý thông qua Blockchain.

Khi quyền sở hữu một tài sản được chuyển giao, mọi người trong mạng lưới nhận được thông báo về việc chuyển giao tài sản đó, đại đa số thành viên mạng lưới đều công nhận việc chuyển giao

tài sản, nên hoạt động này được bổ sung vào Blockchain với tư cách một hồ sơ mà mọi người có thể xem xét.

Nếu chủ sở hữu tài sản cố bán quyền sở hữu tài sản cho hai người khác nhau, mọi thành viên trong mạng lưới sẽ thấy hoạt động chuyển giao nước đôi và một trong hai hoạt động chuyển giao sẽ bị mạng lưới từ chối.

Như đã đề cập trong chương trước, mạng lưới Blockchain sở hữu tiềm năng to lớn tại những quốc gia nơi mà các công ty, tổ chức ngân hàng và chính phủ không đáng tin cậy đồng thời thực hiện lưu trữ hồ sơ bằng tay hoặc không đảm bảo. Khi đó, khả năng thay thế các tổ chức và cơ sở dữ liệu trung tâm bằng mạng lưới Blockchain đối với hồ sơ tài sản có thể mang đến lợi ích to lớn cho người dân các quốc gia này.

Chúng ta đã nghiên cứu tổng thể cách thức công nghệ Blockchain hoạt động và xem xét một vài ví dụ ứng dụng của công nghệ này. Trong phần sau của cuốn sách, chúng ta sẽ tìm hiểu thêm nhiều ví dụ về các lĩnh vực mạng lưới Blockchain có thể thay thế cho các tổ chức và công nghệ hiện thời.

**Điểm Cốt Lõi:**

• Khi một giao dịch được xử lý và công nhận là hợp lệ, nó sẽ được tập hợp lại với những giao dịch khác rồi được bổ sung vào khối mới.

• Khối mới này được thêm vào trên khối trước đó trong chuỗi. Mỗi khối dựa vào số khối trước đó, liên kết với nhau thành một chuỗi, vì thế thuật ngữ "Blockchain" ra đời.

• Một chuỗi các khối trong Blockchain liên kết với nhau ngược trở về đến khối đầu tiên trong chuỗi, khối này được gọi là "khối

nguyên thủy".

• Đối với Blockchain phi tập trung, mỗi khối giao dịch trên Blockchain được mạng lưới kiểm nhận. Mọi thành viên trong mạng lưới nhận được thông tin về giao dịch trên mạng lưới, mạng lưới không bị một cơ sở dữ liệu trung tâm thuộc quyền sở hữu của một công ty hay tổ chức nào điều hành.

• Ngay khi một khối các giao dịch được thêm vào Blockchain, rất khó để thay đổi. Mỗi khối đưa vào phía trên khối trước đó là một xác nhận giao dịch không đổi. Càng nhiều khối được đưa vào, càng khó thay đổi cho đến khi không thể thay đổi được nữa. Trong mạng lưới Bitcoin, 6 khối được coi là một xác nhận giao dịch sẽ không được thay đổi.

• Đối với đồng thuận phân tán, phần lớn các máy tính trong mạng lưới cần chấp nhận rằng một giao dịch là hợp lệ trước khi nó được đưa vào Blockchain.

• Giao dịch lặp chi xảy ra khi một người trong mạng lưới cố gắng thực hiện hai giao dịch cùng một lúc. Thông thường, trường hợp này diễn ra khi gửi nhiều hơn một giao dịch trước khi một trong số các giao dịch đó được xác thực và chấp nhận trên Blockchain.

• Tấn công giao dịch lặp chi xảy ra khi một người dùng kiểm soát hơn 50% số máy tính trong mạng lưới. Điều này cho phép người dùng nhân đôi việc truyền gửi giao dịch bằng cách kiểm soát giao dịch nào được chấp nhận và giao dịch nào bị từ chối.

• Khai thác là quá trình kiểm nhận giao dịch rồi đưa vào khối mới trong Blockchain. Những phần thưởng nhỏ sẽ được trao tặng khi mỗi khối mới được đưa vào chuỗi, tương tự như khai thác một phần thưởng nhỏ từ khối lớn.

• Bằng Chứng Xử Lý liên quan đến hoạt động tìm ra mảnh ghép tính toán để bổ sung khối mới vào Blockchain. Tìm ra rất khó nhưng chứng thực rất dễ, giống như trường hợp khóa mật mã. Hoạt động này cung cấp bằng chứng rằng công suất tính toán cũng như nhiều nguồn lực đã được sử dụng và đóng góp cho mạng lưới.

# Chương 3
# Lịch sử Blockchain và Bitcoin

*"Tôi tin rằng thực tế một thuật toán trong hệ thống Bitcoin thay thế được chức năng của [chính phủ]… thật sự tuyệt vời. Tôi rất hâm mộ Bitcoin."*

**- Al Gore,** Phó Tổng thống Mỹ thứ 45

Blockchain lần đầu tiên được đề cập đến trong mã nguyên thủy cho Bitcoin. Dù hiện nay có sự phân tách giữa công nghệ Blockchain và Bitcoin, lịch sử của Blockchain lại liên quan mật thiết tới lịch sử hình thành Bitcoin. Vì thế, chúng ta sẽ thảo luận về quá trình hình thành liên quan lẫn nhau này.

Mật mã học là nền tảng cốt lõi của Blockchain. Mật mã học đã trải qua quá trình lịch sử lâu dài cũng như được sử dụng để bảo vệ những thông điệp và bí mật từ hàng ngàn năm trước. Một ví dụ rất nổi tiếng về mật mã học cổ đại là bản "Mật mã Caesar" (hay còn gọi là Mật Mã Dịch Chuyển) được Julius Caesar sử dụng khi phải gửi đi những thông tin nhạy cảm.

Mật mã Caesar quy ước thay mỗi ký tự trong thông điệp bằng một ký tự khác trong bảng chữ cái sao cho ký tự thay thế và ký tự được thay thế cách nhau một số ký tự định trước. Ví dụ, tất cả các ký tự có thể lệch đi 3 ký tự, khi đó A thay bằng D, B thay bằng E, C thay bằng F, và tương tự như thế cho đến khi mọi ký tự trong thông điệp đều được mã hóa.

Chỉ người biết số ký tự lệch nhau mới có thể đọc được thông điệp dễ dàng.

Trình độ đọc hiểu khi đó vẫn còn kém và có rất nhiều ngôn ngữ được sử dụng trên thế giới, vì thế kẻ thù dù lấy được thông điệp cũng không thể đọc được hoặc nghĩ rằng bức thư được viết bằng ngoại ngữ. Đó là phương thức mã hóa mà ngày nay có thể giải mã dễ dàng, tuy nhiên đủ hiệu quả để che giấu thông tin và gây khó khăn giải mã trong thời điểm đó.

Mật mã học hiện đại đã có bước tiến dài dù nền tảng cơ bản vẫn tương tự như vậy. Thông điệp và dữ liệu được mã hóa bằng cách thay thế ký tự và chữ số, vì thế thông điệp ban đầu sẽ không thể đọc được trừ khi một người có phương thức hoặc mã bí mật để giải mã.

Tới mật mã học trong công nghệ Blockchain, nhiều nghiên cứu vào giữa những năm 1980 và 1990 đã chỉ ra rằng có thể bảo toàn dữ liệu thông qua quá trình mã hóa, đồng thời kết nối chặt chẽ dữ liệu đó vào chuỗi cùng với các đề xuất lưu hành đồng tiền ảo.

Năm 1982, David Chaum viết một bài nghiên cứu có nhan đề Blind Signatures for Untraceable Payments (tạm dịch: Chữ ký mù cho những giao dịch không thể dò ra), David Chaum được vinh danh là nhà phát minh tiền ảo và chữ ký mù nhờ bài viết này. Chữ ký mù ẩn nội dung thông điệp trước khi được ký, chữ ký số có thể được xác thực với chữ ký gốc tuy nhiên nội dung vẫn được ẩn, đây là phiên bản sơ khai của chữ ký mã hóa dùng cho đồng tiền ảo.

Bài luận này và bài tiếp sau mà David Chaum xuất bản cho rằng, người dùng có thể sở hữu và chi tiêu tiền ảo theo cách mà các ngân hàng và tổ chức khác không thể lần ra dấu vết. David Chaum cùng với Amos Fiat và Moni Naor còn đề xuất rằng, các giao dịch ngoại

tuyến kèm chữ ký sẽ có khả năng phát hiện liệu khoản tiền mặt trước đó đã được chi tiêu hay chưa, một giải pháp khả thi cho vấn đề giao dịch lặp chi.

Năm 1990, David thành lập DigiCash để sáng tạo ra một loại tiền ảo dựa trên ý tưởng trong các bài viết của ông và đến năm 1994, khoản chi điện tử đầu tiên của DigiCash được gửi đi. Mở đầu thông cáo báo chí của DigiCash năm 1994 như sau:

"Thanh toán bằng tiền ảo qua mạng máy tính đầu tiên trên thế giới. (Ngày phát hành: 27 tháng 05 năm 1994).

Tiền ảo có đặc tính nặc danh của tiền giấy, nhưng lại đạt đến độ bảo mật cao cần thiết cho các hoạt động mạng điện tử xuyên suốt những bước tiến trong công nghệ mật mã hóa khóa công khai."

Thông cáo báo chí này ra đời trước khi Bitcoin xuất hiện 14 năm nhưng nếu bạn thay từ "tiền ảo" bằng "Bitcoin", bạn có thể nhận được bản thông cáo báo chí dành cho Bitcoin.

DigiCash tạo ra hệ thống tiền ảo đầu tiên không thể bị các ngân hàng, chính phủ hoặc các tổ chức khác truy nguyên. Hệ thống này sử dụng khóa mật mã, khóa cá nhân và khóa công khai để ẩn nội dung thông điệp theo cách rất giống hệ thống tiền ảo sử dụng hiện nay.

DigiCash có lẽ đã vượt quá xa so với thời đại vì vào năm 1994 hầu hết mọi người còn không biết về mạng Internet. DigiCash tuyên bố phá sản vào năm 1998 và tài sản bị bán cho công ty công nghệ eCash, một công ty khác chuyên về tiền ảo.

Vào những ngày đầu của mạng Internet, thư quảng cáo tràn lan đã trở thành một vấn nạn mà không ai tìm ra giải pháp xử lý. Năm 1997, Adam Back đề xuất một hệ thống hạn chế thư quảng cáo

cùng với phương thức tấn công từ chối dịch vụ bằng cách sử dụng một thuật toán Bằng Chứng Xử Lý được biết đến với tên gọi Hashcash.

Thuật toán Bằng Chứng Xử Lý yêu cầu hệ thống gửi một thư điện tử xử lý một mảnh ghép tính toán, sau đó đưa đáp án vào tiêu đề thư điện tử. Hoạt động này đòi hỏi người gửi phải sử dụng công suất tính toán và nhiều nguồn lực để gửi thư điện tử, từ đó gây khó khăn trong việc gửi tràn lan thư quảng cáo. Mảnh ghép này rất khó giải đối với người gửi nhưng rất dễ để người nhận xác định xem đáp án đúng hay sai, đồng thời lọc các thư quảng cáo không thỏa mãn thuật toán Bằng Chứng Xử Lý này.

Năm 1998, Nick Szabo, đề xuất một loại tiền ảo phi tập trung gọi là Bit Gold. Trong đề xuất về Bit Gold, mọi người sẽ định phần cách thức tính toán để giải các mảnh ghép mật mã. Đa phần thành viên mạng lưới sẽ phải nhận định lời giải có hợp lệ hay không trước khi chuyển sang mảnh ghép tiếp theo. Ngay khi một mảnh ghép được giải và được mạng lưới chấp thuận, nó sẽ trở thành một phần của mảnh ghép tiếp theo để mạng lưới xử lý. Mảnh ghép được ghi nhãn thời gian và, vì mỗi câu trả lời trở thành một phần của mảnh ghép tiếp theo, chúng liên kết lại với nhau thành một chuỗi.

Nick Szabo nhận định rằng, tại thời điểm đó, đồng tiền ảo đối mặt với vấn nạn giao dịch lặp chi vì chúng có thể bị sao chép và tái tạo nếu không trao quyền kiểm soát cho các tổ chức hoặc ngân hàng trung tâm. Công việc với Bit Gold của ông là nỗ lực giải quyết tình trạng giao dịch lặp chi gắn với loại tiền ảo phi tập trung này.

Bit Gold không bao giờ trở thành một đồng tiền chân chính và chỉ tồn tại trong lý thuyết, dù vậy nó được coi là đã cung cấp những

điều kiện thuận lợi để sau này công nghệ Blockchain và Bitcoin ra đời.

Vào năm 1998, Wei Dai xuất bản một bài viết nhan đề B-money, an Anonymous, Distributed Electronic Cash System (tạm dịch: Đồng B, một hệ thống tiền ảo phân tán ẩn danh). Bài viết đã thảo ra những nền tảng cho tiền kỹ thuật số, bao gồm Bitcoin; sau này, bài viết được Satoshi Nakamoto nhắc đến trong bài về Bitcoin.

Trong bài viết của Wei Dai, ông tuyên bố rằng hệ thống tiền ảo cần những chức năng dưới đây:

• Một lượng lớn hoạt động tính toán và bằng chứng của hoạt động đó.

• Phần thưởng được phân chia cho hoạt động tính toán đã hoàn thành.

• Sổ cái nhóm tập thể được tất cả các thành viên xác thực và cập nhật.

• Các khoản chuyển giao quỹ được hoàn thiện trong sổ cái nhóm tập thể và xác thực bằng Mã hóa sử dụng hàm băm.

• Mọi chuyển giao được xác nhận bằng chữ ký điện tử sử dụng mật mã hóa khóa công khai và được mạng lưới xác minh.

Năm 2000, Stephan Konst công bố chuyên đề trình bày giải pháp thực tiễn để xử lý các chuỗi an toàn mã hóa.

Cùng với nhiều chuyên đề học thuật được xuất bản, tác phẩm này đã đặt nền móng cho Bitcoin và Blockchain trong suốt những năm 1980 tới những năm 2000.

Vào năm 2008, Satoshi Nakamoto (thường được coi là bút danh của tác giả) đăng một bài luận trên mạng Internet có nhan đề Bitcoin: A peer-to-peer Electronic Cash System (tạm dịch: Bitcoin:

Hệ thống tiền ảo mô hình ngang cấp). Bài viết này đưa ra kiến thức tổng quan về sự hình thành Bitcoin và khối các giao dịch kết nối trong chuỗi. Bài viết không sử dụng trực tiếp thuật ngữ "Blockchain" khi đề cập đến phương thức này.

Năm 2009, Bitcoin vượt ra khỏi khuôn khổ một ý tưởng trên văn bản học thuật khi Satoshi Nakamoto thiết lập mạng lưới Bitcoin cùng với

Blockchain đầu tiên. Blockchain lần đầu tiên được đề cập đến với cụm từ rời rạc "Blockchain" trong mã nguồn nguyên thủy cho Bitcoin.

Blockchain đầu tiên này là đặc điểm cốt lõi của Bitcoin, ngăn chặn được tình trạng giao dịch lặp chi và hoạt động với vai trò sổ cái công khai phân tán cho tất cả các giao dịch trên mạng lưới Bitcoin.

Nakamoto được công nhận là người đầu tiên khai thác khối đầu tiên trên mạng lưới Bitcoin, hay còn gọi là "khối nguyên thủy".

Trong "Khối Nguyên Thủy", Satoshi Nakamoto để lại một thông điệp: "Tờ Times, ngày 03/01/2009, Đại Pháp Quan đứng bên bờ vực phải viện trợ ngân hàng lần thứ hai".

Thông điệp này được lưu lại như bằng chứng rằng ngày khối được khởi tạo là vào ngày mùng ba tháng Một hoặc sau đó đồng thời đưa ra nhận định về sự thất bại trong cấu trúc hiện tại của ngân hàng và thị trường tiền tệ. Vì đây là tiêu đề trên một tờ báo của Vương quốc Anh nên rất có khả năng Satoshi sinh sống tại Anh vào thời điểm đó.

Những từ "block" (khối) và "chain" (chuỗi) được sử dụng riêng biệt với Bitcoin và ngay cả khi chúng có liên quan đến nhau. Mãi đến nhiều năm sau thuật ngữ Blockchain mới hình thành.

Blockchain Bitcoin nguyên thủy không phải không có lỗi. Tương tự hầu hết các dự án kinh doanh và công nghệ tầm cỡ, luôn tồn tại nhiều vấn đề trong quá trình phát triển dự án. Suốt tháng Tám năm 2010, vấn đề nghiêm trọng đầu tiên trong các giao thức của Bitcoin được phát hiện. Các giao dịch bị thay đổi trước khi chúng được ghi vào Blockchain, giả mạo các giao dịch chính thức. Vì lý do nào đó, nhiều người tránh được những hạn định sẵn có trong Bitcoin và tạo được một số vô hạn bằng cách sửa đổi các giao dịch nguyên bản rồi biển thủ.

Lỗ hổng này trong hệ thống đã bị lợi dụng và có tới hơn 184 tỷ bitcoin được sinh ra từ một giao dịch rồi gửi tới đúng hai địa chỉ trên mạng lưới. Trong vòng vài giờ, giao dịch đã bị phát hiện và xóa bỏ khỏi mạng lưới. Mạng Bitcoin trải qua quá trình cập nhật sửa chữa toàn diện, và kể từ đó tới nay, vấn đề như vậy không xảy ra được nữa.

Vào năm 2011, một thị trường ma túy mang tên Silk Road hình thành, cũng như trang thương mại điện tử eBay, thị trường này cho phép người dùng mua bán ma túy trực tuyến. Bitcoin được sử dụng làm hình thức thanh toán chính cho Silk Road; điều này mặc dù giúp làm tăng giá trị sử dụng của Bitcoin nhưng lại khiến Bitcoin dính vào các hoạt động phi pháp và buôn bán ma túy.

Bitcoin dần dần trở nên phổ biến và được công chúng chú ý; vào năm 2013, Bitcoin đạt đỉnh điểm khoảng 1.000 đô la và không ngừng tăng bất chấp nhiều chỉ trích từ yêu cầu luật pháp và chính quyền.

Sau đó vào năm 2013, Silk Road bị FBI đóng cửa và phong tỏa toàn bộ tài sản, kẻ chủ mưu bị bắt giữ và đối mặt với án tù chung

thân. Vào khoảng thời gian đó, sàn giao dịch Bitcoin lớn nhất Mt. Gox, chiếm tới 70% toàn bộ giao dịch Bitcoin, nhận được lệnh bắt và giấy phạt, đồng thời đối mặt với các vấn đề về luật định từ nhiều cơ quan chính phủ Mỹ. Cuối năm 2013, Mt. Gox buộc phải ngừng cho rút tiền và tuyên bố phá sản vào đầu năm 2014.

Những đồng tiền ảo khác đã bắt đầu xuất hiện cũng dựa trên mã nguồn của Bitcoin nhưng sử dụng Blockchain khác. Litecoin tách ra từ Blockchain Bitcoin nguyên bản với vai trò một nhánh trong Blockchain, sau đó trở thành Blockchain và đồng tiền ảo riêng biệt với thời gian bổ sung khối vào Blockchain ngắn hơn cùng với nhiều thay đổi khác. Một khối được thêm vào Blockchain Bitcoin tốn khoảng 10 phút, còn Litcoin thêm khối vào chuỗi khoảng 2 phút rưỡi.

Sau khi Mt. Gox và Silk Road bị đóng cửa, Bitcoin rơi từ đỉnh điểm 1.000 đô la xuống còn khoảng 200 đô. Những đồng tiền ảo khác ra đời và nhiều người công khai tuyên bố rằng Bitcoin đã sụp đổ.

Tuy nhiên, Bitcoin còn lâu mới sụp đổ. Trên thực tế, vì Silk Road đóng cửa, Bitcoin đã bớt dính dáng đến tội phạm và buôn bán ma túy hơn, vì thế các công ty bắt đầu quan tâm tới công nghệ của Bitcoin.

Để các công ty, ngân hàng và tổ chức tài chính lớn nghiêm túc nhìn nhận Bitcoin vẫn còn rất khó khăn vì họ khó mà quên được sự thất bại của Mt. Gox, buôn bán ma túy và những vụ thuê người ám sát bằng Bitcoin. Mặc dù không có tội ác phát sinh do Bitcoin, nhưng nhiều người vẫn cho rằng Bitcoin là tiền giả, trào lưu nhất thời, bong bóng tiền tệ tài chính hoặc một mưu đồ bất lương.

Cái tên Bitcoin vẫn gặp rất nhiều ý kiến tiêu cực mặc dù thuật ngữ "Blockchain" đã trở thành một từ quan trọng thường được nhắc tới khi bàn luận về công nghệ. Từ Blockchain được sử dụng riêng biệt với công nghệ của đồng tiền ảo Bitcoin hoặc mạng lưới Bitcoin. Các nhà đầu tư và các tổ chức tài chính không quan tâm đến Bitcoin, nhưng họ bắt đầu chú ý tới công nghệ Blockchain.

Giá trị của Bitcoin, cùng với mức độ quan tâm tới Bitcoin, suy giảm vào năm 2014; tuy nhiên, sự chú ý tới Blockchain lại tăng nhanh. Blockchain bắt đầu được sử dụng khi nhắc tới cơ sở dữ liệu hoặc sổ cái phân tán thay vì tiền tệ. Người ta đề xuất thay thế những cuốn sổ cái ghi chép dữ liệu thủ công và lỗi thời bằng Blockchain.

Năm 2015, Blockchain động Ethereum ra đời. Sự kiện này đã đưa tiềm năng của công nghệ Blockchain lên tầm cao mới. Mạng lưới Ethereum cho phép các ứng dụng phi tập trung chạy trên một Blockchain cùng với giao thức hợp đồng thông minh. Các hợp đồng thông minh và những ứng dụng phi tập trung được nhiều người nhận định là tương lai của công nghệ Blockchain, thường được gọi là Blockchain 2.0.

Đa phần các công ty dịch vụ tài chính và ngân hàng trên thế giới đều phát triển hệ thống xây dựng dựa trên nền tảng Blockchain để thay thế cho các mạng lưới hoặc cơ sở dữ liệu vốn có. Nhờ truy cập dễ dàng và khả năng cho phép các ứng dụng phi tập trung phối hợp với hợp đồng thông minh, công nghệ Blockchain đã được khai mở tới hầu hết các lĩnh vực công nghiệp. Các lập trình viên đã có thể xây dựng phần mềm hoạt động trên Blockchain mà không cần khởi tạo Blockchain của riêng họ.

Đến năm 2017, Tạp chí Kinh doanh Harvard tuyên bố Blockchain có tiềm năng tạo nên những cơ sở mới trong hệ thống kinh tế và xã hội. Nhận định này dường như hé lộ sự phát triển Blockchain sẽ mở ra như thế nào đồng thời gợi nhớ tới mạng Internet vào thời kỳ sơ khai với vô vàn tiềm năng chỉ vừa mới được khai phá. Nhiều công ty lớn, công ty khởi nghiệp, các nhà tư bản mạo hiểm, cơ quan chính phủ và các lập trình viên đều làm việc trên các ứng dụng phi tập trung, cơ sở dữ liệu và hệ thống xây dựng dựa trên Blockchain.

Đến lúc này, bạn đã có hiểu biết cơ bản về khái niệm và lịch sử phát triển của Blockchain. Trong chương tiếp theo, chúng ta sẽ thảo luận về ưu thế, bất lợi, rủi ro và tiềm năng tương lai của công nghệ Blockchain.

**Điểm Cốt Lõi:**

• Mật mã học là nền tảng của Blockchain. Mật mã học đã có từ hàng ngàn năm khi các thông điệp được mã hóa để bảo vệ nội dung khỏi kẻ thù.

• Nhiều chuyên đề được xuất bản suốt những năm 1980 và 1990 đã phát triển cách ứng dụng mật mã học kết hợp với chuỗi dữ liệu an toàn và sự ra đời của tiền ảo.

• Năm 1982, David Chaum viết bài nghiên cứu có nhan đề Blind Signatures for Untraceable Payments và sau đó được công nhận là nhà sáng chế tiền ảo và chữ ký mù.

• Năm 1990, David sáng lập DigiCash tạo nên một loại tiền ảo không thể truy dấu ứng dụng mật mã học, khóa công khai, khóa cá nhân kèm chữ ký. DigiCash tuyên bố phá sản vào năm 1998 và tài sản bị bán cho công ty công nghệ eCash.

• Năm 1997, Adam Back sáng tạo thuật toán Bằng Chứng Xử Lý để giới hạn thư điện tử quảng cáo tràn lan, thuật toán này được biết đến với tên Hashcash. Thuật toán yêu cầu người gửi thư điện tử phải chứng thực họ đã giải được một mảnh ghép tính toán trước khi gửi thư. Nhiệm vụ này cần đến nhiều nguồn lực và công suất tính toán, khiến việc gửi thư điện tử quảng cáo tràn lan trở nên đắt đỏ hơn.

• Năm 1998, Nick Szabo đề xuất một loại tiền ảo phi tập trung có tên Bit Gold. Loại tiền này kết hợp chặt chẽ với thuật toán Bằng Chứng Xử Lý cùng một mạng máy tính chấp nhận các bằng chứng xử lý hợp lệ rồi tích hợp vào mảnh ghép gắn nhãn thời gian tiếp sau. Nhưng Bit Gold không bao giờ trở thành đồng tiền chân chính, nó chỉ tồn tại trên lý thuyết mà thôi.

• Năm 1998, Wei Dai xuất bản bài viết nhan đề B-money, an Anonymus, Distributed Electronic Cash System. Bài viết đã đưa ra những nền tảng cho đồng tiền kỹ thuật số, bao gồm Bitcoin, và sau này được nhắc đến trong chuyên đề về Bitcoin của Satoshi Nakamoto.

• Cùng với nhiều chuyên đề học thuật được xuất bản, tác phẩm này đã đặt nền móng cho Bitcoin và Blockchain trong suốt những năm 1980 tới những năm 2000.

• Năm 2008, Satoshi Nakamoto (thường được coi là bút danh của tác giả) đăng một bài luận trên mạng Internet có nhan đề Bitcoin: A Peer-to-peer Electronic Cash System. Bài viết này đưa ra kiến thức tổng quan về sự hình thành Bitcoin và khối các giao dịch kết nối trong chuỗi.

Bài viết không sử dụng trực tiếp thuật ngữ "Blockchain" khi đề cập đến phương thức này.

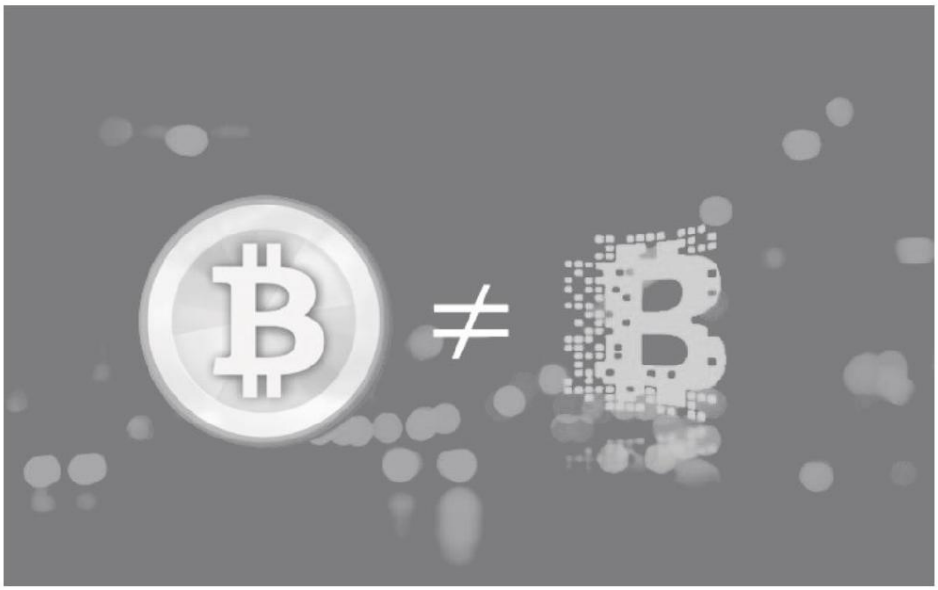
• Năm 2009, Bitcoin vượt ra khỏi khuôn khổ một ý tưởng trên văn bản học thuật khi Satoshi Nakamoto sáng tạo mạng lưới Bitcoin cùng Blockchain đầu tiên. Blockchain lần đầu tiên được đề cập đến với cụm từ rời rạc "Blockchain" trong mã nguồn nguyên thủy cho Bitcoin.

• Blockchain đầu tiên này là đặc điểm cốt lõi của Bitcoin, ngăn chặn được tình trạng giao dịch lặp chi và hoạt động với vai trò sổ cái công khai phân tán cho tất cả các giao dịch trên mạng lưới Bitcoin.

• Nakamoto được công nhận là người đầu tiên khai thác khối đầu tiên trên mạng lưới Bitcoin, hay còn gọi là "khối nguyên thủy", kèm một thông điệp: "Tờ Times ngày 03/01/2009, Đại Pháp Quan đứng bên bờ vực phải viện trợ ngân hàng lần thứ hai". Thông điệp này được lưu lại như bằng chứng về ngày khối được khởi tạo là vào ngày mùng ba tháng Một hoặc sau đó, đồng thời đưa ra nhận định về sự thất bại trong cấu trúc hiện tại của ngân hàng và thị trường tiền tệ.

• Người sáng tạo Bitcoin và Blockchain, Satoshi Nakamoto, vẫn còn là một ẩn số. Nhiều người hoài nghi rằng Nick Szabo hay Wei Dai chính là người sáng lập Bitcoin, tuy nhiên cả hai đều phủ nhận điều này.

• Năm 2015, Blockchain Ethereum ra đời, cho phép các ứng dụng phi tập trung và hợp đồng thông minh hoạt động trên Blockchain. Sự kiện này đã nâng tầm công nghệ Blockchain lên và được gọi là Blockchain 2.0.



# Chương 4
# Lợi ích của công nghệ Blockchain

*"Công nghệ Blockchain có khả năng tối ưu hóa cơ sở hạ tầng toàn cầu để giải quyết các vấn đề quốc tế hiệu quả hơn nhiều các hệ thống hiện hành trong bối cảnh hiện nay."*

**- Marwan Forzley,** Nhà sáng lập Align Commerce

Trong các chương trước, chúng ta đã bàn luận về khái niệm Blockchain, cách thức Blockchain hoạt động và ví dụ một số tiềm năng. Dù rằng một số lợi ích đã được giới thiệu ngắn gọn trong các chương trước nhưng trong chương này, chúng ta sẽ đi sâu vào chi tiết về những lợi ích của công nghệ Blockchain.

**Tính Minh Bạch**

Các hệ thống xây dựng dựa trên nền tảng Blockchain cung cấp nhiều bước tiến về tính minh bạch hơn nhiều so với sổ cái và cách lưu trữ hồ sơ hiện hành. Những thay đổi này cho phép mọi người trong mạng lưới có thể xem xét sổ cái và, ngay khi nhập vào Blockchain, các giao dịch không thể bị sửa đổi hay xóa bỏ.

Với cách thức ghi chép hồ sơ hiện tại, một người có thể thay đổi cơ sở dữ liệu rồi che giấu sự thay đổi với mọi người. Có vô số trường hợp lừa đảo quy mô lớn nhưng không bị phát hiện vì sổ cái không minh bạch. Tình trạng thiếu minh bạch này cho phép mọi người thay đổi thông tin đầu vào hoặc ngụy tạo dữ liệu mà người khác không biết.

Công nghệ xây dựng dựa trên nền tảng Blockchain cung cấp sự rõ ràng tới toàn bộ mọi người trong mạng lưới, nhờ các giao dịch được thông báo tới mọi máy tính kết nối trong mạng lưới. Đa số các máy tính được liên kết trong Blockchain phải chấp nhận giao dịch hoặc sự thay đổi ở Blockchain, vì thế tránh được tình trạng che giấu hoặc ngụy tạo giao dịch.

Tất cả các thay đổi đều thuộc quá trình xử lý dữ liệu gần sát thời gian thực, quá trình này diễn ra khi các giao dịch được xác nhận và bổ sung vào Blockchain. Trường hợp một người trong tổ chức trộm cắp tiền hoặc che giấu các khoản thua lỗ của công ty bằng cách ngụy tạo dữ liệu nhập vào sổ cái hiếm khi xảy ra trong sổ cái phân tán xây dựng trên nền tảng Blockchain.

Blockchain trong các ngành công nghiệp khác nhau sẽ cung cấp tính minh bạch trên khắp các phạm trù. Với một giao dịch tài chính, bạn có thể quan sát trạng thái chuyển giao trên Blockchain theo thời gian thực, thay vì không biết tình trạng giao dịch như thế nào cho đến khi giao dịch kết thúc, một vấn đề thường xảy ra trong các hệ thống hiện hành.

Tính minh bạch không đổi khi áp dụng với mọi giá trị được ghi trên Blockchain. Trong các chương sau, chúng ta sẽ nghiên cứu các ngành công nghiệp khác nhau nơi công nghệ Blockchain được phát triển và tính minh bạch công nghệ này tạo ra cho người tiêu dùng và doanh nhân khi so sánh với các hệ thống hiện hành.

**Loại Bỏ Đơn Vị Trung Gian**

Như đã thảo luận trong phần đầu cuốn sách, hầu hết các giao dịch ngày nay giữa mọi người đều cần một trung gian, chẳng hạn như ngân hàng, để đảm bảo độ tin cậy và an toàn cho giao dịch.

Một lợi thế của công nghệ Blockchain so với các hệ thống hiện hành là khả năng xóa bỏ các đơn vị trung gian bằng cách cho phép mọi người giao dịch trực tiếp với nhau thay vì qua một bên thứ ba nào đó.

Điều này giúp ích cho hàng tỷ người đang phải sống ở những quốc gia mà họ không thể đặt lòng tin vào các đơn vị trung gian vì chính quyền mục nát, tỷ lệ tội phạm cao, điều lệ doanh nghiệp lỏng lẻo, hoạt động lưu trữ hồ sơ thủ công hoặc các phương án lựa chọn hợp pháp rất hạn chế.

Blockchain đặc biệt hữu dụng trong những trường hợp khi mà niềm tin vào các đơn vị trung gian không tồn tại và hoạt động giao dịch trực tiếp giữa mọi người quá khó khăn hoặc rủi ro cao.

Blockchain cung cấp niềm tin và tính minh bạch, đồng thời giảm thiểu rủi ro khi giao dịch mà không cần bên thứ ba đóng vai trò trung gian giao dịch.

**Phi Tập Trung**

Đặc điểm phi tập trung trong một cơ sở dữ liệu Blockchain là lý do then chốt giải thích cách thức chuỗi loại bỏ vai trò của các đơn vị trung gian đồng thời tăng cường tính minh bạch và độ tin cậy như thế nào. Các Blockchain được lưu giữ trong một sổ cái chung, thay vì nhiều sổ cái riêng do các tổ chức khác nhau quản lý. Các cá nhân và công ty không phải trao quyền cho một tổ chức đơn lẻ nào khi sử dụng Blockchain.

Điều này giúp quản lý sự cộng tác giữa các bên nhanh chóng và dễ dàng hơn.

Ví dụ, một nhóm các ngân hàng chuyển giao tài sản cho nhau, với cấu trúc và hệ thống hiện hành, mỗi ngân hàng sẽ giữ một sổ cái

và hồ sơ giao dịch riêng. Khi sử dụng sổ cái dựa trên nền tảng Blockchain, họ sẽ chỉ cần thống nhất giao dịch trên một sổ cái chung mà tất cả các ngân hàng thành viên có thể truy cập và chấp thuận đó là hồ sơ giao dịch chính xác.

Cấu trúc phi tập trung của Blockchain là một lợi thế đối với các công ty cạnh tranh lẫn nhau nhưng lại cùng là thành viên của một nhóm công nghiệp hoặc tập đoàn. Một công ty có thể lo sợ khi chuyển giao dữ liệu hoặc phối hợp trên một cơ sở dữ liệu mà đối thủ cạnh tranh sở hữu. Khi các đối thủ cạnh tranh cộng tác với nhau, sẽ có một bên nắm giữ toàn bộ dữ liệu liên quan đến các hợp đồng pháp lý dài dòng và các thỏa thuận bí mật để bảo vệ sự riêng tư và khả năng truy nhập dữ liệu. Tuy nhiên, với hệ thống xây dựng dựa trên nền tảng Blockchain, các công ty đối thủ cạnh tranh có thể cùng làm việc trên một cơ sở dữ liệu chung mà họ có toàn quyền truy cập và kiểm soát.

Cơ sở dữ liệu tập trung dễ bị tấn công, mất mát và sai hỏng dữ liệu. Blockchain không có cơ sở dữ liệu trung tâm nơi dễ xảy ra hỏng hóc, ngụy tạo hoặc sai lệch dữ liệu. Toàn bộ máy tính trong mạng lưới Blockchain đều có một phiên bản sao lưu Blockchain, giúp giảm thiểu nguy cơ thất thoát dữ liệu. Để có thể ngụy tạo dữ liệu trên Blockchain cần phải xâm nhập đồng thời hơn 50% số máy tính trong mạng lưới, điều này gần như không thể thực hiện được.

**Niềm Tin**

Như đã đề cập đến trong phần trước, các phương thức giao dịch hiện hành giữa mọi người cần tới lòng tin vào đơn vị trung gian để quá trình diễn ra thuận lợi.

Blockchain cho phép loại bỏ các đơn vị trung gian nhưng vẫn duy trì sự tin tưởng và độ bảo mật giữa mọi người tham gia giao dịch.

Niềm tin được đặt vào mạng lưới Blockchain thay vì vào bên thứ ba. Mạng Blockchain thường phân tán, nên tất cả các thành viên trong mạng đều có thể truy cập vào Blockchain.

Cấu trúc phi tập trung với tính minh bạch được tăng cường và khả năng loại bỏ được bên thứ ba của Blockchain đã được thảo luận trên đây. Blockchain còn gia tăng niềm tin giữa các đối tượng trong một giao dịch, đây là lợi ích quan trọng trong tất cả những thay đổi.

**Độ Bảo Mật**

Dữ liệu khi đã được đưa vào Blockchain sẽ bất khả sửa đổi, tức là không thể thay đổi hoặc chỉnh sửa. Mọi khối dữ liệu trên Blockchain đều có thể được truy ngược về "khối nguyên thủy", tức khối đầu tiên.

Tính bất khả sửa đổi của dữ liệu đầu vào cùng với các khối kết nối dẫn về khối nguyên thủy trên Blockchain đã giúp việc lần theo lịch sử hoạt động của từng giao dịch trên Blockchain dễ dàng hơn.

Trong suốt chiều dài lịch sử, có vô số trường hợp lừa đảo và ngụy tạo dữ liệu. Thông thường, khi xảy ra lừa đảo, để tìm ra dấu vết vụ gian lận rất khó khăn và tốn thời gian. Lịch sử dữ liệu có thể bị thay đổi nhiều đến mức không thể tìm ra các giao dịch và các vụ lừa đảo.

Với hệ thống xây dựng dựa trên công nghệ Blockchain, các giao dịch trong quá khứ không thể bị thay đổi nên để lại lịch sử hoạt động trong Blockchain rất rõ ràng. Như đã đề cập trong mục bàn về tính

phi tập trung của Blockchain, để thay đổi một giao dịch hiện có sẽ cần phải kiểm soát được đồng thời trên 50% máy tính trong mạng lưới, điều này gần như bất khả thi. Ngay cả nếu trường hợp này xảy ra đi chăng nữa, nó cũng sẽ bị các máy tính thành viên khác trong mạng lưới phát hiện ra nhanh chóng.

Độ bảo mật của Blockchain không phải là không có sơ hở, nhưng những hệ thống Blockchain hiện nay đã liên tục chứng minh được tính bảo mật vượt trội. Blockchain giải quyết được nhiều vấn đề về bảo mật trong những hệ thống thông thường. Mặc dù tình trạng lừa đảo có lẽ không thể bị xóa sổ hoàn toàn, nhưng Blockchain tạo ra một lịch sử hoạt động rất sáng tỏ cho phép truy ngược về điểm khởi đầu để dễ dàng xác định âm mưu lừa đảo.

**Tiềm Năng Ứng Dụng Rộng Lớn**

Gần như mọi giá trị đều có thể ghi lại trong Blockchain, cụm từ "mọi giá trị" không nhất thiết phải là giá trị tài chính. Như trong chương đầu tiên với ví dụ về thư viện, giá trị là sách, nhưng cũng có thể là biên bản quyền sở hữu, nhận diện kỹ thuật số, chứng nhận bản quyền, tài liệu kỹ thuật số hoặc bất cứ thứ gì có thể được ghi vào cơ sở dữ liệu ngày nay.

Ví dụ về chứng nhận bản quyền, đây là những tài sản có giá trị dù chứng nhận chỉ là dữ liệu hoặc bộ số lưu trên một cơ sở dữ liệu. Giá trị đến từ những chứng nhận này giúp bảo vệ quyền sở hữu và lợi nhuận thu được từ những hoạt động trong phạm vi bản quyền.

Nhiều tổ chức và hiệp hội kiểm soát, quản lý các chứng nhận về bản quyền trong một cơ sở dữ liệu tập trung. Những chứng nhận này là tài sản chứa giá trị được lưu trữ trên Blockchain và nhờ đó loại bỏ được yêu cầu về một bên thứ ba phụ trách quản lý chứng

nhận đó. Các tài sản chứa giá trị chẳng hạn như các loại tiền ảo, các chứng nhận và nhiều tài sản kỹ thuật số khác có thể tồn tại chỉ trên Blockchain với tư cách tài sản Blockchain tự nhiên, điều này giúp quản lý hồ sơ quyền sở hữu hiện thời dễ dàng hơn.

Công nghệ Blockchain là một công nghệ mới rất dễ tiếp cận, đặc biệt khi gần đây có nhiều cải tiến như nền tảng Ethereum và hợp đồng thông minh. Điều này cho phép mọi người phát triển các ứng dụng để tận dụng công nghệ Blockchain.

Blockchain có tiềm năng thay đổi gần như mọi lĩnh vực công nghiệp trên thế giới. Nhiều dự án đang được phát triển cho thấy công nghệ Blockchain có thể ảnh hưởng tới cuộc sống thường nhật vì nhiều doanh nghiệp đã mở rộng hệ thống của họ dựa trên nền tảng Blockchain.

Phần sau cuốn sách, chúng ta sẽ tìm hiểu sâu hơn về các ngành công nghiệp khác nhau đã sử dụng công nghệ Blockchain như thế nào qua ví dụ về các dự án đang được phát triển hiện nay.

**Tiết Kiệm Chi Phí**

Công nghệ Blockchain có thể giúp giảm bớt rất nhiều chi phí trong nhiều ngành công nghiệp nhờ loại bỏ được các đơn vị trung gian liên quan đến quá trình lập hồ sơ và chuyển giao tài sản. Mọi đơn vị trung gian hay các lớp trong một giao dịch đều gây tăng chi phí lập hồ sơ và chuyển giao tài sản.

Trong nhiều hệ thống hiện hành, khi chuyển giao hoặc lập hồ sơ tài sản, mỗi tổ chức thường sử dụng nhiều cơ sở dữ liệu và sổ cái khác nhau. Một sổ cái phân tán sẽ cho phép các bên liên quan chuyển giao tài sản trên một sổ cái chung, tiết kiệm chi phí bảo quản nhiều sổ cái trong các tổ chức.

Duy trì nhiều sổ cái hoặc cơ sở dữ liệu rất tốn kém và thường là quá trình rất thủ công vì cần nhiều người phụ trách kiểm kê tính nhất quán của từng sổ cái. Nhưng sổ cái phân tán dựa trên nền tảng Blockchain sẽ giảm được nhiều chi phí vì thay thế được từng sổ cái riêng rẽ thành một sổ cái chung, tạo khả năng thanh toán theo thời gian thực và kiểm toán tất cả các thành viên trong mạng lưới mỗi khi xuất hiện một giao dịch.

**Tăng Tốc Độ Giao Dịch**

Các hệ thống sử dụng công nghệ Blockchain không chỉ giúp giảm chi phí giao dịch mà còn thực sự tăng tốc độ giao dịch. Nhờ loại bỏ được các đơn vị trung gian và thiết lập giao dịch trên sổ cái phân tán chung, các sổ cái ứng dụng công nghệ Blockchain có thể xử lý giao dịch gần như ngay lập tức.

Nếu bạn chuyển tiền từ tài khoản ngân hàng, bạn có thể thấy khoản tiền đã rời khỏi tài khoản của bạn, tuy nhiên thường phải vài ngày sau số tiền đó mới tới tài khoản khác.

Tương tự, khi mua hàng bằng thẻ tín dụng, các giao dịch có thể trong trạng thái đang xử lý suốt nhiều ngày trên bảng ghi giao dịch của tài khoản. Đối với chủ hàng, họ cung cấp hàng hóa cho người mua nhưng nhiều ngày sau, khi công ty dịch vụ tín dụng giải quyết xong giao dịch, mới nhận được thanh toán.

Để khắc phục tình trạng như những ví dụ kể trên, hệ thống xây dựng dựa trên nền tảng Blockchain đang được phát triển để tăng tốc giao dịch. Tuy nhiên, không chỉ trong các tình huống đó mà mọi loại giao dịch hoặc chuyển giao giá trị đều có thể áp dụng công nghệ Blockchain để tăng cường tốc độ giao dịch.

Trong phần sau cuốn sách, chúng ta sẽ thảo luận về những công ty đang phát triển các hệ thống xây dựng nền tảng trên công nghệ Blockchain để cải thiện tốc độ giao dịch trong lĩnh vực tài chính và nhiều lĩnh vực công nghiệp khác.

**Phần Kết**

Đa phần thông tin được xuất bản về công nghệ Blockchain đều đề cập tới lợi thế, bất lợi và những đồn thổi xoay quanh tiềm năng của nó. Dù chương này đã trình bày nhiều lợi ích trong việc sử dụng các hệ thống xây dựng trên nền tảng công nghệ Blockchain, nhưng không có nghĩa là nó đã hoàn hảo hoặc trả lời được toàn bộ vấn đề liên quan tới một ngành công nghiệp.

Trong chương sau, chúng ta sẽ xem xét những bất lợi và rủi ro khi sử dụng các hệ thống xây dựng trên nền tảng Blockchain.

**Điểm Cốt Lõi:**

• Tính minh bạch: Blockchain cung cấp nhiều bước tiến to lớn trong việc cải thiện tính minh bạch khi so sánh với cách thức ghi chép hồ sơ và sổ cái hiện hành trong nhiều ngành công nghiệp.

• Loại bỏ đơn vị trung gian: Các hệ thống xây dựng dựa trên công nghệ Blockchain cho phép loại bỏ các đơn vị trung gian liên quan đến hoạt động lập hồ sơ và chuyển giao tài sản.

• Phi tập trung: Các hệ thống xây dựng dựa trên công nghệ Blockchain có thể hoạt động trên mạng lưới máy tính phi tập trung, từ đó giảm thiểu rủi ro bị tấn công, thời gian chết trên máy chủ và thất thoát dữ liệu.

• Niềm tin: Các hệ thống xây dựng dựa trên công nghệ Blockchain gia tăng niềm tin giữa các bên giao dịch nhờ tính minh bạch được cải thiện và mạng lưới phi tập trung đồng thời loại bỏ các

đơn vị trung gian tại những quốc gia nơi người ta khó lòng tin tưởng vào các đơn vị trung gian trong giao dịch.

• Độ bảo mật: Dữ liệu nhập vào Blockchain sẽ không thể sửa đổi, nhờ đó tránh được tình trạng gian lận qua việc ngụy tạo giao dịch và lịch sử dữ liệu. Các giao dịch đưa vào Blockchain sẽ tạo nên một lịch sử hoạt động rõ ràng từ điểm khởi đầu của Blockchain, cho phép dễ dàng thẩm tra và kiểm kê mọi giao dịch.

• Tiềm năng ứng dụng rộng: Đa phần mọi giá trị đều có thể được lập hồ sơ dựa trên Blockchain và nhiều công ty trong nhiều lĩnh vực công nghiệp đã phát triển các hệ thống dựa trên công nghệ Blockchain. Ví dụ cụ thể sẽ được trình bày trong phần sau cuốn sách.

• Công nghệ dễ tiếp cận: Cùng với tiềm năng ứng dụng rộng rãi, công nghệ Blockchain còn giúp việc tạo lập các ứng dụng dễ dàng hơn, nhờ các bước tiến hiện nay như nền tảng Ethereum, mà không cần phải đầu tư quá nhiều vào cơ sở hạ tầng. Các ứng dụng phi tập trung, các hợp đồng thông minh và nền tảng Ethereum sẽ được trình bày trong phần sau cuốn sách.

• Tiết kiệm chi phí: Sổ cái thiết lập trên nền tảng Blockchain cho phép loại bỏ đơn vị trung gian và các lớp xác nhận trong giao dịch. Các giao dịch, dù cần nhiều sổ cái riêng biệt, đều có thể được thiết lập trên một sổ cái chung, từ đó giảm thiểu chi phí kiểm nhận, xác thực và thẩm tra một giao dịch trên các tổ chức khác nhau.

• Tăng tốc độ giao dịch: Khả năng loại bỏ đơn vị trung gian và thiết lập trên sổ cái phân tán cho phép tăng tốc độ giao dịch cao hơn so với nhiều hệ thống hiện có.

• Bất lợi: Có một loạt lý do hợp lý và đầy thuyết phục về việc chuyển đổi từ hệ thống hiện có sang hệ thống xây dựng dựa trên công nghệ Blockchain. Tuy nhiên, cũng có những khuyết điểm và rủi ro không thể bỏ qua.

# Chương 5
# Bất lợi/Rủi ro khi sử dụng công nghệ Blockchain

*"Blockchain được thiết kế đặc biệt vì một mục đích trọng đại: ngăn chặn tình trạng 'giao dịch lặp chi' khi sử dụng đồng tiền điện tử mà không cần đến một tổ chức trung tâm. Nhưng một số trường hợp sử dụng gây chú ý dễ bị các giao dịch lặp chi hoặc các vấn đề tương tự tấn công. Đồng thời, nhiều mục tiêu bảo mật quan trọng không được Blockchain cung cấp.*

*Vì thế, Blockchain vừa không cần thiết vừa không hiệu quả trong nhiều ứng dụng đề xuất của nó; trên thực tế, công nghệ này phức tạp một cách không cần thiết, hoặc chưa hoàn thiện, hoặc cả hai."*

**- Steve Wilson,** tác giả cuốn "Beyond the Hype: Understanding the Weak Links in the Blockchain" [1]

[1] *Vượt qua lời đồn: Thấu hiểu những mắt xích yếu kém trong Blockchain*

Công nghệ Blockchain có lẽ đã bị mời chào như một giải pháp toàn năng cho mọi vấn đề trong các lĩnh vực công nghiệp và trên thế giới.

Nhiều công ty khởi nghiệp từ công nghệ Blockchain và nhiều đồng tiền ảo được ra đời hứa hẹn giải quyết được mọi việc từ phá bỏ hệ thống ngân hàng tới xóa bỏ đói nghèo trên thế giới.

Nhiều nhận định về công nghệ Blockchain gợi nhắc tới mạng Internet vào những ngày đầu tiên. Trong khi mạng Internet đã thực sự thay đổi thế giới, nhiều dự đoán về Blockchain lại quá phóng đại, thời gian diễn ra phi thực tế và nhiều công ty khởi nghiệp đang thành công được dự báo là sẽ phá sản trong tương lai.

Trong chương này, chúng ta sẽ nghiên cứu một số vấn đề và bất lợi của công nghệ Blockchain.

**Thiếu Tính Riêng Tư**

Các Blockchain phi tập trung thiếu tính riêng tư, điều này gây khó khăn trong việc đạt được đồng thuận triệt để. Thông tin không chỉ thiếu tính riêng tư mà còn có thể được truy cập dễ dàng vào bất cứ thời điểm nào từ bất cứ người dùng nào trong hệ thống.

Việc xác định danh tính một tài khoản trên Blockchain Bitcoin sau khi nhận được khoản thanh toán từ người đó cũng tương đối dễ dàng.

Nếu bạn đến một cửa hàng và thực hiện thanh toán, chủ cửa hàng có thể thấy giao dịch đó trên Blockchain. Thông tin trong giao dịch sẽ cho thấy khoản tiền được gửi từ ví nào, họ còn có thể kiểm tra tài khoản đó và biết được bạn sở hữu bao nhiêu tiền cũng như toàn bộ các giao dịch xuất nhập từ tài khoản đó của bạn.

Ý nghĩ về một Blockchain phi tập trung cung cấp rõ ràng từng giao dịch đơn lẻ từ đó công khai mạng lưới đã trở thành nỗi lo lắng của nhiều người. Đặc biệt trong trường hợp mua sắm tại những cửa hàng nơi danh tính có thể liên kết trực tiếp tới tài khoản và giao dịch.

Điều này cũng gây nên ái ngại rằng nhiều máy tính hoạt động trên mạng lưới Blockchain quy mô lớn tại những quốc gia như Nga và Trung Quốc, nơi tình trạng tội phạm công nghệ cao và thông tin

cá nhân có thể bị lợi dụng để gây hại cho những người sinh sống và khách du lịch tới các quốc gia đó.

Có nhiều Blockchain phi tập trung cung cấp mức độ bảo mật giao dịch cao hơn hoặc giới hạn người có thể truy cập để theo dõi thông tin. Tuy nhiên, Bitcoin, Ethereum và nhiều đồng tiền ảo Blockchain quy mô lớn khác không vận hành theo cách đó và hiện tại không có kế hoạch tăng cường tính riêng tư cho giao dịch hay tài khoản.

**Những Lo Ngại Về Bảo Mật**

Tài sản trong công nghệ Blockchain là tiền mặt, nên tiền mặt trong ví của bạn sẽ mất hẳn nếu bị trộm cắp hay thất lạc. Các hệ thống dựa trên công nghệ Blockchain sử dụng mật mã học và mã hóa cao cấp an toàn hơn các mật khẩu tiêu chuẩn trên mạng Internet hay mã số truy cập. Tuy nhiên, bảo mật hơn đôi khi có thể khiến một hệ thống thiếu tin cậy hơn.

Có vô số trường hợp trong thế giới tiền ảo nơi mà người dùng quên khóa cá nhân nên không thể truy cập khoản tiền của họ. Bạn chỉ cần xem chủ đề trên các diễn đàn trực tuyến nơi người khởi tạo chủ đề cảnh báo mọi người đừng làm mất khóa cá nhân kèm theo một câu chuyện về việc chính họ đã làm mất khóa cá nhân và rồi không thể lấy được tiền trong ví như thế nào.

Những trường hợp này thường xảy ra khi người ta mua một loại tiền ảo nào đó với giá thấp nhưng không quá quan tâm đến chuyện đó. Sau này, họ thấy giá trị đồng tiền đó tăng lên nhiều và khoản đầu tư nho nhỏ ban đầu nay đã thành hàng ngàn đô la, vì thế họ cố gắng truy cập lại.

Khoản mua Bitcoin với giá 50 đô vào năm 2009 sẽ có giá hơn một triệu đô vào tám năm sau, vì thế những trường hợp như trên xảy ra là điều rất dễ hiểu. Một trường hợp rất nổi tiếng trong số này là James Howells, sống tại Vương quốc Anh, đã vứt bỏ chiếc máy tính xách tay với 7.000 Bitcoin trong đó. Ngày nay, giá trị của số Bitcoin này là hơn 15 triệu đô la.

Vì tính minh bạch trong Blockchain, nếu mọi người có khóa công khai, họ có thể xem số dư tài khoản và giá trị của nó nhưng không thể truy cập được. Điều này cũng tương tự như một ngân hàng có thể cho bạn biết số dư tài khoản ngân hàng của bạn nhưng bạn không có cách nào tiếp cận được số tiền đó.

Đối với những tài khoản ngân hàng truyền thống, nếu bạn mất mật khẩu ngân hàng trực tuyến, thẻ tín dụng hoặc số tài khoản, bạn có thể tới ngân hàng và chứng minh danh tính để lấy lại quyền truy cập. Nhưng đối với các loại tiền ảo dựa trên công nghệ Blockchain phi tập trung như Bitcoin thì lại không như vậy. Trong vài năm vừa qua, có hàng tỷ đô la tiền ảo bị mất do bị tấn công, gian lận hoặc bảo vệ kém.

Nếu một người truy cập thẻ tín dụng của bạn và rút tiền trong đó, bạn có thể gọi cho ngân hàng yêu cầu khóa thẻ để người kia không rút được thêm nữa. Ngân hàng sẽ thường có bảo mật chống gian lận, đồng thời có khả năng đảo chiều giao dịch và truy nguyên các khoản thanh toán.

Đối với các hệ thống xây dựng trên nền tảng Blockchain, các giao dịch có thể bị thay đổi hoặc đảo ngược nhưng không có lấy một đơn vị trung gian nào hỗ trợ bạn nếu xảy ra gian lận trong tài khoản của bạn. Nếu bạn gửi tiền tới nhầm tài khoản (ví) trên Blockchain,

bạn sẽ mất hẳn số tiền đó. Nếu có người giành được quyền truy cập khóa cá nhân của bạn, họ có thể rút toàn bộ tiền ra khỏi tài khoản của bạn và không có cách nào đảo ngược giao dịch đó hoặc yêu cầu đền bù.

Thắc mắc đầu tiên trong số những câu hỏi phổ biến nhất về hệ thống áp dụng công nghệ Blockchain là: "Tôi có thể đặt lại mật khẩu bằng cách nào nếu tôi quên hoặc làm mất nó?", đáp án là "Bạn không thể đặt lại". Lời khuyên cho mọi người khi thiết lập khóa cá nhân trên Blockchain là "ghi chép lại". Mọi tiến bộ trong mật mã học rốt cuộc lại khiến người ta phải chép lại khóa cá nhân vào đâu đó, rồi giấu ở nhà hoặc trong máy tính, tất cả điều đó gây sụt giảm tính bảo mật nếu so sánh với phương thức bảo mật truyền thống.

Đối với việc xử lý vấn đề chung trong các hệ thống dựa trên Blockchain, nhiều phương thức bảo mật, dù giúp tài sản Blockchain an toàn hơn, lại khiến việc đồng thuận vấn đề chung đó trở nên khó khăn hơn. Loại ví Blockchain dựa trên nền tảng web rất phổ biến, nơi mọi người lưu trữ tiền ảo qua một công ty thứ ba. Khi sử dụng các ví dựa trên nền tảng web do bên thứ ba cung cấp, mọi người phải hy sinh những lợi ích bảo mật của Blockchain chẳng hạn như khóa cá nhân để đổi lấy các mật khẩu truyền thống mà họ có thể đặt lại nếu chẳng may quên mất.

**Không Tồn Tại Quyền Quản Lý Tập Trung**

*"Trong thị trường tài chính, luôn tồn tại một cơ chế sửa chữa khi bị tấn công. Trong Blockchain, không có cơ chế sửa chữa vấn nạn đó - mọi người phải chấp nhận chuyện đó."*

**- Robert Sams,** Nhà sáng lập và Giám đốc Điều hành Clearmatics, Công ty có trụ sở đặt tại London, Anh

Hệ thống dựa trên nền tảng Blockchain được thiết kế để thay thế vai trò trung gian của các bên thứ ba, trao lại trách nhiệm và quyền kiểm soát cho các cá nhân tham gia giao dịch.

Quyền kiểm soát này được đặt vào đại đa số các thành viên của mạng lưới, gây ra các vấn đề về quyền quản lý trong Blockchain.

Bản chất phi tập trung của nhiều Blockchain đồng nghĩa với việc mạng lưới phải đồng thuận cũng như quyết định hướng tương lai của mạng lưới và Blockchain. Đối với chương trình và mạng lưới truyền thống, khi một tổ chức muốn có sự thay đổi, họ có thể tiến hành thay đổi sau khi có sự nhất trí từ các phòng ban liên quan thuộc nội bộ tổ chức. Nhưng đối với mạng lưới Blockchain phi tập trung như Bitcoin, sự thay đổi phải nhận được đồng thuận của đa số nào đó trong mạng lưới, con số này thường là hơn 50%, nhưng cũng có thể cao tới mức 70% đến 80% thành viên trong mạng lưới.

Một ví dụ mới đây về đặc điểm này là việc biểu quyết chọn thực thi SegWit (Nhân Chứng Tách Rời) hay Bitcoin Unlimited (một phiên bản phân nhánh của Bitcoin) trong mạng lưới Bitcoin. Rất nhiều thành viên của mạng lưới ủng hộ những thay đổi đa dạng trong mạng lưới Bitcoin, nhưng không bên nào đạt đến đa số để được yêu cầu thực hiện thay đổi.

Sự bất đồng này cũng cho thấy các mạng lưới Blockchain và những đồng tiền ảo khác có khả năng tiến xa hơn Bitcoin về mặt cải tiến công nghệ. Sự bất đồng này còn khiến mạng lưới Bitcoin bị trì trệ vì thời gian giao dịch chậm, thời gian xác nhận lâu và nhiều vấn đề về khả năng mở rộng liên tục.

Công nghệ, chẳng hạn như phần mềm, thay đổi liên tục theo thời gian. Các mạng lưới Blockchain phi tập trung có thể đi đến tình cảnh

chia tách vì hướng thay đổi, đặc biệt khi không đạt được đồng thuận theo số đông. Nếu đạt tới đồng thuận số đông, vẫn còn một số lớn thành viên trong mạng lưới không đồng ý với những thay đổi vừa được phê chuẩn.

Điều này khiến các mạng lưới phi tập trung trở nên đầy rủi ro khi sử dụng đối với các tổ chức. Một công ty có thể thiết lập một giao dịch hoặc phần mềm xoay quanh một mạng lưới mà họ không có quyền kiểm soát những thay đổi có nguy cơ ảnh hưởng tới giao dịch hoặc phần mềm của chính họ.

**Rủi Ro Từ Tấn Công Quá Bán**

Tiếp tục với vấn đề quản lý, nếu một người có khả năng kiểm soát trên 50% số máy trong mạng lưới Blockchain, họ sẽ kiểm soát được các giao dịch trên Blockchain. Một người dùng hiểm độc kiểm soát được trên 50% số máy trong mạng lưới Blockchain được gọi là "Tấn Công Quá Bán".

Nếu tận dụng được quyền kiểm soát trên mạng lưới tiền ảo này, theo lý thuyết, họ có thể khiến các giao dịch mới không được xác nhận, đảo chiều giao dịch và cho phép "giao dịch lặp chi" tai hại xảy ra.

Một cuộc Tấn Công Quá Bán trên mạng lưới Blockchain thường được coi là lý thuyết vì để kiểm soát một số lớn trên mạng lưới rất khó khăn; tuy nhiên, có nhiều trang trại khai thác khổng lồ đặt tại Trung Quốc, Nga và nhiều nơi khác trên thế giới nắm quyền kiểm soát phần lớn công suất tính toán trong mạng lưới Blockchain. Nếu những trang trại khai thác khổng lồ này liên kết lại với nhau, họ có khả năng chiếm dụng mạng lưới Blockchain và thao túng mạng lưới vì lợi ích riêng.

Ngay cả khi không kiểm soát được 51% mạng lưới, họ cũng có thể thao túng mạng lưới bằng cách phân bổ công suất tính toán theo hướng gây ảnh hưởng tới sự phát triển tương lai của mạng lưới. Đây cũng là trường hợp liên quan đến vấn đề biểu quyết của mạng lưới Bitcoin đã đề cập phía trên.

**Công Nghệ Mới Chưa Được Chứng Thực**

Hệ thống dựa trên nền tảng Blockchain là công nghệ mới chưa được chứng minh, và chỉ được dùng chủ yếu trong lĩnh vực tiền ảo. Vẫn còn tồn tại tình trạng khuyết thiếu các ứng dụng thực tế hiện thời để chứng minh hiệu quả của công nghệ này.

Công nghệ này còn mới mẻ với nhiều tiềm năng, nhưng hầu hết tiềm năng đều là lý thuyết. Câu nói "Hãy làm chiếc bẫy chuột hấp dẫn hơn, rồi cả thế giới sẽ đổ xô đến nhà bạn" là quan niệm kinh doanh sai lầm rất phổ biến. Nếu chỉ vì một công nghệ có thể tốt hơn nhiều mặt của những hệ thống hiện hành, thì cũng không có nghĩa rằng mọi người sẽ muốn sử dụng nó thay vì những phương án chọn lựa sẵn có.

Như đã đề cập, khả năng bảo mật của mật mã học hiệu quả hơn nhiều các phương thức bảo mật hiện có, tuy nhiên nếu bạn mất khóa để mở các hệ thống dựa trên nền tảng Blockchain, bạn sẽ không thể lấy lại được. Mọi người thường chọn cách ghi lại khóa cá nhân lên giấy, hoặc lưu trong máy tính để không bị quên mất; chính điều này lại phá hỏng những lợi ích của bảo mật tăng cường và có nguy cơ khiến hệ thống thiếu an toàn hơn.

Một lợi ích khác của mạng lưới Blockchain là loại bỏ được các đơn vị trung gian. Quá trình kết nối các mạng lưới Blockchain, truyền gửi giao dịch, thiết lập khóa cá nhân rất phức tạp và rủi ro đối

với nhiều người. Nhiều cá nhân ưa thích trao quyền sử dụng khóa cá nhân cho đơn vị trung gian với các ví trên nền tảng web hoặc các phần mềm tương tự, tuy nhiên những lựa chọn này lại triệt tiêu lợi ích cơ bản của mạng lưới Blockchain.

**Chi Phí**

Thuật toán Bằng Chứng Xử Lý, mà nhiều mạng lưới Blockchain sử dụng, yêu cầu chứng thực rằng các nguồn lực và công suất tính toán được đóng góp vào mạng lưới trước khi một khối được bổ sung vào mạng. Bằng chứng này được thể hiện dưới dạng lời giải cho một mảnh ghép được đính kèm vào khối để mạng lưới kiểm nhận xem có chính xác hay không. Giải đáp mảnh ghép này cần điện năng và công suất tính toán lớn.

Giáo sư John Quiggin thuộc trường Đại học Queensland đã tính ra rằng, cứ nửa giờ, mạng Bitcoin sử dụng một lượng điện năng gần tương đương với lượng điện các hộ gia đình bình thường tại Mỹ dùng trong một năm.

Các hộ gia đình bình thường tại Mỹ tiêu thụ điện năng từ 10.000 tới 12.000 kWh mỗi năm, gần bằng lượng điện cần thiết để tạo ra 04 Bitcoin với giá trị khoảng 1.000 đô.

Do chi phí điện năng vận hành máy tính trên mạng Blockchain sử dụng thuật toán Bằng Chứng Xử Lý rất cao, nên rất lợi thế cho những quốc gia có nguồn điện giá rẻ hoặc cho các tổ chức có những thỏa thuận hời với các công ty năng lượng.

Vì độ khó của các mảnh ghép trên Blockchain tăng, nên lượng tiêu thụ điện năng cũng sẽ tăng, điều này khiến chi phí càng cao và đòi hỏi càng nhiều nguồn lực để vận hành Blockchain sử dụng thuật toán Bằng Chứng Xử Lý trên quy mô lớn.

**Thiếu Khả Năng Mở Rộng**

Với mức tiêu thụ năng lượng hiện tại, chi phí điện để vận hành một Blockchain có sử dụng thuật toán Bằng Chứng Xử Lý khiến việc ứng dụng Blockchain để giải quyết số lượng lớn các giao dịch ở các công ty tín dụng như Visa và MasterCard trở nên không tưởng. Đây là một trong những yếu tố hiện đang ảnh hưởng tới khả năng mở rộng của mạng lưới Blockchain.

Cứ 10 phút sẽ có một khối được bổ sung vào Blockchain Bitcoin, mỗi khối hiện thời chứa khoảng 2.000 giao dịch, tức là mạng lưới Bitcoin hiện đang xử lý khoảng 3 giao dịch mỗi giây.

Vì kích thước khối hạn chế nên mạng lưới Bitcoin chỉ có khả năng xử lý tối đa 7 giao dịch mỗi giây. Visa đã thực hiện nhiều thử nghiệm với IBM trong đó mạng lưới Visa có khả năng thực hiện trên 20.000 giao dịch mỗi giây.

Nếu bạn đi mua hàng và muốn dùng thẻ tín dụng, nhưng bạn lại không có đủ tiền trong thẻ để thanh toán, giao dịch đó sẽ bị từ chối. Mạng lưới Bitcoin lại không có cơ chế sẵn sàng như thế.

Một giao dịch trên Blockchain Bitcoin sẽ cần tối thiểu 10 phút mới được bổ sung vào Blockchain nên các công ty có thể sẽ phải chờ nhiều khối được thêm vào hơn trước khi xác nhận giao dịch, để đảm bảo rằng giao dịch sẽ không bị đảo chiều.

So sánh sự khác biệt giữa hai phương thức này, nếu bạn định mua hàng và thanh toán bằng Bitcoin, chủ cửa hàng có thể sẽ phải chờ một tiếng để chắc chắn rằng giao dịch đã được xác nhận sau khi nhiều khối khác phía trên khối chứa giao dịch đã được bổ sung vào chuỗi.

Có những mạng Blockchain nhanh hơn mạng Bitcoin nhiều nhưng lại không được phổ biến hoặc được chấp nhận là một hình thức thanh toán như Bitcoin. Nhưng ngay cả những Blockchain và các loại tiền ảo sở hữu thời gian xác nhận giao dịch nhanh hơn cũng không có khả năng sánh được với trình độ của các mạng thanh toán tài chính đương thời như Visa hay MasterCard.

Vì những vấn đề về khả năng mở rộng này, nhiều người coi việc thực hiện của Blockchain trên quy mô lớn chẳng khác gì thông tin đề thời gian trong một cuốn sổ cái chung.

**Niềm Tin, Uy Tín Và Hiểu Biết Về Blockchain**

Vẫn còn tồn tại nhiều sự thiếu hiểu biết về cách thức Blockchain hoạt động cũng như tai tiếng bắt nguồn từ mối liên hệ với Bitcoin.

Bitcoin là ứng dụng Blockchain phổ biến nhất, và nhiều người có quan niệm nặng nề rằng Bitcoin gắn với tội phạm. Mặc dù loại tiền ảo này đang ngày càng được chấp nhận rộng rãi với tư cách một hình thức thanh toán hợp pháp, nhưng tội phạm máy tính và khủng bố đã đẩy Bitcoin vào những tin tức liên quan đến vấn đề đó.

Một trường hợp gần đây xảy ra trong mạng lưới máy tính tại Sở Y tế Quốc gia (NHS) tại Vương quốc Anh. Một vi rút đã khóa các máy tính của NHS, khiến người ta không thể truy cập được trừ phi trả tiền chuộc bằng Bitcoin. Vụ việc đã đưa Bitcoin lên tiêu đề các trang báo tại Anh trong đó quy kết Bitcoin với tội phạm máy tính, hacker và khủng bố nặc danh. Các bệnh viện đã không thể truy cập được hồ sơ bệnh án, điều này gây hậu quả nặng nề đến sinh mạng của nhiều bệnh nhân đang cần chữa trị y tế trong suốt thời gian này.

Blockchain tuyên bố sẽ tạo được niềm tin giữa mọi người trong giao dịch mà không cần đặt lòng tin vào đơn vị trung gian. Tuy

nhiên, người ta vẫn cần đặt niềm tin vào mạng lưới Blockchain và những máy tính vô danh đang vận hành nó. Thật khó để khiến người ta tin tưởng một hệ thống có thể bị tội phạm sử dụng thoải mái, đặc biệt là vì nhiều máy tính đang vận hành mạng lưới lại được đặt tại nhiều quốc gia không được chính phủ sở tại quy định và kiểm soát.

Những sự cố về tội phạm máy tính liên quan đến Bitcoin là nguyên nhân chính khiến nhiều công ty phát triển hệ thống dựa trên nền tảng Blockchain đang cố gắng tách biệt Bitcoin và Blockchain. Thuật ngữ "sổ cái phân tán" đã trở nên phổ biến hơn trong thời gian gần đây, khiến khoảng cách giữa Bitcoin và công nghệ dựa trên nền tảng Blockchain mới trở nên xa xôi hơn.

Những lợi ích của hệ thống dựa trên nền tảng Blockchain khá khó hiểu đối với nhiều người. Như đã đề cập, nhiều người đã cho phép đơn vị trung gian truy cập Blockchain để họ có thể sử dụng loại mật khẩu thông thường đăng nhập vào các trang web, chính điều này đã triệt tiêu lợi ích của công nghệ Blockchain. Nhiều người không thích người khác biết được số dư tài khoản hay các giao dịch của họ hoặc những phương diện khác của Blockchain nên ưa thích sử dụng các hệ thống vốn có hơn.

Nói chung, niềm tin và hiểu biết về mạng lưới Blockchain sẽ đóng vai trò quan trọng trong việc thúc đẩy sự chấp nhận công nghệ này. Có lẽ cần nhiều thời gian để công chúng có thể đặt niềm tin vào mạng lưới Blockchain và an tâm giao dịch trên đó.

**Quy Định Và Kết Hợp**

*"Các chuyên viên phân tích và tay chơi tài chính tài năng nhất thế giới đang bàn tán sôi nổi về một phát kiến đang phần nào nổi*

*tiếng vì hứa hẹn sẽ đánh bại họ."*

**- Mike Gault**

Các tài sản dựa trên nền tảng Blockchain đang đối mặt với quy trình xử lý các vấn đề luật định và phối hợp trường kỳ với các hệ thống hiện hành. Chính phủ và ngân hàng phản đối thay đổi vì quy mô và chi phí cần để thay đổi các hệ thống đang sử dụng.

Nếu các hệ thống dựa trên nền tảng Blockchain không thể chứng minh được rằng chúng có thể tạo nên khoản tiết kiệm chi phí hoặc lợi ích to lớn xứng đáng thay thế các hệ thống hiện thời, thì các tổ chức lớn như chính phủ và ngân hàng sẽ không nhanh chóng sử dụng chúng.

Chính phủ nước Cộng hòa Estonia đang thử nghiệm các hệ thống dựa trên nền tảng Blockchain, nhưng quốc gia này có dân số chưa tới 1,5 triệu người. Nhiều thành phố ở Mỹ, Trung Quốc và nhiều nước khác có số dân lớn hơn 10 lần. Mặc dù các hệ thống dựa trên nền tảng Blockchain có thể hoạt động trên quy mô nhỏ, nhưng đối với các quy mô tầm cỡ ngân hàng và chính phủ lớn như Mỹ lại không dễ dàng như vậy.

Hiệp hội Tài chính Quốc tế R3 và Ripple là các ví dụ về sổ cái phân tán hoặc sổ cái dựa trên nền tảng Blockchain được tích hợp vào nhiều công ty tài chính tại nhiều quốc gia.

Có nhiều công ty tài chính từ chối chuyển tiếp sang sổ cái dựa trên nền tảng Blockchain vì Blockchain mới chỉ được thử nghiệm trên quy mô "nhỏ".

Nếu nhiều tổ chức tài chính lớn chuyển sang công nghệ mới và đang sử dụng thì có vấn đề xảy ra, điều này có thể đẩy thị trường tài

chính thế giới và dữ liệu khách hàng vào một hiểm họa nghiêm trọng.

Hội đồng Giám sát Độ Ổn định Tài chính (Financial Stability Oversight Council - FSOC) còn lo ngại rằng một số hệ thống dựa trên nền tảng Blockchain dễ bị gian lận hơn so với những nhận định thu được gần đây qua thử nghiệm trên quy mô nhỏ.

Một vấn đề khác đối với nhiều tổ chức tài chính sử dụng hệ thống dựa trên nền tảng Blockchain hoặc sổ cái phân tán chung là lĩnh vực hoạt động của các nhà quản lý. Một hệ thống dựa trên nền tảng Blockchain, theo lý thuyết, có thể trải rộng trên nhiều phạm vi quản lý và lãnh thổ quốc gia khác nhau, vì thế càng làm mối quan hệ giữa các nhà quản lý và phạm vi thực hiện giao dịch trở nên u ám.

Nhiều tổ chức tài chính lớn sẽ rất thận trọng với việc chuyển đổi sang bất cứ hệ thống nào mà các quy định của chính phủ chưa rõ ràng. Rủi ro kinh doanh và tài chính sẽ quá cao nếu các chính phủ không đưa ra quy định cụ thể về cách thức ứng đối với các tài sản dựa trên nền tảng Blockchain. Quan ngại về luật định, chi phí tích hợp cùng với việc thiếu thốn các ứng dụng hệ thống dựa trên nền tảng Blockchain trên quy mô lớn sẽ dẫn tới việc áp dụng chậm chạp công nghệ này vào các chính phủ và tổ chức tài chính lớn.

**Những Lời Đồn Thổi**

Nhiều bài viết về công nghệ Blockchain có thể coi là quá mức thổi phồng hoặc quá sốt sắng với những nhận định rằng công nghệ Blockchain sẽ biến đổi thế giới, hủy hoại các chính phủ, triệt tiêu các ngân hàng, giải quyết vấn nạn đói nghèo trên thế giới, và có khi còn giúp bạn có được cơ bụng săn chắc mà không cần tập thể hình.

Nhận định cuối cùng về cơ bụng không phải là sự thật, nhưng lại cho thấy những đồn thổi xoay quanh Blockchain, và sẽ chẳng bất ngờ gì nếu một công ty khởi nghiệp đặt tại Thung lũng Silicon đã đưa ý tưởng này vào quỹ đầu tư mạo hiểm.

Rất dễ lạc trong những đồn thổi về một công nghệ mới, mạng Internet cũng không phải ngoại lệ. Đó là một công nghệ có tính cách mạng đã làm thay đổi cả thế giới, tuy nhiên rất nhiều dự đoán vào thuở sơ khai của mạng Internet gọi nó là "niềm lạc quan phi lý".

Khoảng thời gian ước lượng về mức độ ảnh hưởng của công nghệ mới này thay đổi chóng mặt và thường sai lệch rất lớn. Như đã đề cập trong phần lịch sử hình thành của Blockchain, DigiCash và những công nghệ dựa trên nền tảng mật mã học cùng nhiều đồng tiền ảo khác đã ra đời từ vài thập kỷ trước Bitcoin nhưng lại là quá sớm so với dự đoán về khả năng chấp nhận công nghệ của thị trường.

Ngay cả khi nhiều dự đoán về ảnh hưởng của công nghệ Blockchain chính xác, chúng cũng sẽ không có bất kỳ tác động lớn nào tới xã hội trong nhiều năm tới. Các công ty khởi nghiệp tiên phong trong công nghệ mới này có lẽ không có khả năng tồn tại đủ lâu để thấy công nghệ của họ tiếp cận được thị trường đại chúng.

Như đã đề cập trong chương trước, ngay cả khi mọi người muốn sử dụng Bitcoin và hệ thống dựa trên nền tảng Blockchain, nhiều người vẫn thích các phương thức mà Blockchain định thay thế. Điều này sẽ ngay lập tức xóa bỏ nhu cầu sử dụng các hệ thống dựa trên nền tảng Blockchain nếu mọi người ưa dùng các hệ thống hiện có hơn là những lợi ích hứa hẹn đến từ Blockchain.

Công nghệ Blockchain chỉ là cách thức mới để lưu trữ và quản lý dữ liệu. Công nghệ này không phải giải pháp cho mọi vấn đề trên thế giới, vì thế đừng tin vào những lời đồn thổi.

**Điểm Cốt Lõi:**

• Thiếu tính riêng tư: Nhiều Blockchain phi tập trung không có tính riêng tư. Số dư tài khoản và các giao dịch đều có thể bị mọi người trên mạng lưới xem xét.

• Những lo ngại về bảo mật: Tài sản dựa trên nền tảng Blockchain như tiền mặt, nếu tiền trong ví bạn bị mất hoặc bị đánh cắp, bạn sẽ mất số tiền đó. Nhiều phương thức bảo mật trong Blockchain lại khiến việc đồng thuận vấn đề chung đó trở nên khó khăn hơn và có thể kém an toàn hơn so với những phương thức hiện thời vì mọi người sẽ chép lại khóa cá nhân để họ không bị quên mất.

• Không tồn tại quyền quản lý tập trung: Với một mạng Blockchain như Bitcoin, những sự thay đổi phải nhận được đồng thuận của một đa số nào đó trong mạng lưới, con số này có thể hơn 50% nhưng cũng có thể đạt tới 70% hoặc 80% mạng lưới. Không một tổ chức đơn lẻ nào kiểm soát các thay đổi hoặc định hướng trong Blockchain phi tập trung, điều này khiến các tổ chức sử dụng có nguy cơ gặp rủi ro khi giao dịch vì họ không thể kiểm soát được thay đổi nào trong hệ thống.

• Rủi ro từ Tấn Công Quá Bán: Nhiều máy tính vận hành Blockchain trên quy mô toàn cầu được đặt tại các quốc gia nơi mà người dân không an tâm vì vấn đề tội phạm, hệ thống pháp luật và tình trạng thiếu các quy định. Chi phí điện thấp và chi phí máy tính tại nhiều quốc gia đã tạo nên nhiều trung tâm khai thác khối lớn trên

Blockchain. Nếu những trung tâm dữ liệu này liên kết lại với nhau, chúng có khả năng kiểm soát hơn 50% mạng lưới và chiếm quyền quản lý mạng lưới.

• Công nghệ chưa được kiểm chứng: Các công nghệ Blockchain là công nghệ mới chưa được chứng thực và được sử dụng chủ yếu trong các loại tiền ảo. Điều này vẫn hạn chế các công ty hoặc phần mềm thực tế sử dụng công nghệ Blockchain để chứng minh hiệu quả cao hơn các hệ thống hiện có.

• Chi phí: Cần lượng điện năng lớn để vận hành. Theo ước tính, cứ nửa giờ mạng Blockchain tiêu thụ lượng điện bằng lượng điện mà các hộ gia đình thông thường tại Mỹ sử dụng trong trọn một năm.

Ghi chú: Các tính toán về lượng tiêu thụ điện năng dựa trên lượng tiêu thụ điện hộ gia đình thông thường tại Mỹ vào khoảng 10.000 tới 12.000 kWh. Số lượng này bằng với lượng điện để sản sinh ra 4 khối trên Blockchain Bitcoin.

• Vấn đề về khả năng mở rộng: Mạng lưới Blockchain chưa được chứng minh rằng có hiệu quả sánh ngang với các hệ thống hiện có. Mạng lưới Bitcoin chỉ có thể xử lý khoảng 7 giao dịch một giây trong khi mạng lưới Visa có thể xử lý trên 20.000 giao dịch một giây.

• Sự thiếu hiểu biết về công nghệ Blockchain: Cách thức Blockchain hoạt động và lợi ích của nó rất khó hiểu với nhiều người. Nhiều người còn lo ngại về các phương diện trên mạng lưới Blockchain như số dư và giao dịch của họ bị công khai. Ngay cả khi hiểu được các lợi ích, nhiều người vẫn thích các hệ thống hiện hành hơn.

• Quy định và kết hợp: Các hệ thống dựa trên nền tảng Blockchain sẽ phải đối mặt với những vấn đề về luật định cùng với việc tốn kém thời gian và chi phí trong vấn đề phối hợp với các hệ thống hiện hành. Các chính phủ và ngân hàng phản đối thay đổi vì quy mô và chi phí thay thế hệ thống hiện thời quá lớn.

• Đồn thổi: Có rất nhiều đồn thổi xoay quanh khả năng của các hệ thống dựa trên nền tảng Blockchain. Blockchain chỉ là một hình thức dữ liệu mới, không phải một giải pháp quyền năng như thường bị phóng đại. Công nghệ này cũng chưa được kiểm chứng trên quy mô lớn hoặc các ứng dụng thực tiễn khác ngoài lĩnh vực tiền ảo.

# Chương 6
# Blockchain và ngành công nghiệp tài chính

*"Công nghệ Blockchain tiếp tục tái định nghĩa không chỉ cách thức địa hạt giao dịch vận hành mà còn nền kinh tế tài chính toàn cầu nói chung."*

**- Bob Greifeld,** Giám đốc Điều hành Sàn Giao dịch Chứng khoán NASDAQ

Bitcoin là cách thức sử dụng rộng rãi và ổn định đầu tiên của công nghệ Blockchain và mau chóng thu hút sự chú ý của giới tài chính. Nhiều công ty dịch vụ tài chính không thấy nhiều tiềm năng ở Bitcoin cho đến khi họ xem xét kỹ hơn và hiểu rõ công nghệ Blockchain phía sau nó. Ngay khi họ nhận ra tiềm năng của công nghệ Blockchain, họ đã đầu tư hàng triệu đô la vào nghiên cứu, phát triển và tiếp nhận để phát triển Blockchain của chính họ.

Việc tận dụng công nghệ dựa trên nền tảng Blockchain trong giới tài chính có rất nhiều triển vọng. Khả năng của Blockchain trong việc xử lý thông tin nhanh hơn nhờ loại bỏ được các đơn vị trung gian có thể giúp giảm bớt chi phí đồng thời đẩy nhanh tốc độ. Năng lực này không chỉ được ứng dụng trong chuyển giao tiền tệ, buôn bán cổ phiếu, thanh toán, thỏa thuận và nhiều hoạt động khác thuộc phạm vi nghiệp vụ cốt lõi của các cơ sở tài chính.

Việc chuyển giao giá trị là một quá trình xử lý chậm chạp khi so sánh với độ dài trung bình của các giao dịch tài chính. Đôi khi phải

mất nhiều tuần để chuyển tiền tới các quốc gia với tốc độ giao dịch bất định tại thời gian giao dịch. Một sổ cái dựa trên nền tảng Blockchain không chỉ giảm được chi phí tính trên giá trị chuyển giao mà còn tăng tốc độ xử lý lên đáng kể vì loại bỏ được các kênh trung gian mà thông tin cần chuyển qua để kiểm nhận giao dịch.

Đối với các ngân hàng, công nghệ Blockchain cải thiện tốc độ giao dịch đồng thời loại bỏ được các lớp xác thực tính minh bạch trên giao dịch.

Các ngân hàng giải quyết các giao dịch trên sổ cái nội bộ, hoạt động này có thể được hoàn thành trong những khoảng thời gian xử lý khác nhau đối với mỗi ngân hàng. Điều này thường dẫn tới kết quả là một hoạt động chuyển giao tiền đã rời khỏi sổ cái của ngân hàng này nhưng nhiều ngày sau vẫn chưa xuất hiện trong sổ cái của ngân hàng kia.

Ở các nước đang phát triển nơi mà việc xử lý còn thủ công hơn có thể còn lâu hơn và dễ gặp sai sót. Việc thay thế quá trình này bằng Blockchain sẽ cho phép các ngân hàng xử lý một giao dịch trên sổ cái chung gần như ngay lập tức và mọi thành viên trong mạng lưới đều có thể thấy giao dịch đó.

Giao dịch cổ phiếu cũng tương tự như vậy. Các Blockchain có thể được tận dụng để giảm bớt thời gian xử lý giao dịch cũng như tăng độ chính xác trong giao dịch. Trên thực tế, NASDAQ đã thiết lập một Blockchain dùng để giao dịch cổ phiếu.

Trong thời gian gần đây, Blockchain mà NASDAQ đang vận hành được sử dụng vào buôn bán cổ phiếu tiền-IPO (pre-IPO), tức là chuyển giao quyền sở hữu cổ phần của các công ty nội bộ giữa các nhà đầu tư trước khi các công ty này được niêm yết trên sàn

giao dịch chứng khoán. Blockchain NASDAQ đang được sử dụng cho thấy thế giới đang gần với việc ứng dụng các hệ thống Blockchain trong nhiều ngành công nghiệp như thế nào.

Sau khi giao dịch đầu tiên trong đó quyền sở hữu cổ phần được chuyển giao giữa các nhà đầu tư, Bob Greifeld tuyên bố đó là khoảnh khắc trọng đại trong việc ứng dụng công nghệ Blockchain và là bước tiến quan trọng trong lĩnh vực tài chính toàn cầu.

Bất kể lợi ích tiềm tàng của công nghệ Blockchain to lớn đến đâu, liệu các tổ chức tài chính có sẵn sàng áp dụng công nghệ này không?

Họ có sẵn lòng tin rằng hàng triệu và có khi là hàng tỷ đô la giá trị giao dịch sẽ được xử lý bằng công nghệ Blockchain không?

Đáp án ngắn gọn, có.

Ngành công nghiệp dịch vụ tài chính là một trong những ngành đầu tiên vui vẻ thừa nhận các lợi ích đến từ việc sử dụng công nghệ Blockchain.

Nhiều công ty đã và đang dùng công nghệ Blockchain, chẳng hạn như NASDAQ trong ví dụ trên. Gần như mọi tổ chức tài chính trọng yếu trên thế giới hiện nay đang tham gia phát triển công nghệ Blockchain thông qua việc phát triển nội bộ hoặc liên doanh với các công ty khác.

NASDAQ, Visa, Citibank, Capital One đã và đang đầu tư hơn 30 triệu đô la vào trang web chain.com để thiết lập sổ cái phân tán cho các giao dịch giữa các tổ chức tài chính.

Ripple là mạng lưới thanh toán có thể sử dụng để chuyển giao nhiều loại tiền tệ và hàng hóa khác nhau, hoặc bất kỳ giá trị nào dùng sổ cái phân tán.

Mạng lưới thanh toán Ripple đang được các ngân hàng và tổ chức tài chính tầm cỡ trên khắp thế giới sử dụng như một mạng lưới thanh toán cho phép các ngân hàng truyền gửi những khoản chi trả quốc tế ngay lập tức với chi phí thấp hơn nhiều so với các phương thức vốn có.

Hiện nay, 15 trong số 50 ngân hàng đứng đầu thế giới đang làm việc với Ripple để phát triển nền tảng Blockchain.

Paolo Cederle, đến từ Unicredit, đã nói, "Blockchain và các công nghệ liên quan là sự thay đổi khuôn mẫu nhận thức thoát khỏi hoàn cảnh hiện tại và đang dần trở thành trọng tâm phát triển công nghệ đối với chúng ta. Nhờ quan hệ đối tác với Ripple, chúng ta đang hoàn thiện hóa hoạt động thanh toán toàn cầu với vai trò như một trong những ngân hàng tầm cỡ đầu tiên triển khai công nghệ tài chính phân tán trong bối cảnh thương mại."

Công ty công nghệ R3 đã làm việc với 25 ngân hàng trọng yếu bao gồm Wells Fargo, JP Morgan và Citibank. Các công ty tham gia vào dự án này được gọi chung là Hiệp hội R3. R3 là công nghệ dữ liệu phân tán quy tụ nhiều nhà phát triển trứ danh đến từ Bitcoin Core, mật mã học và ngành công nghiệp công nghệ. Sổ cái phân tán mà họ tạo ra khác với Blockchain nhưng lại có nhiều điểm tương đồng. Mười một ngân hàng trong tập đoàn R3 đã kết nối với sổ cái phân tán R3.

Một cái tên nổi tiếng khác đang phát triển công nghệ Blockchain là Ngân hàng Anh. Họ nói rằng họ sẽ cam kết thay đổi nền tảng cơ sở dữ liệu và áp dụng Blockchain. Ngân hàng Anh có một đội tập trung riêng vào Blockchain, tuyên bố rằng đó là bước đổi mới công nghệ then chốt của họ.

Ngân hàng Anh hy vọng tận dụng được công nghệ này để tăng cường khả năng phòng chống các cuộc tấn công mạng ngày một gia tăng, giúp hệ thống của họ chấp nhận các khoản thanh toán phi ngân hàng, từ đó công nghệ dựa trên nền tảng Blockchain sẽ được kiểm chứng trên các hệ thống quyết toán tổng tức thời, giải quyết hàng trăm, hàng triệu giao dịch ngân hàng mỗi ngày.

Estonia là quốc gia đang sử dụng công nghệ Blockchain. Chính phủ Estonia đi tiên phong trong việc ứng dụng công nghệ kỹ thuật số vào các hoạt động chính phủ bằng cách phát triển các Blockchain phục vụ lưu trữ hồ sơ nhận diện và sức khỏe với các lĩnh vực khác như thu thuế, cùng với việc bầu cử dự kiến được xây dựng trên những cơ sở này.

Công nghệ Blockchain đang được nhiều ngân hàng trung tâm và ngành công nghiệp tài chính ứng dụng nhanh chóng, đồng thời nó cũng trở nên phổ biến hơn với các tổ chức ngoài lĩnh vực tài chính. Chương tiếp theo sẽ xem xét các công ty không thuộc lĩnh vực tài chính đang sử dụng công nghệ mới này để thay đổi các ngành công nghiệp khác như thế nào.

**Điểm Cốt Lõi:**

• Quá trình chuyển giao giá trị giữa các công ty và các quốc gia hiện nay đang rất chậm. Công nghệ Blockchain giúp tăng cường tốc độ giao dịch với tiềm năng chuyển giao tức thì.

• Công nghệ Blockchain có thể thay thế các lớp xác thực với tính minh bạch của các giao dịch.

• Nhiều ngân hàng, ngân hàng trung tâm, chính phủ và các công ty tài chính đã sử dụng công nghệ Blockchain hoặc đang nghiên cứu, phát triển công nghệ này.

• Hoạt động giao dịch cổ phiếu liên quan tới việc chuyển giao quyền sở hữu giữa nhiều người. Các Blockchain có thể được tận dụng để thay thế các bên trung gian và quá trình thực hiện tại NASDAQ đều được triển khai trên một Blockchain.

• Nhiều chức năng quyết toán và hành chính mà các tổ chức tài chính sử dụng đã lỗi thời và rất thủ công. Những chức năng này đều có thể được thay thế bằng các Blockchain và sổ cái phân tán.

# Chương 7
# Blockchain và những ngành công nghiệp ngoài lĩnh vực tài chính

*"Blockchain và các công nghệ liên quan là sự thay đổi khuôn mẫu nhận thức thoát khỏi hoàn cảnh hiện tại và đang dần trở thành trọng tâm phát triển công nghệ đối với chúng ta."*

**- Paolo Cederle,** Tổng giám đốc Công ty Giải pháp Tích hợp trong Kinh doanh Unicredit

Trong chương trước, chúng ta đã thấy ngành công nghiệp tài chính nhanh chóng áp dụng công nghệ Blockchain như thế nào. Dù rằng Blockchain có mối liên hệ chặt chẽ với các hoạt động thanh toán và giao dịch, chủ yếu vì khởi đầu với Bitcoin, tiềm năng của công nghệ Blockchain to lớn hơn rất nhiều so với địa hạt tài chính và thanh toán.

Blockchain có tiềm năng thay đổi gần như mọi ngành công nghiệp trên thế giới. Các dự án phát triển cho thấy công nghệ Blockchain có ảnh hưởng đến nhiều mặt trong đời sống thường nhật.

Trong chương này, chúng ta sẽ thảo luận về tiềm năng ứng dụng của Blockchain qua các ví dụ về những công ty đang tạo dựng hệ thống dựa trên nền tảng Blockchain.

**Quản Lý Nhận Dạng Và Nhận Diện Kỹ Thuật Số**

Quản lý nhận dạng sử dụng công nghệ Blockchain là tiến bộ then chốt giúp mở đường cho các hoạt động bảo mật và cơ sở nền tảng của nhiều ngành công nghiệp. Nếu bạn có thể tin rằng ai đó đúng là người như họ tuyên bố, vậy bạn có thể kết nối điều đó với một chuỗi những chuyện khác.

Công nghệ Blockchain giải quyết được nhiều vấn đề tồn đọng nhờ nhận diện kỹ thuật số. Hiện nay, tạo hình ảnh nhận diện giả hoặc trộm cắp nhận dạng trực tuyến của ai đó tương đối dễ dàng. Các mật khẩu không đủ an toàn và các cơ sở dữ liệu tập trung dễ bị tấn công. Một khi cơ sở dữ liệu tập trung bị xâm nhập, nó có thể cho phép tiếp cận tới toàn bộ dữ liệu khách hàng được lưu trữ trong hệ thống.

Hệ thống nhận diện dựa trên nền tảng Blockchain cung cấp các chữ ký số sử dụng mật mã học. Những chữ ký này là độc nhất vô nhị, không thể chối bỏ, bảo mật và gần như không thể sao chép hoặc truy cập khi không được cấp quyền.

Hoạt động nhận diện dựa trên nền tảng Blockchain có triển vọng thực sự khi chính phủ Estonia và các công ty như ShoCard đang xây dựng hệ thống nhận diện trên Blockchain.

Trong tương lai, công nghệ này cũng có thể được sử dụng trong việc nhận diện kỹ thuật số, hộ chiếu, bằng lái xe, thẻ cư trú, giấy khai sinh, giấy đăng ký kết hôn và nhiều mẫu giấy tờ nhận diện khác.

**Bầu Cử Kỹ Thuật Số**

Sau khi xây dựng công nghệ cho phép sử dụng nhận diện kỹ thuật số và chữ ký kỹ thuật số, chứng thực danh tính một người

trong một loạt các giao dịch và hoạt động trực tuyến khác nhau trở nên dễ dàng hơn.

Bầu cử kỹ thuật số là một công nghệ đã được triển khai không mấy thành công tại nhiều quốc gia vì rủi ro bảo mật và những quan ngại về tính riêng tư.

Estonia, Đan Mạch và Na Uy đã thử nghiệm bầu cử kỹ thuật số nhưng chỉ Estonia thực hiện thành công bầu cử kỹ thuật số trên quy mô lớn.

Đan Mạch, đã áp dụng công nghệ Blockchain trên quy mô bầu cử nhỏ với Liên Minh Tự Do (Liberal Alliance), một đảng phái chính trị của Đan Mạch ứng dụng hệ thống bầu cử dựa trên nền tảng Blockchain vào năm 2014.

Bằng cách sử dụng hệ thống bầu cử dựa trên nền tảng Blockchain, một cử tri có thể kiểm tra xem lá phiếu của họ đã được gửi thành công chưa, nhưng vẫn duy trì được tính riêng tư và bảo vệ được danh tính của họ. Cách này cũng giúp nhiều người có thể tham gia bầu cử hơn, tăng cường tỷ lệ tham gia bỏ phiếu bầu cử.

**Lập Hồ Sơ Y Tế Và Chăm Sóc Sức Khỏe**

Blockchain cung cấp một sổ cái phân tán mà khi thay đổi được đưa vào một sổ, tất cả các sổ khác sẽ cập nhật đồng thời. Điều này đảm bảo rằng mọi người có dữ liệu hợp lệ mới nhất giống với mọi bản sao lưu trên mạng lưới.

Công nghệ này sở hữu rất nhiều tiềm năng để được ứng dụng trong lĩnh vực chăm sóc sức khỏe. Nếu bạn từng đến gặp một hoặc nhiều bác sĩ hay bệnh viện, bạn sẽ nhận ra rằng những nơi đó cần đủ loại giấy tờ lịch sử bệnh án, chứng dị ứng và nhiều vấn đề y tế

khác mà bạn có lẽ phải điền rất nhiều lần trước khi tới địa điểm khác.

Lưu trữ loại thông tin này trên cơ sở dữ liệu y tế chung sẽ đồng nghĩa với việc bác sĩ, bệnh viện, bác sĩ phẫu thuật, y tá và các chuyên gia y tế đều có thể truy cập dữ liệu chung về một bệnh nhân. Họ sẽ có đầy đủ chi tiết về hồ sơ sức khỏe, từ đó giúp tiết kiệm thời gian và đưa ra quyết định toàn diện hơn khi chữa trị cho bệnh nhân.

Công nghệ này còn có khả năng lớn trong việc cứu sống một bệnh nhân khi họ phải phẫu thuật khẩn cấp. Các dữ liệu về những vấn đề sức khỏe quan trọng, nhóm máu, chứng dị ứng với loại thuốc nào đó, số điện thoại khẩn cấp, phương án trị liệu hiện tại, hoặc các vấn đề khác đều có thể được truy cập ngay lập tức khi cần thiết.

Những chi tiết về tiền sử bệnh tật của một bệnh nhân còn giúp trả lời đầy đủ nguyên nhân gây ra các vấn đề sức khỏe hiện tại của bệnh nhân đó. Khi bác sĩ khám bệnh gặp tình trạng nào đó, có lẽ họ không tìm ra nguyên do đáng báo động nào, nhưng nếu khám bệnh kết hợp với cơ sở dữ liệu bệnh án chi tiết, thì những biểu hiện dường như không liên quan lại có thể là triệu chứng của căn bệnh nào đó. Chuyên gia sức khỏe có thể phát hiện ra một triệu chứng khiến họ chỉ thấy được phần nào tình hình sức khỏe bệnh nhân, nhưng khi có thông tin bổ trợ, họ có thể chẩn đoán bệnh trạng tốt hơn.

Các công ty bảo hiểm y tế cũng có thể tiết kiệm được rất nhiều tiền bạc và thời gian nhờ việc tiếp cận được cơ sở dữ liệu này. Nếu bạn đang mua bảo hiểm y tế, nhiều công ty hiện nay đều yêu cầu bạn trả lời nhiều câu hỏi và kiểm tra y tế có thể khá phức tạp, tốn thời gian và không dễ chịu. Bằng cách cho phép công ty bảo hiểm

tiếp cận hồ sơ sức khỏe của bạn, họ sẽ thu được bức tranh tổng thể về tình hình sức khỏe của bạn từ đó có thể đưa ra các quyết định bảo hiểm dựa trên thông tin này mà không cần trải qua nhiều bài kiểm tra và câu hỏi mở rộng.

Nhiều công ty như Gem, Tieroim và Phillips Healthcare đang thực hiện lưu trữ hồ sơ sức khỏe trên Blockchain. Estonia là quốc gia dẫn đầu trong lĩnh vực này. Cơ quan eHealth của Estonia đã làm việc với công ty công nghệ Blockchain Guardtime để đưa dữ liệu y tế của các công dân vào cơ sở dữ liệu Blockchain an toàn.

Cơ quan Quản lý Đường bộ của Estonia nhận được giấy chứng nhận sức khỏe kỹ thuật số để đảm bảo rằng một cá nhân nào đó có thích hợp lái xe hay không trước khi tái cấp bằng lái cho người đó. Hoạt động này trước đây là một quá trình thủ công nhưng đang dần được tự động hóa và số hóa. Trong tương lai, các hồ sơ sức khỏe trên Blockchain có thể cập nhật kèm các thông tin như người đó có đủ khả năng lái xe hay không. Các phòng ban chính phủ sẽ có thể truy cập nguồn thông tin và các hệ thống có khả năng tự động cấp mới dựa theo dữ liệu lưu trong Blockchain hồ sơ sức khỏe này.

Một Blockchain hồ sơ sức khỏe sẽ mang đến nhiều lợi ích cho một cá nhân cũng như các chuyên gia y tế. Các cá nhân sẽ thấy được rõ ràng và chính xác về dữ liệu sức khỏe và hồ sơ y tế của họ. Không một chính phủ hay công ty nào có thể thay đổi thông tin này mà bệnh nhân, cùng với toàn bộ thành viên khác trong mạng lưới, không nhận ra.

Estonia đã thiết lập một cổng dành cho bệnh nhân, tại đó các công dân có toàn quyền truy cập lịch sử khám chữa bệnh, đơn thuốc, các chi tiết tham chiếu và thông tin bảo hiểm. Trong cổng

thông tin bệnh nhân, các công dân còn có thể đưa ra quyết định xem họ có muốn trở thành người hiến tạng hay không, hoặc lựa chọn phác đồ điều trị trong quá trình phẫu thuật.

Trong tương lai, toàn bộ cơ sở dữ liệu hồ sơ sức khỏe này có thể ở cả trên Blockchain. Nhờ quá trình tiên phong nhanh chóng của Estonia, điều này có thể trở thành hiện thực trong vài năm tới.

**Chứng Nhận Học Thuật**

Trường Holbertson tại California đang lên kế hoạch sử dụng công nghệ Blockchain vào việc chứng thực các bằng cấp học thuật của trường. Tình trạng giả mạo bằng cấp và bảng điểm đang trở nên phổ biến vì nhiều sinh viên mạo nhận những chứng chỉ mà họ không đạt được.

Blockchain sẽ tạo nên sự minh bạch về chứng chỉ và thành tích học tập của sinh viên. Công nghệ này cho phép xác minh dễ dàng các loại bằng cấp, xóa bỏ tình trạng gian lận, đồng thời tiết kiệm thời gian và tiền bạc tiêu tốn cho việc kiểm tra hoặc chứng thực thủ công.

**Âm Nhạc**

Ngành công nghiệp âm nhạc đang phát triển công nghệ dựa trên nền tảng Blockchain để phục vụ theo nhiều cách thức khác nhau. Có nhiều công ty đang tạo các ứng dụng dựa trên nền tảng Blockchain để thay đổi cách thức phân phối, chia sẻ và mua bán nhạc cũng như phương thức thanh toán bản quyền thương mại cho các nghệ sĩ.

Peertracks, Uio Music và Mycelia là một số ít các công ty khởi nghiệp hoạt động trên nền tảng dựa trên công nghệ Blockchain để các nghệ sĩ có thể trực tiếp bán tác phẩm âm nhạc của họ cho

người hâm mộ mà không cần tới đơn vị trung gian hoặc hãng thu âm.

Spotify gần đây đã mua lại Mediachain, một giải pháp dữ liệu được xây dựng dựa trên nền tảng Blockchain sẽ cho phép các nghệ sĩ tạo bản thu âm ca khúc kỹ thuật số trên Blockchain Bitcoin và hệ thống InterPlanetary File. Spotify đặt mục tiêu tận dụng nền tảng Blockchain từ Mediachain để thiết lập những khoản thanh toán minh bạch hơn và mau chóng hơn cho các nghệ sĩ.

**Lưu Trữ Đám Mây**

Các công ty lưu trữ dựa trên công nghệ điện toán đám mây như Google Drive, Dropbox và Microsoft OneDrive đã trở thành chuẩn mực lưu trữ dữ liệu và hồ sơ. Nhiều người sử dụng lưu trữ đám mây để lưu trữ mọi loại dữ liệu cá nhân và kinh doanh của họ.

Lưu trữ đám mây hiện nay đòi hỏi rất nhiều niềm tin vào công ty trung gian. Người ta thường đưa toàn bộ dữ liệu của họ lên một khu vực mà một công ty lưu trữ đám mây chỉ yêu cầu mật khẩu truy cập có độ an toàn tiêu chuẩn. Các hệ thống lưu trữ đám mây tập trung dễ bị tấn công và các mật khẩu có thể giành được dễ dàng qua các thủ đoạn xâm nhập hoặc lừa đảo đơn giản.

Hiện có nhiều công ty khởi nghiệp cung cấp giải pháp thay thế bằng cách kết hợp lưu trữ đám mây với công nghệ Blockchain.

Những công ty như Storj đã xây dựng hệ thống lưu trữ đám mây phi tập trung, một hệ thống ít gặp rủi ro tấn công và xâm nhập hơn. Lưu trữ đám mây được phân tán trên không gian lưu trữ trống trên các máy tính thành viên của mạng lưới, được mã hóa và chỉ chủ sở hữu mới có thể truy cập.

Siacoin và Filecoin là các công ty khởi nghiệp cũng hoạt động trên sự kết hợp giữa lưu trữ đám mây với công nghệ Blockchain như Storj.

**Dịch Vụ Thuê Mướn Xe Hơi**

Ngành công nghiệp xe hơi là một ngành khác đã biến đổi nhờ công nghệ Blockchain. Visa và DocuSign đã thiết lập quan hệ đối tác để phát triển một hệ thống cho thuê xe dựa trên nền tảng Blockchain.

Hoạt động này sẽ cắt giảm được nhiều việc giấy tờ và các khâu trung gian trong việc cho thuê mướn xe. Khách hàng chọn chiếc xe họ muốn thuê, nhận dạng kỹ thuật số của họ đã được đưa vào thông tin tài chính và giấy phép, họ chấp nhận một hợp đồng bảo hiểm thuê mướn và Blockchain được cập nhật hợp đồng cho thuê mới.

Thuê xe sân bay ngắn hạn đang tiến tới tự động hóa hơn nhờ loại bỏ được các loại giấy tờ và quy trình dài lê thê trước khi thuê xe. Công nghệ đang được phát triển để phục vụ nhận dạng kỹ thuật số và thuê xe dài hạn cũng có thể được ứng dụng cho việc thuê xe ngắn hạn.

Hồ sơ sức khỏe của nhiều công dân tại Estonia đã được số hóa và chuyển tới Cơ quan Quản lý Đường bộ để làm mới giấy phép tự động. Sự kết hợp thông tin Blockchain với nhận diện kỹ thuật số còn có thể được sử dụng để tự động cấp phép thuê xe trong tương lai.

**Dịch Vụ Đi Chung Xe**

Ứng dụng cung cấp dịch vụ đi chung xe như Uber đã thay đổi ngành công nghiệp xe taxi cũng như cách thức đi lại của hàng triệu người trên thế giới. Các công ty taxi đã từng độc quyền phương tiện

di chuyển xe hơi tại nhiều thành phố trên khắp thế giới với một tổ chức kiểm soát toàn bộ các giấy phép lái taxi cho một thành phố.

Mặc dù Uber và nhiều ứng dụng cung cấp dịch vụ đi chung xe khác đã đưa ra giải pháp thay thế cho taxi, các công ty này vẫn sử dụng cơ sở dữ liệu tập trung với các hệ thống do một công ty toàn quyền kiểm soát.

Dịch vụ đi chung xe được thực hiện giữa chủ xe và hành khách, tuy nhiên trong nền tảng dịch vụ đi chung xe hiện tại, vẫn còn tồn tại một đơn vị trung gian giữa hoạt động tương tác và giao dịch đi chung xe.

Công nghệ Blockchain sẽ giúp xóa bỏ mọi trung gian và tạo nên một ứng dụng dịch vụ đi chung xe phi tập trung.

Công ty khởi nghiệp La'zooz hiện đang hoạt động trên nền tảng dịch vụ đi chung xe phân tán dựa trên nền tảng Blockchain.

Dịch vụ đi chung xe là một ngành công nghiệp chuyển mình nhanh chóng để thay thế các nền tảng hiện hành bằng công nghệ Blockchain.

Sự an toàn của các tài xế cũng là một điều cần phải quan tâm, tuy nhiên ngay khi nhận dạng kỹ thuật số được kết nối với các Blockchain cơ quan đường bộ hoặc Blockchain thuê mướn xe được đưa vào sử dụng, dịch vụ đi chung xe cũng sẽ được kết hợp với các Blockchain đó.

**Tài Sản**

Tài sản, bất động sản và mua bán nhà đất là lĩnh vực hiện còn liên quan nhiều đến công việc giấy tờ và các trung gian môi giới để giao dịch được dễ dàng. Các giao dịch tài sản thường kèm theo hồ sơ khó thu giữ, dễ sai sót, thất lạc hoặc tốc độ xử lý chậm.

Hồ sơ và giao dịch tài sản dựa trên nền tảng Blockchain có thể nhanh chóng đẩy mạnh tốc độ cũng như tính minh bạch của các giao dịch tài sản, đồng thời giảm bớt chi phí giao dịch.

Các nền tảng thương mại bất động sản dựa trên công nghệ Blockchain có thể lưu trữ thông tin chứng khoán đất đai, chuyển giao giấy tờ sở hữu nhà đất, theo dõi những thay đổi quy hoạch và các kế hoạch xây dựng; và gần như mọi tài sản hiện nay đều do chính quyền địa phương và các công ty lưu giữ.

Ubitquity là một công ty khởi nghiệp hiện đang xây dựng một nền tảng tài sản dựa trên nền tảng Blockchain cho các ngân hàng, tổ chức tài chính, các công ty môi giới, thế chấp tài sản và nhiều đối tượng khác để theo dõi các tài liệu liên quan đến giao dịch tài sản.

**Dịch Vụ Thuê Mướn Nhà Ở**

AirBnB là ví dụ về một mô hình khác tương tự như Uber đã làm thay đổi cả một ngành công nghiệp bằng cách cung cấp dịch vụ giúp các cá nhân cho người khác ở nhiều thành phố trên khắp thế giới thuê mướn căn hộ của họ.

AirBnB đã loại bỏ các đơn vị trung gian như khách sạn và đại lý du lịch, đưa mọi người đến gần nhau để có thể giao dịch trực tiếp với nhau. Mặc dù đây là một bước tiến trong việc xóa bỏ các đơn vị trung gian, nó vẫn chỉ thay thế được những trung gian cung cấp các dịch vụ giúp đơn giản hóa giao dịch giữa mọi người.

Các nền tảng cung cấp dịch vụ cho thuê căn hộ và khách sạn dựa trên nền tảng Blockchain có thể vận hành tương tự như AirBnB nhưng không cần đến các đơn vị trung gian giúp đơn giản hóa toàn bộ các giao dịch và đặt chỗ. Những điều này có thể được mọi người thực hiện trực tiếp trên Blockchain.

**Ngành Công Nghiệp Du Lịch**

Ngay cả những hệ thống đặt phòng khách sạn truyền thống cũng có thể được thay thế bằng các hệ thống đặt phòng dựa trên nền tảng Blockchain.

John Guscic, Giám đốc Điều hành Webjet nói rằng, "Cứ 25 giao dịch đặt phòng khách sạn trên khắp thế giới lại có 1 giao dịch kết thúc trong cảnh một người cung cấp dịch vụ nhưng không được trả tiền".

Điều này phát sinh do quá nhiều đơn vị trung gian liên quan trong ngành công nghiệp đặt phòng du lịch và khách sạn, nơi việc đặt phòng có thể bị lỗi hoặc không được thanh toán chính xác. Một hệ thống đặt phòng dựa trên nền tảng Blockchain sẽ tạo ra một hệ thống đặt phòng rõ ràng hơn và ít sai sót hơn.

Webjet hiện đang làm việc với Microsoft để phát triển một hệ thống dựa trên nền tảng Blockchain cho ngành công nghiệp du lịch, tuy nhiên chưa có khoảng thời gian ra mắt cụ thể.

**Các Chương Trình Phần Thưởng/Khách Hàng Trung Thành**

Những chương trình Phần thưởng/Khách hàng Trung thành rất phổ biến trong nhiều ngành công nghiệp, từ các quán cà phê địa phương tới hãng hàng không lớn. Tuy nhiên, những chương trình phần thưởng vận hành rất tốn kém, dễ bị lừa đảo và các khách hàng thường không thỏa mãn với những phần thưởng nhận được hoặc quy trình kiểm tra thu chi để trao thưởng.

Công nghệ Blockchain có thể là giải pháp cho nhiều vấn đề tồn đọng trong các chương trình Phần thưởng/Khách hàng Trung thành hiện nay. Công ty dịch vụ tài chính Deloitte đã phát hành một chuyên đề có tên "Ứng dụng Blockchain vào chương trình Phần thưởng/

Khách hàng Trung thành" trong đó nghiên cứu cách thức các chương trình tặng thưởng dựa trên nền tảng Blockchain có thể đem lại lợi ích cho công ty và khách hàng như thế nào.

Bài viết còn nhận định rằng các chương trình khách hàng trung thành hiện nay đang gặp tình trạng ít khách hàng tham gia, thời gian xử lý chậm, gian lận và chi phí vận hành cao. Một chương trình tặng thưởng dựa trên nền tảng Blockchain sẽ minh bạch hơn, tiết kiệm được rất nhiều chi phí và thời gian xử lý, đồng thời tăng cường độ bảo mật.

Khi một giao dịch diễn ra, khách hàng sẽ nhận được điểm trung thành, quá trình tặng điểm này sẽ diễn ra ngay lập tức thay vì quá trình xử lý số dư của khách hàng chậm chạp hiện nay. Nhiều công ty đã phối hợp rất trơn tru các chương trình khách hàng trung thành cho phép nhiều cơ hội tăng thêm giá trị cho khách hàng và cơ hội kinh doanh tiềm năng bằng cách kết hợp với các công ty dịch vụ bổ sung.

Một công ty khởi nghiệp có tên Loyyal đã làm việc với nhiều công ty về công nghệ, kế toán và nhiều lĩnh vực khác để xây dựng một chương trình khách hàng trung thành dựa trên nền tảng Blockchain. Với sự minh bạch cao, chi phí được tiết giảm và tốc độ được cải thiện, nhiều chương trình Phần thưởng/Khách hàng Trung thành sẽ đến với các công ty và khách hàng của họ.

**Dự Đoán Và Đầu Tư**

Lĩnh vực đầu tư đã bắt đầu thay đổi nhờ có sự xuất hiện của nhiều công ty khởi nghiệp hoạt động dựa trên nền tảng Blockchain. Không chỉ là đầu tư trong trò may rủi ở những sự kiện thể thao mà

toàn bộ ngành công nghiệp về phân tích và dự đoán, bao gồm phân tích thị trường tài chính và dự báo tình hình.

Một trong những đồng tiền ảo lớn mạnh nhanh nhất là Augur, đồng tiền này đã tạo nên cả một thị trường giao dịch các hợp đồng dự đoán nơi mọi người có thể suy đoán và thu lợi từ kết quả giao dịch.

Augur sẽ là một nền tảng phi tập trung giúp dự đoán những khả năng xảy ra của bất cứ giao dịch nào được dự báo. Hệ thống này được xây dựng dựa trên quá trình nghiên cứu cho thấy thị trường giao dịch các hợp đồng dự đoán đã được kiểm chứng là chính xác hơn nhiều so với các cuộc thăm dò ý kiến hay điều tra, từ các chuyên gia và phân tích viên.

Trong thăm dò ý kiến, nhiều người thường trả lời những gì họ muốn diễn ra, chứ không phải những gì họ nghĩ sẽ diễn ra. Đây thường là lý do tại sao kết quả bầu cử và thăm dò dư luận có thể hoàn toàn sai lệch, vì kết quả khác xa so với dự báo thăm dò dư luận. Các thị trường giao dịch hợp đồng dự đoán thường nhắc mọi người rằng "miệng ở đâu nhét tiền vào đó", tức là thể hiện niềm tin bằng hành động chứ không phải lời nói; và vì thế, số tiền đầu tư mạo hiểm vào kết quả sự kiện diễn ra sẽ ngày càng chính xác hơn.

**Hợp Đồng Thông Minh**

Các dẫn chứng trong chương này cho thấy công nghệ Blockchain có thể trở thành phát kiến to lớn tiếp theo trên khắp các ngành công nghiệp. Những dẫn chứng này chỉ là phần nổi của tảng băng chìm về tiềm năng của công nghệ Blockchain. Nhiều ứng dụng công nghệ Blockchain sẽ sử dụng các hợp đồng thông minh.

Trong chương sau, chúng ta sẽ tìm hiểu về hợp đồng thông minh, các ứng dụng phân tán, nền tảng Ethereum và nhiều dẫn chứng khác về tiềm năng của công nghệ Blockchain.

**Điểm Cốt Lõi:**

• Không chỉ các công ty dịch vụ tài chính mới sử dụng các hệ thống dựa trên nền tảng Blockchain. Công nghệ Blockchain còn có khả năng ứng dụng rộng rãi trong nhiều lĩnh vực công nghiệp khác.

• Công nghệ dựa trên nền tảng Blockchain có thể được sử dụng để chuyển giao và lưu trữ gần như mọi loại giá trị.

• Nhiều công ty đã phát triển hệ thống Blockchain của riêng họ, vì một số hệ thống dựa trên nền tảng Blockchain đã trở nên khả dụng và được đưa vào hoạt động.

• Trong tương lai, các đơn vị trung gian và các nền tảng có thể được thay thế bằng các nền tảng Blockchain.

• Công nghệ Blockchain đang dần được đưa vào thực tiễn nhiều hơn mọi người nhận thấy. Trong vài năm tới, rất có khả năng một loạt các ngành công nghiệp sẽ sử dụng công nghệ Blockchain.

# Chương 8
# Nền tảng Ethereum, hợp đồng thông minh và các ứng dụng phi tập trung

*"Trao cho người dùng khả năng truy cập dễ dàng tới nhiều loại tài sản kỹ thuật số đa dạng trên Blockchain, đặc biệt các thẻ liên kết với tài sản thực, là yếu tố tiên quyết để đưa công nghệ Blockchain lên tầm cao mới…"*

**- Vitalik Buterin,** Nhà nghiên cứu và đồng sáng lập Ethereum

**Giới Thiệu Về Ethereum**

Ethereum là bước tiến tương lai của công nghệ Blockchain. Ethereum được xây dựng trên cùng các kỹ thuật nền tảng như Blockchain Bitcoin nhưng nắm giữ nhiều tiềm năng phát triển công nghệ Blockchain.

Ethereum là một Blockchain với ngôn ngữ lập trình cho phép các ứng dụng và hợp đồng thông minh hoạt động trên Blockchain. Điều này cũng cho phép các nhà phát triển tạo ra các chương trình hoạt động trên một Blockchain đồng thời sử dụng công suất tính toán của hàng ngàn máy tính kết nối vào mạng lưới Blockchain.

Gần như mọi ứng dụng đang vận hành trên máy tính ngày nay đều có tiềm năng vận hành trên một Blockchain. Nhờ tận dụng được mạng lưới Ethereum, các lập trình viên có thể mau chóng và dễ dàng tạo nên nhiều ứng dụng mà không cần phải tự lập Blockchain và đồng tiền ảo của riêng họ.

Mạng lưới Ethereum sử dụng đồng tiền ảo "Ether" hoạt động với tư cách tiền tệ của mạng lưới. Ether được trao đổi như một cách thức chi trả cho việc vận hành các ứng dụng phi tập trung trên mạng lưới.

Đồng tiền ảo Ether là đồng tiền ảo lớn thứ hai trên thế giới vì giá trị vốn hóa thị trường chỉ đứng sau Bitcoin với con số lên đến hơn 10 tỷ đô la.

**Sự Khác Biệt Giữa Ethereum Và Bitcoin**

Điểm khác biệt chính giữa Ethereum và Bitcoin là: Bitcoin được sử dụng chủ yếu như một sổ cái phân tán cho các giao dịch tài chính trong khi Ethereum được thiết kế để sử dụng như một nền tảng điện toán phân tán để vận hành các ứng dụng.

Bitcoin có thể sử dụng để thanh toán hàng hóa và dịch vụ tại bất cứ nơi nào đồng tiền này được chấp nhận, còn đồng tiền ảo Ether của mạng lưới Ethereum được thiết kế cho các lập trình viên sử dụng để chi trả công suất tính toán trên mạng lưới khi vận hành các ứng dụng phi tập trung.

Ethereum và Bitcoin đều là tiền kỹ thuật số nhưng nói chung mục đích sử dụng của chúng khác nhau. Đặc điểm của Ether là đồng tiền này không được thiết kế như một giải pháp thanh toán thay thế, mà là để thúc đẩy các lập trình viên sáng tạo và vận hành ứng dụng trong mạng Ethereum.

Nói ngắn gọn: Bitcoin, chủ yếu là một đồng tiền dùng trong giao dịch tài chính. Ethereum thì đa diện hơn, nó có đồng tiền ảo riêng (đồng Ether ), nhưng đó không phải là tất cả. Đồng tiền này chỉ là một phần nhỏ của mạng lưới vì Ethereum còn sở hữu một nền tảng điện toán toàn diện ngoài công nghệ Blockchain.

**Những Lợi Ích Của Ethereum**

Vì mạng Blockchain Ethereum được vận hành bởi hàng ngàn máy tính trên khắp thế giới, các ứng dụng có thể được vận hành nhờ công suất tính toán của một mạng lưới máy tính toàn cầu đồ sộ.

Một trong những vấn đề với mạng lưới Bitcoin là, dù mạng này mạnh hơn cả những siêu máy tính hàng đầu thế giới cộng lại nhưng công suất xử lý của nó lại bị lãng phí vào việc tạo ra những số ngẫu nhiên để thêm các khối vào Blockchain.

Ethereum đưa toàn bộ các máy tính trong mạng lưới kết nối lại với nhau và công suất xử lý của chúng lên mức hiệu dụng cao hơn, từ đó giúp các lập trình viên tạo ra nhiều ứng dụng vận hành nhờ công suất xử lý gộp của mạng lưới cùng công nghệ Blockchain.

Các lập trình viên không cần tạo lập Blockchain của riêng họ và kết nối máy tính vào đó. Ethereum đã xây dựng mạng lưới các máy tính trên Blockchain Ethereum.

Nền tảng Ethereum còn có Máy Ảo Ethereum và ngôn ngữ lập trình Solidity. Solidity có thể được sử dụng để sáng tạo nên những ứng dụng phi tập trung hoặc các hợp đồng thông minh mà sau đó được Máy Ảo Ethereum thông dịch và vận hành trên Blockchain.

**Các Ứng Dụng Phi Tập Trung (dApps)**

Các ứng dụng phi tập trung là ứng dụng có mã nguồn mở, không chịu sự kiểm soát của một cá nhân hoặc đối tượng nào, và chạy trên Blockchain phân tán hoặc mạng lưới máy tính.

Các ứng dụng phi tập trung không có máy chủ trung tâm, người dùng liên hệ với nhau thông qua các kết nối đồng cấp.

Các ứng dụng thông thường đều chịu sự kiểm soát của một đối tượng, chạy trên một máy chủ trung tâm và dễ bị tấn công hoặc gặp

thời gian chết do máy chủ rơi vào trạng thái ngoại tuyến.

Một ứng dụng phi tập trung không có máy chủ hoặc đối tượng đơn lẻ nào kiểm soát, nó hoạt động trên một mạng máy tính và các thay đổi đều do người dùng quyết định.

Không có vấn đề nghiêm trọng rằng máy chủ có thể bị sập hoặc bị tấn công. Nếu một máy tính trên mạng lưới thoát tuyến, ứng dụng không bị ảnh hưởng vì còn hàng ngàn máy khác đang vận hành ứng dụng vào thời điểm đó.

Ngay cả khi một máy tính trong mạng lưới bị tấn công, cũng không thể thực hiện các thay đổi trên ứng dụng vì cần phần lớn mạng lưới phải đồng thuận với thay đổi đó.

**Hợp Đồng Thông Minh**

Hợp đồng thông minh là những hợp đồng được viết bằng mã máy tính và hoạt động trên một Blockchain hoặc sổ cái phân tán.

Chúng sẽ tự động xác thực, xử lý và ép buộc thực hiện hợp đồng dựa theo thuật ngữ được viết trong mã. Các hợp đồng thông minh có thể là dạng tự xử lý và tự buộc phải thực hiện một phần hoặc toàn bộ.

Các hợp đồng thông minh có thể được sử dụng để trao đổi bất kỳ giá trị nào, như đã đề cập trong chương về tiềm năng ứng dụng của Blockchain, nhiều ngành công nghiệp đang tận dụng công nghệ Blockchain sẽ sử dụng các hợp đồng thông minh.

Khi chạy trên Blockchain, hợp đồng thông minh vận hành tự động. Nếu các điều kiện của một hợp đồng được thỏa mãn, các khoản thanh toán hoặc giá trị sẽ được trao đổi dựa theo thuật ngữ trên hợp đồng. Tương tự như vậy, nếu các điều kiện trong hợp đồng

không được thỏa mãn, các khoản thanh toán có thể bị từ chối dù đã được viết trong hợp đồng.

Các hợp đồng thông minh hoạt động vì chúng được lập trình trên một mạng lưới máy tính phi tập trung trên Blockchain, nhờ đó loại bỏ được rủi ro về những thay đổi trái phép, gian lận, lỗi máy chủ hoặc tình trạng bất tuân thuật ngữ trong hợp đồng. Những hợp đồng này tự động xử lý, trao đổi giá trị và các khoản thanh toán giữa mọi người mà không cần sự xuất hiện của luật sư hay tòa án để ép buộc họ.

Dữ liệu nhập trên Blockchain được gắn nhãn thời gian và không thể thay đổi được. Điều này tạo nên một nền tảng hoạt động lý tưởng cho các hợp đồng vì bất cứ thay đổi nào về hợp đồng đều được ghi lại thời gian, và những phiên bản trước đó còn được lưu lại trên Blockchain.

Các hợp đồng được lưu trữ, các phiên bản mới được tạo ra trong khi các phiên bản trước đó vẫn được lưu trữ (cùng với nhãn thời gian chuẩn xác trên tất cả các bản biên tập và hiệu chỉnh). Điều này không chỉ giúp tạo ra bản tóm tắt các quy trình chính xác hơn, mà còn khiến tất cả các bên liên quan trung thực hơn về các giao dịch vì sổ cái không thể sửa đổi được.

Mạng lưới Blockchain này loại bỏ nhu cầu về bên trung gian để quản lý các giao dịch.

**Lợi Ích Của Hợp Đồng Thông Minh**

Một rủi ro với mạng lưới Bitcoin là nếu bạn mua một mặt hàng bằng Bitcoin, sau khi thực hiện thanh toán, không có gì bảo đảm rằng bạn sẽ nhận được món đồ đã mua. Cá nhân khác có liên quan

có thể quyết định không chuyển hàng hoặc tuyên bố rằng họ không nhận được khoản thanh toán đó.

Vì không có bên thứ ba làm trung gian giao dịch trên mạng Bitcoin, loạt hành động phản ứng thông thường như ngừng giao dịch, yêu cầu bồi hoàn hay liên hệ với đơn vị trung gian là không thể.

Các ví Bitcoin còn ẩn danh nên bạn có thể sẽ không có nhận được thông tin về nơi mà giao dịch được gửi đi. Nếu một giao dịch bị gửi nhầm địa chỉ thì bạn sẽ bị mất giao dịch cùng khoản tiền đó.

Các hợp đồng thông minh xử lý được nhiều rủi ro liên quan đến hoạt động giao dịch trong mạng lưới Blockchain. Các hợp đồng giao dịch có thể được sử dụng cho bất cứ giá trị nào có thể trao đổi được và có nhiều công ty đang phát triển các ứng dụng phi tập trung dựa trên nền tảng Blockchain có sử dụng hợp đồng thông minh.

Ascribe là một công ty khởi nghiệp trong lĩnh vực nghệ thuật, giúp đỡ nhiều nghệ sĩ khác nhau thiết lập quyền sở hữu tác phẩm và phát hành bản in số lượng hạn chế. Việc phát hành các tác phẩm nghệ thuật đánh số trong các phiên bản kỹ thuật số sử dụng một Blockchain để có thể tìm ngược lại tất cả tác phẩm ban đầu và giao dịch nguyên thủy trong những tác phẩm đó. Đó là một thị trường nơi các nghệ sĩ có thể quảng cáo và mọi người có thể mua bán các tác phẩm nghệ thuật từ trang web của họ.

UProov, một công ty luật và truyền thông, cung cấp các nhãn thời gian tức thời và có thể kiểm tra được trên mọi hình ảnh và phim trong mọi thiết bị số. Các hình ảnh và đoạn phim, đã gắn nhãn thời gian không thể thay đổi, có thể được coi như một bằng chứng rất có giá trị trong những vấn đề liên quan đến pháp luật.

BitProof, một công ty khác sử dụng Blockchain để thiết lập các nhãn thời gian, đã tạo ra một ứng dụng có thể dễ dàng tải từ điện thoại. Ứng dụng này kích hoạt các nhãn thời gian có thể xác minh trên từng phần của tài liệu mà bạn đang xem. Nó có thể truy nguyên các tác phẩm ban đầu trên Blockchain mà không thể sửa đổi được. Công nghệ này có tiềm năng loại bỏ nhu cầu về công chứng viên trong tương lai.

Warranteer là một công ty khác đã liên kết với GoPro và LG trong việc sử dụng hợp đồng thông minh để đưa giấy tờ bảo hành sản phẩm lên một Blockchain nơi nó có thể được truy cập, chuyển giao và lưu trữ dễ dàng. Mọi dấu vết biên tập, thay đổi, cập nhật và di chuyển đều có thể ghi lại trên Blockchain mà cả người bảo chứng và người được bảo chứng đều có thể truy cập vào bất cứ thời điểm nào.

Peertracks, Mycelia và Ujo Music là những công ty riêng biệt đều tập trung vào việc ứng dụng công nghệ Blockchain trong ngành công nghiệp âm nhạc. Cả ba công ty này đều sử dụng hợp đồng thông minh theo nhiều cách khác nhau với mục đích chính là loại bỏ các đơn vị trung gian như hãng thu âm, giúp các nhạc sĩ dễ dàng bán trực tiếp sản phẩm cho người hâm mộ và nhận được thanh toán từ đó.

Tín dụng vi mô là mô hình cho vay các khoản vay nhỏ, chủ yếu tại các quốc gia đói nghèo trên thế giới. Các khoản vay này khá nhỏ đối với các ngân hàng nhưng lại to lớn đối với người vay, vì thế có thể giúp họ bắt đầu kinh doanh, kiếm thu nhập và giúp đỡ gia đình.

Tín dụng vi mô đã đưa hàng triệu người trên thế giới thoát khỏi đói nghèo, giúp Mohamed Yunus giành được giải Nobel Hòa Bình vì

công trình về tín dụng vi mô của ông. Trước khi có mô hình hiện đại hóa tín dụng vi mô của Mohamed Yunus, hầu hết các ngân hàng đều không hỗ trợ các khoản vay nhỏ vì công việc giấy tờ tốn kém hơn nhiều so với lợi nhuận từ khoản vay.

Bảo hiểm vi mô lại không được nhìn nhận như một sự thay đổi mạnh mẽ như tín dụng vi mô. Công ty khởi nghiệp Stratumn hướng đến mục tiêu thay đổi ngành bảo hiểm vi mô bằng cách phối hợp với Lemonway để tạo ra một hệ thống bảo hiểm vi mô dựa trên nền tảng Blockchain có tên "LenderBot". LenderBot sẽ sử dụng hợp đồng thông minh trên Blockchain để thiết lập và quản lý các hợp đồng bảo hiểm vi mô.

Khi thảo luận về tương lai của Blockchain, thuật ngữ "Blockchain 2.0" thường xuyên được sử dụng để diễn tả bước phát triển tiếp theo của công nghệ này. Các ứng dụng phi tập trung cùng với hợp đồng thông minh nắm giữ tiềm năng đưa công nghệ Blockchain lên tầm cao mới. Tương lai của Blockchain sẽ xoay quanh các hợp đồng thông minh và ứng dụng phi tập trung. Blockchain 2.0 có rất nhiều khả năng sẽ tạo ảnh hưởng mạnh mẽ hơn rất nhiều so với ảnh hưởng của Bitcoin và công nghệ Blockchain nguyên bản đã tạo ra.

**Điểm Cốt Lõi:**

• Ethereum là nền tảng trên công nghệ Blockchain với ngôn ngữ lập trình cho phép các nhà phát triển kiến tạo và vận hành các ứng dụng phi tập trung và hợp đồng thông minh trên một nền tảng điện toán phân tán, mạnh mẽ và Blockchain trong nền tảng Ethereum.

• Đồng tiền và mạng lưới Bitcoin chủ yếu được sử dụng để giao dịch tài chính. Ethereum có đồng tiền "Ether" nhưng nền tảng này lại

được thiết kế để trao đổi công suất tính toán, chứ không chỉ các giao dịch tài chính ngoài nền tảng Ethereum.

• Các ứng dụng phi tập trung không có máy chủ hoặc đối tượng đơn nhất kiểm soát và có thể hoạt động trên toàn mạng lưới máy tính.

• Hợp đồng thông minh là các hợp đồng được viết bằng mã máy tính và vận hành trên một Blockchain hoặc sổ cái phân tán. Các hợp đồng thông minh sẽ tự động xác thực, xử lý và bắt buộc thực hiện hợp đồng dựa theo thuật ngữ được viết trên mã mà không cần đến bên thứ ba làm đơn vị trung gian như các luật sư và tòa án để ép buộc thực hiện hợp đồng.

• Bất cứ giá trị nào cũng có thể được trao đổi bằng cách sử dụng hợp đồng thông minh. Những hợp đồng này không chỉ liên quan tới các vấn đề pháp luật mà còn giảm bớt rủi ro trong giao dịch trên mạng lưới Blockchain, vì các giao dịch và các khoản thanh toán được mạng lưới xử lý tự động.

• Có nhiều công ty đang phát triển các hợp đồng thông minh và ứng dụng phi tập trung dựa trên công nghệ Blockchain trên nền tảng Ethereum.

• Nền tảng Ethereum là bước tiến tương lai của công nghệ Blockchain trong đó bao gồm hợp đồng thông minh và các ứng dụng phi tập trung, thường được gọi là "Blockchain 2.0".

# Chương 9
# Tương lai của Blockchain

*"Trong tương lai, tôi thấy một Blockchain công khai - nơi mà hoặc Bitcoin hoặc một công nghệ nào đấy mở ra trong tương lai, đó là cách đăng ký quyền sở hữu tất cả các loại tài sản, là cách chuyển giao quyền sở hữu các loại tài sản đó trong đúng một hệ thống mà tất cả những người thích hợp đều có thể đọc được còn những người không thích hợp thì không.*

*Sẽ rất đơn giản để tôi có thể chuyển tiền mua cổ phiếu IBM của bạn, hay bạn mua nhà của tôi. Mọi loại tài sản mà chúng ta gán cho một giá trị và muốn chắc chắn về người sở hữu, đều có thể được ghi nhận thông qua công nghệ này."*

**- James Smith,** Giám đốc Điều hành Elliptic

Như đã đề cập, công nghệ Blockchain có tiềm năng vươn tới mọi quốc gia, nền công nghiệp và các cá nhân trên hành tinh trong vòng vài thập kỷ tới. Nhiều dự đoán về tương lai của công nghệ Blockchain chỉ là những nhận định thiếu chứng cứ, nhưng không phải tiên đoán kiểu "sẽ có ô tô bay trong tương lai". Nhiều hệ thống dựa trên nền tảng Blockchain đã được phát triển trong nhiều ngành công nghiệp.

Bước tiến trong lĩnh vực đầu tư vào các dự án của doanh nghiệp và chính phủ mà công nghệ Blockchain đạt được trong vài năm vừa qua đã làm cho dự báo về một tương lai nơi công nghệ Blockchain

gắn kết với đời sống thường nhật của chúng ta trở nên vô cùng thực tế.

Nếu chúng ta quan sát các hệ thống dựa trên nền tảng Blockchain hiện tại, các ngành công nghiệp nơi chúng được ứng dụng và những xu hướng vừa xuất hiện, chúng ta có thể thấy hướng phát triển của hệ thống dựa trên nền tảng Blockchain.

**Mã Nguồn Mở Phi Tập Trung Và Mã Nguồn Đóng Tập Trung**

Xu hướng hiện nay trong phát triển Blockchain là Blockchain nên được phân tán với mã nguồn khả dụng công khai (mã nguồn mở) hay tập trung với mã nguồn riêng biệt do một tổ chức hoặc nhóm tổ chức (mã nguồn đóng) quản lý.

Những hợp phần ban đầu của công nghệ Blockchain định cho rằng Blockchain nên là mã nguồn mở và phi tập trung. Nhiều công ty và chính phủ thấy rằng các công nghệ Blockchain mã nguồn mở, phân tán rất xuất sắc; tuy nhiên họ lại không muốn đặc tính phân tán và mã nguồn mở của nó.

Điều này tương tự như những ngày sơ khai của máy tính cá nhân khi mà hầu hết các lập trình viên đều cho rằng phần mềm nên là mã nguồn mở và miễn phí cho mọi người. Bill Gates đã gặp phải rất nhiều chỉ trích vì đi ngược lại tư duy trên bằng việc đưa phần mềm vào hoạt động kinh doanh để được cấp phép và buôn bán. Mặc dù các phần mềm mã nguồn mở vẫn rất phổ biến, nhưng đa số các công ty phần mềm hiện nay không chia sẻ công khai mã nguồn của họ.

Ripple là một trong những dự án Blockchain nổi tiếng nhất và hiện nay đang là loại tiền ảo lớn thứ ba trên thế giới nhờ giá trị vốn hóa thị trường. Ripple là mã nguồn đóng và tập trung, được phân

phối trong một nhóm tuyển chọn gồm các tổ chức tài chính đóng vai trò sổ cái phân tán để giải quyết các giao dịch giữa họ.

Ripple vấp phải nhiều chỉ trích từ các cộng đồng mã nguồn mở, những nơi không muốn tương lai của công nghệ Blockchain là những Blockchain đóng, tập trung và thuộc quyền sở hữu của những tổ chức tài chính lớn.

Ethereum là đồng tiền ảo lớn thứ hai trên thế giới nhờ giá trị vốn hóa thị trường và một trong những mạng lưới Blockchain lớn nhất. Ethereum là mã nguồn mở và phi tập trung, cung cấp một nền tảng cho các lập trình viên tạo dựng các ứng dụng phi tập trung kèm các thẻ trên Blockchain sử dụng nền tảng Ethereum.

Có vẻ như chưa có dấu hiệu rõ ràng rằng các hệ thống dựa trên nền tảng Blockchain sẽ chọn các Blockchain tập trung/phân tán mã nguồn đóng hay Blockchain phi tập trung mã nguồn mở. Cả hai phương thức đều có sự đầu tư và phát triển to lớn vì mỗi phương thức có lợi ích phù hợp với những yêu cầu, tổ chức và cộng đồng khác nhau.

Công nghệ Blockchain có khả năng sẽ phát triển đồng thời cả hai hướng mạng lưới phi tập trung mã nguồn mở và mạng lưới tập trung mã nguồn đóng. Các chính phủ và các tổ chức lớn sẽ chọn một phương thức còn các lập trình viên cá nhân, những dự án quy mô nhỏ và các công ty khởi nghiệp sẽ chọn phương thức khác.

**Sổ Cái Phân Tán**

Hiệp hội R3 gồm các tổ chức tài chính trọng yếu là một hướng khác mà các công ty đang lựa chọn. Tổ chức này ban đầu phát trển một Blockchain, tuy nhiên đang chuyển dần sang sổ cái phân tán.

Mặc dù sổ cái phân tán của Hiệp hội R3 có nhiều lợi thế của Blockchain nhưng đó không phải Blockchain.

Sổ cái phân tán hiện nay đang có mối liên quan mật thiết với Blockchain, và có lập luận rằng sổ cái phân tán được dựa trên nền tảng Blockchain. Tuy nhiên, sổ cái phân tán có thể vận hành mà không cần sử dụng Blockchain.

Đa phần các công ty khởi nghiệp và các hoạt động phát triển được dựa trên nền tảng Blockchain, tuy nhiên sổ cái phân tán không dựa trên nền tảng Blockchain có thể là một xu hướng nổi lên trong tương lai.

**Ít Loại Tiền Ảo Hơn**

Vào thời điểm ban đầu của mọi ngành công nghiệp đang phát triển, luôn có rất nhiều công ty xuất hiện; tuy nhiên, khi các ngành công nghiệp và thị trường phát triển hơn, con số này giảm đi cho đến khi chỉ còn một vài doanh nghiệp hoặc thương hiệu lớn mạnh.

Vào đầu những năm 1900 khi xe hơi còn là công nghệ mới, có hàng ngàn hãng sản xuất xe hơi tại Mỹ; hiện nay, chỉ còn lại những công ty sản xuất tầm cỡ.

Mức độ giảm sút này không chỉ trong ngành sản xuất xe hơi mà còn rất phổ biến trong đa số các ngành công nghiệp và có thể cho thấy xu hướng các đồng tiền ảo trong tương lai. Hiện nay, có hàng ngàn đồng tiền ảo và tiền ảo được tạo ra mỗi ngày. Trong tương lai, nhiều khả năng chỉ còn lại một vài đồng tiền ảo lớn còn tồn tại và được phần đông chấp nhận như một hình thức thanh toán.

Xu hướng này đang diễn ra vì nhiều dự án Blockchain mới được ra đời có sử dụng các thẻ trên các Blockchain hiện thời như Ethereum thay vì tạo ra đồng tiền ảo riêng của họ.

**Nhiều Thẻ Blockchain Hơn**

Mặc dù nhiều khả năng con số tiền ảo sẽ giảm, nhưng số lượng thẻ trên nền tảng Blockchain sẽ tăng.

Thẻ, tương tự tiền ảo, có thể được trao đổi trên Blockchain nhằm phục vụ các mục đích mua sắm. Tuy nhiên, thẻ hoạt động trên một Blockchain có sẵn, và mỗi thẻ đại diện cho giá trị ban hành trên tiền tệ của Blockchain khác.

Ethereum là Blockchain nổi tiếng nhất về mô hình này. Blockchain Ethereum sử dụng đồng tiền nguyên bản có tên "Ether". Mọi người có thể xuất thẻ trên Blockchain Ethereum, các thẻ đại diện cho một giá trị và được sử dụng như một phương tiện trao đổi nhưng tận dụng Blockchain Ethereum và đồng tiền Ether sẵn có.

Thẻ cho phép các lập trình viên và các tổ chức sáng tạo nên những ứng dụng hoạt động trên một Blockchain mà không cần phải thiết lập và duy trì Blockchain hay tiền ảo riêng của họ.

**Blockchain 2.0 - Các Ứng Dụng Phi Tập Trung Và Hợp Đồng Thông Minh**

Blockchain 2.0 là thuật ngữ diễn tả chức năng mới của Blockchain đang tồn tại hiện nay so với mã nguồn nguyên thủy.

Nền tảng Ethereum đã hiện thực hóa việc thiết lập và vận hành các ứng dụng phi tập trung và hợp đồng thông minh trên Blockchain. Các hợp đồng thông minh, ứng dụng phi tập trung và nền tảng Ethereum đã được trình bày cụ thể trong phần trước của cuốn sách.

Các ứng dụng phi tập trung và hợp đồng thông minh xây dựng trên mạng lưới Ethereum hoặc các Blockchain hiện thời khác có sử dụng các thẻ thay vì tiền ảo là xu thế mới đang phát triển mạnh mẽ và không có dấu hiệu đi xuống.

**Nhiều Quy Định Và Chấp Thuận Hơn**

Vẫn còn nhiều chỉ trích và quan ngại sâu sắc về công nghệ Blockchain. Bitcoin là một ví dụ về tình trạng này, nhiều chính phủ tuyên bố rằng giao dịch quá riêng tư khiến nó dễ bị lợi dụng cho các mục đích phi pháp, rửa tiền và trốn thuế. Mặt khác, nhiều người lại phàn nàn rằng các cơ sở dữ liệu phi tập trung như Bitcoin, tình trạng công khai cho phép xem xét ví tiền ảo của bất cứ ai, số dư hiện có và các giao dịch khiến nó trở nên quá rõ ràng và thiếu riêng tư.

Nhiều chỉ trích được đưa ra sở dĩ vì Bitcoin là ứng dụng công nghệ Blockchain khả thi, được nhiều nơi chấp nhận, toàn cầu và nổi tiếng nhất trên thế giới. Blockchain vẫn còn trong những ngày sơ khai, liên quan mật thiết tới Bitcoin và nhiều loại tiền ảo và hàng trăm đồng tiền ảo mã nguồn mở đang được tạo ra mỗi tháng.

Trước đây, nhiều chính phủ phản đối Bitcoin vì cho rằng nó chỉ được sử dụng cho mục đích phạm pháp và rửa tiền. Quan niệm đó đã bắt đầu thay đổi khi công nghệ Blockchain được hiểu rõ hơn và các tổ chức tài chính ứng dụng công nghệ này vào thị trường tài chính. Các chính phủ hiện nay đang khuyến khích các công ty ngành Công nghệ Tài chính (FinTech) kinh doanh tại quốc gia của họ thông qua việc chấp nhận đồng tiền ảo như một hình thức thanh toán mới và đảm bảo rằng loại tiền này được quy định đúng đắn trong lãnh thổ quốc gia.

Nhật Bản gần đây đã hợp pháp hóa đồng Bitcoin là một hình thức thanh toán hợp lệ, Úc gần đây đã bỏ thuế tiền ảo đồng thời khuyến khích các công ty sử dụng công nghệ dựa trên nền tảng Blockchain để giao dịch tại Úc.

Các chính phủ sẽ tiếp tục cố gắng thu hút các công ty khởi nghiệp trong lĩnh vực Công nghệ Tài chính phối hợp với các ngân hàng, doanh nghiệp và các tổ chức tài chính để tạo việc làm, kích thích thương mại và phát triển nền kinh tế thông qua công nghệ mới dựa trên nền tảng Blockchain.

**Blockchain Trong Cuộc Sống Thường Nhật**

Dù ứng dụng phi tập trung mã nguồn mở được xây dựng trên các Blockchain sẵn có hay các Blockchain liên hợp cá nhân mới được tạo ra, việc sử dụng số lượng Blockchain sẽ tăng lên trong mọi mặt cuộc sống của chúng ta.

Nhiều cơ sở dữ liệu của doanh nghiệp và chính phủ đang sử dụng bảng tính lỗi thời hay sổ cái thủ công sẽ được thay thế bằng Blockchain. Những ngân hàng lớn đang phát triển Blockchain của riêng họ để xử lý các giao dịch, các khoản trong sổ cái, các trao đổi tiền tệ và hơn thế nữa.

Việc vận dụng công nghệ Blockchain có thể tiếp tục phát triển cho đến khi nó trở nên phổ biến như công nghệ cơ sở dữ liệu hiện đang được nhiều doanh nghiệp và chính phủ sử dụng. Đó cũng là một xu hướng Blockchain thay thế cho những phương án kinh doanh hiện thời trong đời sống.

Một trường hợp cho thấy xu hướng Blockchain thay thế đang tồn tại song song với nhiều phương án hiện thời là lưu trữ đám mây. Storj và Siacoin là các doanh nghiệp đang thiết lập hệ thống lưu trữ đám mây phi tập trung trên Blockchain. Mặc dù chúng không có khả năng sớm thay thế được Google Drive hay Dropbox, nhưng chúng đã tạo nên một phương án thay thế khi lựa chọn khu vực lưu trữ tài liệu trên đám mây.

Những đồn thổi rằng các hệ thống dựa trên nền tảng Blockchain sẽ biến đổi nhiều ngành công nghiệp hiện nay và thay thế nhiều công ty đã không thành hiện thực trong ngắn hạn nhưng có một xu thế rõ ràng là các phương án thay thế dựa trên nền tảng Blockchain sẽ tồn tại song song với những phương án hiện thời trong nhiều ngành công nghiệp.

Công nghệ Blockchain có lẽ không thay thể được những đơn vị trung gian hiện thời như ngân hàng, các công ty như Google hay Uber như một số người đã dự đoán, đặc biệt là trong ngắn hạn. Tuy nhiên, ngay cả khi các đơn vị trung gian không bị thay thế, bạn cuối cùng sẽ bắt gặp các công nghệ Blockchain từ các sổ cái Blockchain phân tán tại nơi làm việc, các hợp đồng thông minh, các ứng dụng phi tập trung hoặc có thể quyết định lựa chọn một giải pháp dựa trên nền tảng Blockchain thay thế cho các phương án hiện thời trong nhiều lĩnh vực của đời sống.

**Điểm Cốt Lõi:**

• Mã nguồn mở phi tập trung và mã nguồn đóng tập trung: Chưa có thiên hướng rõ ràng về tương lai phát triển của Blockchain. Blockchain phi tập trung mã nguồn mở sẽ được phát triển song song với Blockchain liên hợp/ tập trung mã nguồn đóng tùy theo những yêu cầu khác nhau.

• Sổ cái phân tán: Sổ cái phân tán không sử dụng Blockchain nhưng có nhiều lợi ích của một Blockchain là một xu thế có thể cạnh tranh với các sổ cái dựa trên nền tảng Blockchain trong tương lai.

• Ít loại tiền ảo hơn và nhiều thẻ Blockchain hơn: Một xu thế đang diễn ra là nhiều công ty sử dụng thẻ trên nền tảng Ethereum thay vì các Blockchain và tiền ảo của riêng họ. Xu thế này có lẽ đang

tiếp tục vì chức năng của nền tảng Ethereum cho phép sự phát triển của các ứng dụng phi tập trung và các hợp đồng thông minh.

• Blockchain 2.0: Công nghệ Blockchain hiện nay đã phát triển mạnh các chức năng như ứng dụng phi tập trung và hợp đồng thông minh vốn không phải là một phần trong mã Blockchain ban đầu. Blockchain 2.0 được coi như tương lai của công nghệ Blockchain trong đó những cải tiến này đã hiện thực hóa nó từ tiềm năng của Blockchain nguyên thủy.

• Nhiều quy định và chấp thuận hơn: Nhiều chính phủ và doanh nghiệp đã hướng tới việc chấp nhận tiền ảo như một hình thức thanh toán hợp pháp, đồng thời đầu tư mạnh mẽ vào công nghệ và hạ tầng cơ sở của Blockchain.

• Blockchain trong đời sống thường nhật: Mặc dù công nghệ dựa trên nền tảng Blockchain không phải cuộc cách mạng như dự đoán, nó vẫn có thể trở thành một phần trong cuộc sống hằng ngày thông qua sổ cái phân tán, các phương thức thanh toán hoặc giải pháp phần mềm thay thế cho những phương án hiện thời.

# Chương 10
# Hướng dẫn kỹ thuật về Blockchain

### Giới Thiệu Về Nội Dung Hướng Dẫn Kỹ Thuật Blockchain

Hướng dẫn kỹ thuật về cách thức Blockchain vận hành này là phần kết của cuốn sách vì có lẽ nội dung này không hấp dẫn với nhiều độc giả. Phần này sẽ thảo luận về những phương diện nâng cao như hàm băm và mật mã học liên quan đến Blockchain.

Nếu bạn không quá quan tâm đến mật mã học đằng sau Blockchain, bạn có thể bỏ qua phần này rồi đọc lại sau.

Danh sách tham khảo và bảng thuật ngữ sau chương này sẽ cung cấp thông tin chi tiết hơn về Blockchain, Bitcoin, Ethereum và các hợp đồng thông minh mà có thể bạn quan tâm.

### Chỉ Dẫn Kỹ Thuật Về Cách Thức Hoạt Động Của Blockchain

Chỉ dẫn này sẽ tập trung vào cách thức hoạt động của Blockchain Bitcoin vì đây là Blockchain nguyên bản mà tất cả các Blockchain khác đều được xây dựng dựa trên nền tảng này cũng sẽ hoạt động theo cách tương tự.

Blockchain Bitcoin sử dụng thuật toán SHA-256. Thuật toán SHA-256 sinh ra các mã băm 256-bit kích thước ổn định và độc nhất. Một mã băm tương tự như một mã bí mật sử dụng phương thức mã hóa nhằm ẩn giấu dữ liệu theo cách mà gần như không thể giải mã nếu không được cấp quyền.

Mã băm được tạo ra luôn có cùng độ dài. Bất kể bạn đưa vào một từ hay cả cuốn sách, bạn sẽ vẫn thu được một mã băm có độ dài không đổi đối với mọi khối lượng dữ liệu đầu vào.

Nếu bạn thay đổi một ký tự thì mã băm sẽ thay đổi hoàn toàn. Mã băm xuất hiện ngẫu nhiên mà không liên quan đến dữ liệu đầu vào. Gần như không thể tìm ra thông điệp ban đầu từ mã băm trừ phi bạn biết thông điệp ban đầu hoặc khóa cá nhân.

Dưới đây là một số ví dụ về mã băm sinh ra từ những từ và cụm từ khác nhau:

Mã băm của từ "Blockchain" với chữ B viết hoa:

b3f4e9b8455ea3ea20e60aae2cad91d8412a53
bc4f3834e3152f776eb4b44d4c

Mã băm của từ "Blockchain" với chữ b viết thường:

154a5318f688615ba779541d8753e0b7047f5b
a4b5cd7676d124008201803e73

Mã băm của từ "Blockchain" với chữ "block" và "chain" viết cách:

7ef554758e1810b1dec1f43ef6c2d0ff105b6398
7561fdb4f352d9433d231457

Đây là toàn bộ nội dung vở kịch Romeo và Juliet của Shakespeare với 20.000 từ:

e807d23c1ff8e4ba4aa4542d35082e28f9f5804
07ca6031a34bc1eff424fd37a

Trong các ví dụ trên, bạn có thể thấy rằng không thể xác định được dữ liệu đầu vào từ mã băm sinh ra. Cũng rất rõ ràng rằng một thay đổi nhỏ, chẳng hạn như một ký tự viết hoa thành viết thường, hay thêm khoảng cách sẽ khiến mã băm phát sinh thay đổi lớn.

**Giao Dịch Băm Trong Blockchain**

Các ví dụ trên đã chỉ rõ rằng mã băm sinh ra không có mẫu xác định độ dài của văn bản hay loại dữ liệu đầu vào. Các ví dụ trên không chứa các giao dịch, vì thế trong ví dụ tiếp theo chúng ta sẽ ví dụ về giao dịch rồi chuyển sang mã băm. Sau khi mã băm sinh ra, chúng ta sẽ liên kết các mã này vào một Blockchain.

Khối đầu tiên trong Blockchain là khối 0, hay còn gọi là khối nguyên thủy.

**Khối 0**

Khối đầu tiên của giao dịch sẽ chứa nội dung: "John nhận 100 bitcoin

Sally nhận 50 bitcoin

Sam nhận 10 bitcoin"

Mã băm 0 = 0000641727781545e50c0235823c

9ae0785d419499cc5a5dcdff2332a53f0f7f

**Khối 1**

Khối giao dịch thứ hai sẽ chứa các giao dịch sau: John gửi Sally 50 bitcoin

Sally gửi Sam 10 bitcoin

Mỗi giao dịch sẽ được chủ tài khoản gửi Bitcoin xác nhận bằng một khóa cá nhân. Mạng lưới sẽ không thể thấy được khóa cá nhân nhưng họ có thể kiểm nghiệm khóa cá nhân được cấp quyền gửi Bitcoin đã sử dụng.

Khối sẽ còn chứa mã băm của khối trước:

0000641727781545e50c0235823c9ae0785d41

9499cc5a5dcdff2332a53f0f7f

Một số được gọi là "Nonce" (số được dùng một lần) cũng sẽ có trong đó. Số này là đáp án cho mảnh ghép mà một thợ đào phải giải

để bổ sung được một khối hợp lệ trên Blockchain và nhận được phần thưởng.

Mã băm 1 = 0000ed29ee4097b79e194adb355 b18c500a900ffb3a1670dec4673eac2abdd07

**Khối 2:**

Khối giao dịch thứ ba sẽ chứa các giao dịch đã được xác nhận phía dưới, cùng với mã băm của khối trước đó và tham số Nonce:

Sally gửi Sam 20 bitcoin

John gửi Sally 20 bitcoin

Mã băm 2 = 0000d5cada28a39cb0511cc871d5

50fe0c4ba704a93ad33db378936c6ab40caf

**Khối 3:**

Khối giao dịch thứ tư sẽ chứa các giao dịch đã được xác nhận dưới đây và mã băm của khối trước đó cùng với tham số Nonce:

Sam gửi John 10 bitcoin

Sally gửi John 20 bitcoin

Mã băm 3 = 00001bbd6491304360d142bd5f3

2610214937c263b0bc6c44b3ac04574b62d4c

**Tạo Blockchain**

Từ những ví dụ trên, chúng ta có 4 mảnh dữ liệu được chuyển về mã băm. Lúc này, chúng ta có thể thêm các mã băm đó vào các khối và tạo thành một Blockchain liên kết chúng với nhau:

Khối đầu tiên trên Blockchain sẽ có mã băm:

0000641727781545e50c0235823c9ae0785d41

9499cc5a5dcdff2332a53f0f7f

Đây là "khối 0", hay "khối nguyên thủy", không tồn tại khối trước đó trên Blockchain mà khối này cần liên kết.

Khối thứ hai trên Blockchain là "Khối 1" và sẽ liên kết với mã băm của khối nguyên thủy.

Mỗi khối được bổ sung vào Blockchain sẽ liên kết với mã băm của khối trước trong phần đầu, kết nối chúng với nhau như một chuỗi. Từ các giao dịch ví dụ trên, chúng ta có thể tạo ra một Blockchain như sau:

**Khối 0 - Khối nguyên thủy:**

Mã khối trước: 0 - không có khối trước đó: Mã của khối 0:

0000641727781545e50c0235823c9ae0785d41

9499cc5a5dcdff2332a53f0f7f

**Khối 1:**

Mã băm của khối trước đó (Khối 0):

0000641727781545e50c0235823c9ae0785d41

9499cc5a5dcdff2332a53f0f7f

**Mã băm của khối 1:**

0000ed29ee4097b79e194adb355b18c500a900ff

b3a1670dec4673eac2abdd07

**Khối 2:**

Mã băm của khối trước đó (Khối 1):

0000ed29ee4097b79e194adb355b18c500a900ff

b3a1670dec4673eac2abdd07

**Mã băm của khối 2:**

0000d5cada28a39cb0511cc871d550fe0c4ba7

04a93ad33db378936c6ab40caf

**Khối 3:**

Mã băm của khối trước đó (Khối 2):

0000d5cada28a39cb0511cc871d550fe0c4ba7

04a93ad33db378936c6ab40caf

**Mã băm của khối 3:**

00001bbd6491304360d142bd5f32610214937c

263b0bc6c44b3ac04574b62d4c

Trên đây là ví dụ cơ bản về việc thiết lập một Blockchain. Mỗi nhóm giao dịch được chuyển thành một mã băm, kết hợp với mã băm của khối trước đó và một bộ số mà các thợ đào giải được. Mã băm được bao hàm trong phần đầu của khối tiếp theo, liên kết với mỗi khối mới vào khối trước đó.

Chúng ta có thể bám theo các giao dịch từ khối hiện tại ngược trở về khối nguyên thủy để tìm hiểu những gì đã diễn ra trong Blockchain.

**Thay Đổi Blockchain**

Như chúng ta đã thấy trong ví dụ về việc tạo mã băm, mọi thay đổi nhỏ trong văn bản đều sẽ tạo ra một mã băm hoàn toàn mới.

Đây là cách thức Blockchain hoạt động khiến việc thực hiện hành vi gian lận bằng cách thay đổi giao dịch trong các khối trước là gần như không thể.

Trong khối 1, gồm có những giao dịch sau: John gửi Sally 50 bitcoin Sally gửi Sam 10 bitcoin

Nếu Sam muốn thao túng Blockchain và thay đổi giao dịch đó để Sally gửi cho anh ta 20 bitcoin chứ không phải 10 bitcoin. Đó sẽ chỉ là một thay đổi nhỏ xíu bằng cách sửa lại số 1 trong giao dịch đó.

Loại sửa đổi này có thể dễ dàng diễn ra trong cơ sở dữ liệu tài chính hiện nay, nơi một con số, do vô tình hay cố ý, có thể bị nhập sai mà không được phát hiện ra.

Trong Blockchain, việc thay đổi một con số sẽ tạo nên một mã băm hoàn toàn mới cho khối giao dịch đó.

Mã băm nguyên thủy của khối là:

0000ed29ee4097b79e194adb355b18c500a900ff
b3a1670dec4673eac2abdd07

Mã băm mới của khối là:

0000f3e9eda5e3f8782c5051068935abcd710ff
d5fecb7fe7eaa6a57f8aa1208

Vì mỗi khối trong Blockchain kết nối với khối liền trước, phần đầu của mã băm trong khối 2 cũng cần được thay đổi để nó chứa được mã băm mới của khối 1 sinh ra do giao dịch thay đổi.

Điều này sẽ thay đổi mã băm của khối 2, tức là phần đầu mã băm của khối 3 cũng cần thay đổi để liên kết với mã băm mới của khối 2.

Tình trạng này sẽ tiếp tục xảy ra lần lượt tới khối mới nhất trên Blockchain cho đến khi toàn bộ mã băm của các khối đều thay đổi.

**Xác Thực Trên Blockchain**

Cứ 10 phút sẽ có một khối mới được thêm vào trên Blockchain Bitcoin. Nhiều Blockchain khác thêm một khối nhanh hơn hẳn. Để thay đổi một giao dịch trong một khối, mỗi khối phải được đào lại bằng mã băm mới nhanh hơn tốc độ toàn bộ mạng lưới đang thêm khối.

Điều này có lẽ khả thi với một số khối mới đưa vào, nhưng thường thì cứ 6 khối được thêm vào trên một khối giao dịch, việc thay đổi các giao dịch trong một khối, về mặt tính toán, sẽ trở nên không thể thực hiện được.

Một khối mới được đưa vào trên một khối liền trước sẽ được coi là một xác nhận rằng khối giao dịch liền trước hợp lệ và sẽ không đổi. Và 6 khối phía trên sẽ là 6 xác nhận đồng thời đưa ra đủ độ tin cậy để biết rằng giao dịch trước 6 khối đó sẽ không bị sửa đổi hoặc đảo chiều.

**Chỉ Tiêu Độ Khó Trên Mạng Lưới Bitcoin**

Các băm được đưa ra trong ví dụ trên có nhiều số 0 đằng trước. Một khối chỉ có thể được thêm vào Blockchain Bitcoin nếu mã băm thấp hơn băm chỉ tiêu của mạng lưới.

Các ví dụ dưới đây có thể khá chuyên môn, nhưng hãy tưởng tượng nó như trò tung xúc xắc ngẫu nhiên. Một con xúc xắc có các số từ 1 tới 6, nếu bạn chọn số 6 làm chỉ tiêu, thì bất cứ ai tung xúc xắc được số nhỏ hơn 6 đều có thể thêm một khối vào Blockchain.

Con số chỉ tiêu càng thấp, việc tung xúc xắc để có số nhỏ hơn càng khó vì sẽ có ít lựa chọn được chấp nhận hơn. Nếu số chỉ tiêu là 2, chỉ người tung được xúc xắc vào số 1 mới có thể thêm một khối vào Blockchain. Như thế, để tung được con số này sẽ tốn nhiều thời gian hơn, vì thế khi số người tham gia tung xúc xắc tăng, con số chỉ tiêu sẽ giảm xuống để giữ nguyên tốc độ thêm khối vào Blockchain.

Trong ví dụ về Blockchain trước, mã băm của khối 3 có bốn con số 0 như sau:

00001bbd6491304360d142bd5f32610214937c

263b0bc6c44b3ac04574b62d4c

Nếu chỉ tiêu mạng lưới là năm con số 0 và số 5, tức là 000005, thì mã băm chỉ hợp lệ khi nó nhỏ hơn 000005, nếu không nó sẽ không được coi là khối hợp lệ trong Blockchain.

Ví dụ mã băm chỉ tiêu:

000005d6b56a86dd37a43d070fe7eb7e59cf60

26f7f1f5f14286f11a3ab151c9

Ví dụ mã băm chấp nhận được:

Năm số 0 và số 4:

000004e13ccc4e31d500b52bc226dc4abb4627

c383beaef6f4da90a61b7994f0

Bảy số 0 và một số khác:

000000022b64fdf30dd4f28a50b542345b9750

ee24a3467423acdb66dea27e4ff55

Tám số 0 và một số khác:

000000004a4a2e623f745df50e97e62c9e854d0

7b0eef79a07ddad848c780133

Ví dụ mã băm bị loại:

Ba số 0 và một số khác:

0005f765f3c32e5e911ca18e136746daa0befff8

a6d7aa48fa487debd959a69d507f

Bốn số 0 và một số khác:

00001c8d7349aea0dd4acf2d16cb5f575035a9

ea80b080f751c832dfb97223043ab3f

Năm số 0 và số 6:

000006a3842a3742929149840eb13f8343bb9c

332a1c95e9c20f9e20692fe45e24f

Đây là ví dụ nâng cao từ ví dụ tung xúc xắc, nhưng cách thức sử dụng cũng tương tự khi tập hợp số lớn hơn nhiều.

**Khai Thác Khối**

Tham số Nonce là số bao hàm trong khối mà khi được băm, nó sẽ sinh ra một mã băm thấp hơn mã chỉ tiêu để được chấp nhận đưa vào Blockchain.

Một số tạo ra một mã băm hợp lệ thấp hơn chỉ tiêu mạng lưới hiện thời là mảnh ghép mà các thợ đào phải giải đáp để thêm được một khối vào Blockchain và nhận được phần thưởng.

Các thợ đào chọn những giao dịch nổi bật để đưa vào khối kế tiếp được bổ sung trên Blockchain cùng với dữ liệu nhận và gửi giao dịch. Đồng thời còn bao hàm cả mã băm của khối liền trước, chỉ tiêu độ khó hiện thời của mạng lưới, Cây Merkle Gốc, địa chỉ Blockchain để trả thưởng và nhãn thời gian.

Khi thêm giao dịch vào một khối, một thợ đào có thể chọn bất cứ cách kết hợp các giao dịch nổi bật nào đang chờ được đưa vào Blockchain. Thông thường, họ sẽ chọn các giao dịch có mức phí cao nhất đi kèm vì như thế thợ đào có thể nhận được số phí đó kèm theo phần thưởng khối nếu họ thêm được một khối vào Blockchain.

Như đã trình bày trong các ví dụ trên, mã băm sinh ra ngẫu nhiên và không có mối liên hệ nào với nội dung dữ liệu nhập. Các thợ đào không biết mã băm sẽ là gì cho đến khi họ tạo được mã băm.

Họ chỉ có thể bổ sung một khối vào Blockchain nếu mã băm họ tạo ra thấp hơn mã băm chỉ tiêu của mạng lưới. Để đạt được kết quả này, họ thêm một con số cùng với giao dịch và mã băm của khối liền trước sau đó tạo một mã băm.

Nếu mã băm sinh ra thấp hơn chỉ tiêu mạng lưới, họ có thể đưa nó vào Blockchain. Nếu mã băm cao hơn chỉ tiêu mạng lưới, họ có

thể thay đổi tham số Nonce rồi thử lại. Không có cách xác định mã băm là gì, vì thế quá trình tạo số chỉ là ước đoán ngẫu nhiên.

Các thợ đào tìm ra con số mà khi kết hợp với các giao dịch nổi bật sẽ tạo nên một mã băm thấp hơn chỉ tiêu mạng lưới, họ có thể thêm một khối vào Blockchain.

Các thợ đào thêm được một khối hợp lệ vào Blockchain sẽ nhận được phí giao dịch và phần thưởng khối.

Ngay khi con số được tìm ra, tất cả các máy tính khác trong mạng lưới có thể thêm số đó vào dữ liệu giao dịch và xác nhận số đó hợp lệ. Con số ngẫu nhiên này rất khó tìm, nhưng lại rất dễ kiểm nhận xem có hợp lệ không.

Khối hợp lệ được thêm vào Blockchain thì tất cả các máy tính trong mạng lưới sẽ cập nhật phiên bản Blockchain mới nhất có kèm khối mới vào hệ thống của họ.

Các thợ đào sau đó lặp lại quá trình này để thử và thêm khối mới vào Blockchain sao cho nhanh hơn các thợ đào khác trong mạng lưới.

**Tăng Độ Khó Mạng Lưới**

Quá trình tìm ra số phù hợp để tạo ra mã băm hợp lệ là một trò chơi may rủi ngẫu nhiên, tương tự như trò tung xúc xắc. Tốc độ xử lý đóng vai trò to lớn vì một máy tính ước đoán các số càng nhanh, đáp án phù hợp có thể được tìm ra càng mau chóng.

Mạng lưới Bitcoin được thiết kế để bổ sung một khối vào Blockchain cứ 10 phút một lần. Vì nhiều máy tính hơn được thêm vào mạng lưới, công suất tính toán trên mạng lưới càng tăng khiến lượng ước đoán con số phù hợp khả dụng cho mỗi khối càng nhiều. Để đảm bảo rằng thời gian thêm khối duy trì xấp xỉ khoảng 10 phút,

chỉ tiêu độ khó được điều chỉnh mỗi 2,016 khối bằng cách điều chỉnh các số nhỏ nhất và số lớn nhất để đưa vào một khối.

Trở lại ví dụ về xúc xắc, một khối hợp lệ chỉ có thể được thêm vào nếu một cá nhân tung xúc xắc ra số nhỏ hơn 3. Nếu một người tung xúc xắc, họ có hai trong sáu cơ hội tung được con số nhỏ hơn 3, tức là dưới chỉ tiêu 3 của mạng lưới và được cho phép thêm một khối vào Blockchain.

Ví dụ, họ có lẽ cần khoảng 10 phút để tung số 1 hoặc 2, vì thế chỉ tiêu mạng lưới để cứ mỗi 10 phút lại thêm một khối được giữ nguyên. Tuy nhiên, nếu một cá nhân khác gia nhập mạng lưới, cũng tung xúc xắc được số nhỏ hơn 3; việc tung xúc xắc ngẫu nhiên ra số 1 hoặc 2 này có lẽ chỉ cần tới một nửa thời gian, đồng thời làm thời gian thêm một khối vào Blockchain giảm đi một nửa.

Do số lượng người thêm vào mạng lưới tăng nhanh hơn sau mỗi 10 phút, mạng lưới sẽ điều chỉnh chỉ tiêu từ 3 xuống 2, vì thế một khối hợp lệ chỉ được chấp nhận khi nhỏ hơn số 2.

Có hai trong sáu cơ hội thu được số phù hợp, nhưng số người trong mạng lưới tăng gấp đôi, vì thế chỉ tiêu lại giảm bớt và lúc này chỉ còn một trong sáu cơ hội để thu được số phù hợp. Điều này sẽ tăng gấp đôi thời gian để đạt được chỉ tiêu này, tức là sẽ điều chỉnh thời gian khối đưa vào mạng lưới quay về 10 phút.

Blockchain Bitcoin hoạt động theo cách thức tương tự, vì nhiều máy tính được thêm vào mạng lưới, độ khó được điều chỉnh bằng cách giảm bớt chỉ tiêu mạng lưới. Điều này đồng nghĩa với việc sẽ có ít mã băm hợp lệ được chấp nhận và loạt số cần ước đoán nhiều hơn mới có thể tạo nên một khối với mã băm hợp lệ.

**Những Vấn Đề Về Bằng Chứng Xử Lý**

Cách thức tính toán số phù hợp để một mã băm hợp lệ được gọi là Bằng Chứng Xử Lý, vì nó cho biết các nguồn lực và công suất máy tính được đóng góp vào mạng lưới khi thêm một khối.

Các thợ đào được thưởng vì đóng góp công suất tính toán, điện năng và nhiều nguồn lực khác vào mạng lưới bằng khoản thanh toán cho mỗi khối mà họ bổ sung thành công vào mạng lưới, được gọi là "phần thưởng khối". Các thợ đào còn nhận được phí giao dịch cho mỗi khối mà họ thêm vào, đây chính là lý do mà họ có xu hướng chọn lựa những giao dịch có mức phí cao.

Phương thức Bằng Chứng Xử Lý yêu cầu công suất tính toán và điện năng lớn. Mạng lưới Bitcoin lớn mạnh hơn gấp 10.000 lần so với công suất của 500 siêu máy tính mạnh nhất thế giới gộp lại, nhưng hầu như công suất tính toán đó được dùng cho mục tiêu tạo ra các số ngẫu nhiên.

Vấn đề chính của phương thức này là nó vô cùng lãng phí nguồn lực vào việc thực hiện một chức năng mà có vẻ như vô nghĩa và không cần thiết để mạng lưới Blockchain hoạt động.

Hãy suy nghĩ một lát, tồn tại một mạng lưới máy tính mạnh hơn hầu hết các siêu máy tính trên thế giới gộp lại. Nhưng thay vì xử lý những vấn đề tầm cỡ thay đổi thế giới, nó lại được sử dụng vào việc ngẫu nhiên tạo số. Vấn đề lố bịch này là lý do tại sao nhiều người chỉ trích sự tốn kém của phương thức Bằng Chứng Xử Lý mà Blockchain Bitcoin đang sử dụng.

Có nhiều phương thức khác như Bằng Chứng Cổ Phần, Bằng Chứng Dung Lượng, Bằng Chứng Hoạt Động, Bằng Chứng Cháy có thể được sử dụng để thay thế. Những phương thức này sẽ không được bàn luận cụ thể, nhưng cần chú ý rằng có nhiều phương án

thay thế cho Bằng Chứng Xử Lý đang được nhiều Blockchain khác sử dụng.

Nền tảng Ethereum sử dụng mạng lưới để vận hành các ứng dụng phi tập trung, giúp sử dụng công suất tính toán hiệu quả hơn. Ethereum còn đang chuyển từ Bằng Chứng Xử Lý sang Bằng Chứng Cổ Phần trên Blockchain Ethereum.

**Độ Bảo Mật Của Mạng Lưới Blockchain**

Một trong những đặc trưng bảo mật đáng kể của Blockchain phi tập trung là mọi người đều có thể truy cập và tất cả bản sao lưu đều được cập nhật trên toàn mạng lưới.

Đặc điểm này đóng vai trò to lớn trong việc đảm bảo rằng không có cơ sở dữ liệu tập trung nơi mà Blockchain có thể bị một kẻ gian lận thao túng.

Mọi người có thể thêm một khối vào Blockchain nhưng đa số thành viên mạng lưới phải chấp nhận khối đó hợp lệ hay không.

Ngay khi một khối mới được chấp nhận là hợp lệ, nó sẽ được thêm vào Blockchain, toàn bộ các bản sao lưu của Blockchain trên cả mạng lưới đều được cập nhật và khối tiếp theo sẽ được bổ sung vào trên khối đó.

Nếu một người cố gắng ngụy tạo giao dịch, giao dịch đó sẽ không thể tương thích với những bản sao lưu còn lại của Blockchain và sẽ không được mạng lưới chấp nhận.

**Tấn Công Quá Bán Và Phân Nhánh Trong Blockchain**

Tấn Công Quá Bán đã được đề cập trong phần đầu cuốn sách, nó là một trường hợp về lý thuyết khi mà một người dùng nắm được quyền kiểm soát trên 50% mạng lưới. Và bằng cách kiểm soát trên 50% mạng lưới, người đó có thể quyết định giao dịch nào và khối

nào là hợp lệ và toàn bộ phần còn lại của mạng lưới sẽ được cập nhật bản Blockchain của họ.

Phân Nhánh là tình trạng khi một lượng lớn người dùng trên một mạng lưới bất đồng với một thay đổi trong mạng lưới, thay đổi đó có thể là giao dịch và khối được bổ sung hoặc chức năng của mạng lưới.

Sự bất đồng này tạo nên sự phân nhánh trong Blockchain khi mà một số thành viên tách ra và dùng công suất tính toán của họ để vận hành một Blockchain mới phân ra từ Blockchain ban đầu.

Những phân nhánh chính trong Blockchain xảy ra với Ethereum và nhiều đồng tiền ảo khác. "Ether" và "Ether classic" là hai Blockchain riêng rẽ được tạo ra từ Blockchain Ethereum ban đầu; tuy nhiên, vì một sự bất đồng, một phần mạng lưới Ethereum tách ra và sử dụng nguồn lực của họ cho một phiên bản Blockchain khác.

**Tổng Kết**

Chương này đã cung cấp những hiểu biết cụ thể hơn về mặt kỹ thuật cách thức hoạt động của Blockchain.

Có một số thông tin nâng cao bổ sung về mạng lưới Blockchain mà bạn có thể tìm thấy trong phần nguồn tham khảo.

# Nguồn tham khảo

**Lịch sử Blockchain và Bitcoin**

Chuyên đề gốc về Bitcoin của Satoshi Nakamoto, nhan đề Bitcoin: A Peer-to-peer Electronic Cash System.

Mã nguồn nguyên thủy cho Bitcoin trên GitHub:

https://github.com/trottier/original-bitcoin/blob/master/src/main.h#L795-L803

Các tài liệu đóng góp vào việc hình thành Bitcoin và Blockchain

Blind Signatures for Untraceable Payments, David Chaum phát hành, năm 1998:

http://blog.koehntopp.de/uploads/Chaum. BlindSigForPayment.1982.PDF

World's first electronic cash payment over computer networks, Thông cáo báo chí ngày 27/05/1994 của DigiCash:

https://w2.eff.org/Privacy/Digital_money/?f=digicash.announce.txt

Đề xuất về B-money của Wei Dai năm 1998:

http://www.weidai.com/bmoney.txt

Trang web và bài đăng về Bit Gold của Nick Szabo, tái bản năm 2008:

https://unenumerated.blogspot. com/2005/12/bit-gold.html

Ethereum và các hợp đồng thông minh Trang web nền tảng Ethereum: https://www.ethereum.org/

Mã nguồn Ethereum trên GitHub:

https://github.com/ethereum/

Ngôn ngữ lập trình Solidity dùng để tạo hợp đồng thông minh trên Máy ảo Ethereum:

https://solidity.readthedocs.io/en/develop/

**Các loại tiền ảo**

Danh sách tiền ảo lớn nhất dựa theo giá trị vốn hóa thị trường: https://coinmarketcap.com/

Coinbase - một trong những công ty cung cấp dịch vụ ví ảo trên web lớn nhất để giao dịch tiền ảo: https://www.coinbase.com/join

Ghi chú: Đường dẫn giới thiệu trên đây bao gồm 10$ bitcoin miễn phí sau khi giao dịch trên 100$ giá trị bitcoin.

Các trang tìm hiểu về Blockchain Bitcoin Blockchain.info: https://blockchain.info/ Blockr: https://www.coinbase.com/join Nguồn phát triển Bitcoin: https://bitcoin.org/en/development

# Bảng thuật ngữ

Ghi chú: Bảng thuật ngữ sau đây dựa theo chú giải của Oleg Andreev, nhà thiết kế phần mềm và chuyên gia về Bitcoin.

**Bitcoin (chữ B in hoa)**

Bitcoin với chữ B in hoa dùng khi đề cập đến Blockchain, các giao thức và mạng thanh toán tiền ảo.

Với tư cách một giao thức, Bitcoin là một tập hợp luật định mà mọi khách hàng phải tuân thủ để chấp nhận giao dịch và các giao dịch của chính nó được các khách hàng khác chấp nhận.

Với tư cách một mạng lưới, Bitcoin là toàn bộ các máy tính phải tuân thủ cùng một bộ luật đồng thời trao đổi các giao dịch và khối với nhau.

Các giao dịch được máy tính trong mạng lưới xử lý với nhau (Mô hình ngang cấp), không tồn tại một tổ chức, chính phủ hay ngân hàng trung tâm để ban hành hay quản lý giao dịch.

**bitcoin (chữ b viết thường)**

Khi bitcoin với chữ b viết thường, chủ yếu được dùng để chỉ các đơn vị của bitcoin, chẳng hạn "truyền 0,5 bitcoin". Tổng số bitcoin được giới hạn trong con số 21 triệu.

**Khối**

Một khối là một hồ sơ trên Blockchain có chứa dữ liệu về giao dịch và thông tin để xác nhận là một phần hợp lệ của Blockchain.

Các khối có chứa một tiêu đề khối, các giao dịch, nhãn thời gian, bằng chứng xử lý, một hồ sơ của khối liền trước và những giao dịch

mới chưa được ghi lên Blockchain.

Một khối lập hồ sơ vĩnh viễn các giao dịch và dữ liệu nó chứa trên Blockchain. Mỗi khối chứa thông tin về các khối trước đó, tạo nên một chuỗi liên kết các khối.

Bằng Chứng Xử Lý là một thách thức giải đáp một mảnh ghép toán học độc nhất cho khối đó. Mảnh ghép khó giải nhưng lại dễ kiểm nhận sau khi đã giải ra. Các khối mới không thể được đưa vào Blockchain nếu chúng không chứa đáp án chính xác của mảnh ghép này.

Khai thác là quá trình giải quyết một vấn đề để đưa một khối hợp lệ vào Blockchain. Các thợ đào được trao thưởng vì đã giải ra vấn đề và bổ sung khối hợp lệ như một cách khuyến khích họ đóng góp công suất tính toán và nguồn lực vào mạng lưới Blockchain.

Trên Blockchain Bitcoin, một khối giao dịch mới được thêm vào cứ mỗi 10 phút.

**Chiều cao khối**

Chiều cao khối là số khối kết nối với khối đó trên Blockchain.

Chiều cao khối bằng 0 tức là khối đầu tiên, hay còn gọi là "khối nguyên thủy" trên Blockchain. Chiều cao của khối sau "khối nguyên thủy" là số khối trong chuỗi nằm giữa khối đó và khối nguyên thủy.

**Phần thưởng khối**

Phần thưởng khối được trao cho thợ đào đã xử lý thành công một giao dịch và băm được khối giao dịch đó.

Phần thưởng thường là một lượng nhỏ tiền ảo được thanh toán cho thợ đào. Phần thưởng này tùy thuộc vào loại tiền ảo và biến đổi với độ khó tăng lên và phần thưởng khối giảm đi theo thời gian.

Nhờ trao phần thưởng cho thợ đào, mọi người được khuyến khích đóng góp công suất tính toán vào mạng lưới, từ đó gia tăng độ bảo mật và giảm bớt thời gian xử lý, tạo nên mạng lưới nhanh hơn và an toàn hơn.

**Blockchain**

Một sổ cái phân tán, công khai và dùng chung chứa toàn bộ các giao dịch đã được kiểm nhận. Một khối chứa một tập hợp các giao dịch vừa được kiểm nhận và một chỉ dẫn tới khối liền trước.

Nhờ có chỉ dẫn tới khối liền trước, các khối được liên kết lại với nhau, từ đó tạo nên một chuỗi.

Mọi người có quyền truy cập đều có thể truy ngược các giao dịch và các khối trên Blockchain về tới khối đầu tiên, hay còn gọi là khối nguyên thủy.

Một Blockchain được cập nhật bằng cách khai thác các khối với các giao dịch mới. Các giao dịch không được xác nhận sẽ không trở thành một phần trong Blockchain.

**BTC**

Đây là mã tiền ảo nổi tiếng nhất đại diện cho 1 Bitcoin, tương tự như USD của đồng đô la Mỹ hoặc nhiều mã tiền phổ biến khác.

**Giao dịch được xác nhận**

Một giao dịch được xác nhận là một giao dịch đã được xử lý, được mạng lưới xác thực và được đưa vào trong Blockchain.

Giao dịch được xác nhận thông qua khai thác hoặc bằng chứng xử lý trong mạng lưới tiền ảo như Bitcoin.

Khi một giao dịch được xác nhận, sẽ không có khả năng đảo chiều giao dịch đó; tuy nhiên, số xác nhận sẽ xác định thay đổi của

một giao dịch bị từ chối hay đảo chiều. Vui lòng xem phần Số xác nhận.

**Số xác nhận**

Số xác nhận là thước đo xác suất một giao dịch có thể bị từ chối khỏi chuỗi chính.

"Xác nhận 0" tức là một giao dịch không được xác nhận (trong bất kỳ khối nào). "Xác nhận 1" tức là giao dịch được đưa vào khối mới nhất trong chuỗi chính.

"Xác nhận 2" là giao dịch được đưa vào khối ngay sau khối mới nhất. Xác suất một giao dịch bị đảo chiều (giao dịch lặp chi) giảm theo hàm số mũ khi có nhiều khối hơn được bổ sung vào trên đó.

**Blockchain liên hợp**

Một Blockchain liên hợp là Blockchain nằm giữa Blockchain cá nhân và công khai. Blockchain liên hợp phi tập trung một phần nhưng việc xác thực của khối được hoàn thiện bởi một nhóm tuyển chọn các thợ đào.

Một Blockchain liên hợp chấp nhận các giao dịch cá nhân và hữu hiệu mà không trao toàn quyền kiểm soát cho một tổ chức hoặc cá nhân.

**Tiền ảo**

Tiền ảo là một loại tiền tệ kỹ thuật số không do chính phủ, ngân hàng trung tâm hay tổ chức nào đó ban hành.

Sự kết hợp của từ cryptography (mật mã học) và currency (tiền tệ) thành từ cryptocurrency (tiền ảo), loại tiền này được tạo nên và vận hành nhờ áp dụng các kỹ thuật mã hóa và toán học.

**Hàm băm mật mã học**

Một hàm băm mật mã học là một phương thức mã hóa giúp ẩn giấu dữ liệu theo cách mà khiến cho việc giải mã trở nên bất khả thi khi không có quyền truy cập.

Một thuật toán máy tính nhận bất cứ một lượng hoặc độ dài dữ liệu đầu vào nào rồi tạo ra một dữ liệu xuất có độ dài không đổi được gọi là "hàm băm" của dữ liệu. Nó có thể được dùng để dễ dàng xác thực rằng dữ liệu đã không bị thay đổi.

Bất kể độ dài thông điệp hay kích thước đầu vào, dữ liệu đầu ra sẽ luôn có cùng độ dài. Một thay đổi nhỏ trong đầu vào sẽ khiến dữ liệu đầu ra và giá trị băm thay đổi hoàn toàn.

Mã băm sinh ra ngẫu nhiên và vì thế việc cố gắng tạo ra một mã băm đặc biệt bằng cách thay đổi dữ liệu được băm là tuyệt đối khó khăn.

**Mật mã học**

Mật mã học là lĩnh vực toán học tập trung vào hoạt động mã hóa, bảo mật dữ liệu. Mật mã học là nền tảng của tiền ảo, cho phép thiết lập, quản lý và bảo mật mạng lưới.

**Ứng dụng phi tập trung (dApps)**

Các ứng dụng phi tập trung là những ứng dụng mã nguồn mở, không chịu sự kiểm soát của một cá nhân hay đối tượng nào và chạy trên một Blockchain phân tán hoặc mạng lưới máy tính.

Các ứng dụng phi tập trung không có máy chủ trung tâm, các thành viên kết nối với nhau thông qua các kết nối đồng cấp.

**Độ khó**

Độ khó là thước đo để xác nhận khối mới trong mạng lưới Blockchain khó khăn đến mức nào.

Trong Bitcoin, đó là chỉ tiêu lớn nhất được chia ra từ chỉ tiêu hiện tại. Độ khó của Bitcoin được điều chỉnh sau mỗi 2,016 khối căn cứ theo thời gian sử dụng để xác nhận 2,016 khối trước đó.

Độ khó được điều chỉnh để đảm bảo khả năng xác thực của mỗi khối được duy trì sau mỗi chu kỳ khoảng 10 phút.

Vào thời điểm cuốn sách này được viết, độ khó Bitcoin hiện tại là 520.808.749.422 và được dự đoán sẽ tăng trong khoảng 3 - 5% sau mỗi hai tuần.

**Độ sâu**

Độ sâu đề cập tới một điểm trên Blockchain. Một giao dịch với 6 xác nhận còn có thể gọi là "độ sâu 6 khối".

Độ sâu của một giao dịch trong Blockchain càng lớn, độ tin cậy và tín nhiệm của giao dịch đó càng cao.

**Giao dịch lặp chi**

Giao dịch lặp chi xảy ra khi cùng một số tiền được gửi hai lần. Nếu bạn có 5 bitcoin trong ví và bạn gửi 5 bitcoin cho người khác, ngay tiếp sau bạn lại gửi 5 bitcoin đó cho một người khác nữa, đó gọi là giao dịch lặp chi.

Mạng lưới Bitcoin có thể giúp tình trạng giao dịch lặp chi trở nên rất khó khăn vì mạng lưới sẽ phát hiện cả hai giao dịch, sau đó đạt tới đồng thuận rằng giao dịch nào trong đó sẽ được xác nhận và giao dịch nào bị từ chối.

Chỉ một giao dịch sẽ được đưa vào Blockchain và được coi là hợp lệ. Giao dịch càng có nhiều xác nhận (độ sâu), việc giao dịch lặp chi càng khó khăn hơn.

Tấn Công Quá Bán là một trường hợp khi giao dịch lặp chi xảy ra và Blockchain có thể bị thao túng. Vui lòng xem phần Tấn Công

Quá Bán.

**Ether**

Ether là đồng tiền ảo được sử dụng trên mạng lưới Ethereum. Nó được coi như một hình thức thanh toán cho việc vận hành các ứng dụng phi tập trung trên mạng Ethereum.

Đồng tiền ảo Ether là loại tiền ảo lớn thứ hai trên thế giới do giá trị vốn hóa thị trường chỉ đứng sau Bitcoin với giá trị trên 10 tỷ đô la.

**Ethereum**

Ethereum là một nền tảng cho phép các ứng dụng phân tán, phi tập trung, chẳng hạn như các hợp đồng thông minh, hoạt động trên một máy ảo trên một mạng lưới Blockchain.

Mạng lưới Ethereum sử dụng đồng tiền ảo Ether có vai trò như một loại tiền tệ trên mạng lưới. Ether được trao đổi như một hình thức thanh toán cho việc vận hành các ứng dụng phi tập trung trên mạng lưới.

**Khối nguyên thủy**

Khối nguyên thủy là khối đầu tiên trên một Blockchain và không có khối nào trước đó.

Trong Blockchain Bitcoin, khối đầu tiên, hay "khối nguyên thủy", ra đời vào khoảng mùng ba tháng Một năm 2009 và có chứa một trích dẫn từ một bài báo với nội dung "Tờ Times ngày 03/01/2009, Đại Pháp Quan đứng bên bờ vực phải viện trợ ngân hàng lần thứ hai" như một bằng chứng rằng không tồn tại các khối được bí mật đào trước ảnh hưởng tới Blockchain trong tương lai.

Thông điệp hài hước nhắc tới lý do cho sự tồn tại của Bitcoin: tình trạng lạm phát tiền bạc liên miên do chính phủ và ngân hàng gây ra.

**Sổ cái (Phân tán)**

Một sổ cái phân tán là cơ sở dữ liệu trải rộng trên khắp các hệ thống máy tính, quốc gia và tổ chức khác nhau.

Các hồ sơ được lưu trữ lần lượt trong một cuốn sổ cái liên tục cập nhật. Dữ liệu sổ cái phân tán có thể là "cấp quyền" hoặc "không cấp quyền". Xem thêm Sổ cái (cấp quyền) và sổ cái (không cấp quyền) dưới đây.

**Sổ cái (Cấp quyền)**

Một sổ cái cấp quyền là sổ cái yêu cầu quyền hạn truy cập sổ cái.

Có thể có một hoặc nhiều chủ sở hữu sổ cái cấp quyền. Khi những hồ sơ mới được đưa vào sổ cái, chúng sẽ được những người có thẩm quyền kiểm tra và xác nhận.

Một sổ cái cấp quyền có thể được các chính phủ hoặc ngân hàng nơi chứa nhiều dữ liệu bí mật sử dụng. Sử dụng một sổ cái cấp quyền chung nhanh hơn so với sổ cái không cấp quyền, tuy nhiên vẫn cung cấp các khối dữ liệu đã xác thực kèm chữ ký số mà mọi người có thẩm quyền đều xem được.

**Sổ cái (Không cấp quyền)**

Sổ cái không cấp quyền không thuộc sở hữu của cá nhân hay tổ chức nào. Bất cứ ai cũng có thể thêm dữ liệu vào sổ cái và mọi người có quyền truy cập những bản sao lưu sổ cái đầy đủ.

Cách thức này tạo nên khả năng bảo vệ sổ cái khỏi những dữ liệu gian lận hoặc trái phép vì mọi người có thẩm quyền đều phải xác thực dữ liệu nhập vào sổ cái, liên tục đạt tới sự đồng thuận về sổ cái và duy trì tính toàn vẹn của sổ.

Bitcoin là một ví dụ về sổ cái không cấp quyền.

**Chuỗi chính**

Chuỗi chính là một Blockchain chính, là dãy khối dài nhất tính từ khối nguyên thủy tới khối mới nhất.

**Khai thác**

Khai thác là khi công suất tính toán được sử dụng để giải đáp các vấn đề toán học đóng vai trò cho phép giao dịch được xác nhận và các khối giao dịch được bổ sung vào Blockchain.

Các thợ đào đóng góp công suất tính toán và nguồn lực như điện năng vào mạng lưới Blockchain được sử dụng để kiểm nhận các giao dịch và vì họ sẽ nhận được phần thưởng khối và phí giao dịch từ việc xác thực một khối. Các đồng tiền ảo mới được tạo ra thông qua quá trình này vì thế nó được coi là quá trình khai thác tiền ảo từ mạng lưới.

Khai thác Bitcoin là quá trình sử dụng phần cứng máy tính để thực hiện tính toán cho mạng lưới Bitcoin để xác thực các giao dịch. Các thợ đào thu thập phí giao dịch từ các giao dịch mà họ kiểm nhận đồng thời được thưởng bitcoin cho mỗi khối mà họ xác thực.

**Tham số Nonce**

Đại diện cho khái niệm "số được dùng một lần". Một số trong tiêu đề khối sẽ liên tục thay đổi để tìm ra một tham số Nonce có thể tạo một mã băm hợp lệ trong suốt quá trình tìm kiếm bằng chứng xử lý. Mỗi khi tham số Nonce thay đổi, mã băm của tiêu đề khối đều được tính lại.

**Mô hình ngang cấp (P2P)**

Mô hình ngang cấp là hệ thống mà trong đó các thành viên trên mạng lưới liên hệ trực tiếp với nhau mà không thông qua một hệ thống hoặc đơn vị trung gian.

**Blockchain cá nhân**

Blockchain cá nhân là Blockchain trong đó quyền truy cập và cấp phép thuộc về một tổ chức trung tâm. Đó có thể là chính phủ, ngân hàng hay các tổ chức khác nơi dữ liệu chứa trong Blockchain là loại dữ liệu bí mật và bị hạn chế.

Hầu hết các tổ chức và chính phủ đều sử dụng hệ thống và cơ sở dữ liệu cá nhân. Một Blockchain cá nhân có thể được sử dụng với cùng chức năng như cơ sở dữ liệu nội bộ riêng tư.

**Blockchain công khai**

Blockchain công khai là Blockchain mọi người đều được cho phép truy cập. Bất cứ ai cũng có thể truy cập vào Blockchain, thực hiện giao dịch, xác thực giao dịch và chọn lựa khối nào sẽ được thêm vào Blockchain.

Bitcoin là một ví dụ về Blockchain công khai. Blockchain công khai còn thường được dùng khi nhắc tới Blockchain phi tập trung.

**Khóa cá nhân**

Khóa cá nhân là mã hoặc dữ liệu cung cấp cho bạn quyền truy cập ví tiền ảo.

Cũng như mã PIN cấp cho bạn khả năng tiếp cận số tiền trong tài khoản ngân hàng, khóa cá nhân trao cho bạn khả năng tiếp cận ví tiền ảo của bạn.

Bạn nên giữ bí mật khóa cá nhân tương tự như cách bạn giữ bí mật mã PIN của bạn và không chia sẻ với bất cứ ai nếu không họ sẽ có thể lấy được tiền của bạn.

**Khóa công khai**

Khóa công khai tương tự như số tài khoản ngân hàng. Khi bạn kết hợp khóa công khai và khóa cá nhân, bạn có thể tiếp cận khoản

tiền trong ví. Bạn có thể chia sẻ khóa công khai để nhận tiền vào ví đó, nhưng để truy cập vào ví, bạn cần kết hợp với khóa cá nhân.

**Bằng Chứng Xử Lý (PoW)**

Bằng Chứng Xử Lý là giải pháp cho mảnh ghép toán học cần có để thêm được một khối vào Blockchain.

Mảnh ghép rất khó giải nhưng lại rất dễ xác minh, tương tự như bộ mã cho ổ khóa. Rất khó để đoán mã khóa là gì, nhưng ngay khi mã khóa được tìm ra, mọi người đều có thể dễ dàng sử dụng mã đó để kiểm tra xem mã khóa đó có đúng hay không.

Đối với tiền ảo, cần nhiều công suất tính toán và nguồn lực để tạo ra bằng chứng xử lý.

Trong Bitcoin, bằng chứng xử lý là mã băm của tiêu đề khối. Một khối được coi là hợp lệ chỉ khi mã băm thấp hơn chỉ tiêu hiện tại. Mỗi khối đều chỉ dẫn tới khối liền trước nhờ thế mà tích lũy được bằng chứng xử lý và hình thành nên một Blockchain.

**Bằng Chứng Hoạt động (PoA)**

Bằng Chứng Hoạt Động là một giải pháp thay thế cho Bằng Chứng Cổ Phần và Bằng Chứng Xử Lý. Bằng Chứng Hoạt Động đưa quyết định tạo công suất cho một hay nhiều khách hàng trên cơ sở dữ liệu có khóa cá nhân cụ thể từ đó cho phép họ thiết lập các giao dịch và các khối trên Blockchain.

**Bằng chứng cổ phần (PoS)**

Bằng Chứng Cổ Phần là giải pháp thay thế cho hệ thống Bằng Chứng Xử Lý và Bằng Chứng Thẩm Quyền.

Bằng Chứng Cổ Phần là quá trình trong đó một lượng tiền ảo vốn có sẽ quyết định lượng tiền mà người sở hữu có thể khai thác. Một người giữ 5% tiền ảo có thể đào 5% các khối.

Có nhiều công suất tính toán và nguồn lực dùng vào khai thác và quá trình Bằng Chứng Xử Lý chỉ để chứng minh rằng các nguồn lực được đóng góp vào khai thác một khối.

Bằng Chứng Cổ Phần hoạt động trên giả định một người với một cổ phần tiền ảo sẽ không muốn cổ phần của họ mất giá, vì thế sẽ hành động vì lợi ích cao nhất của họ trong mạng lưới đồng thời tiết kiệm công suất tính toán và nguồn lực.

Peercoin là đồng tiền ảo đầu tiên sử dụng Bằng Chứng Cổ Phần.

**Satoshi**

Một Satoshi là lượng Bitcoin nhỏ nhất. Cứ 1 Satoshi tương ứng với 0,00000001 bitcoin.

Cái tên Satoshi được dùng để vinh danh người sáng tạo ra Bitcoin: Satoshi Nakamoto.

**Satoshi Nakamoto**

Satoshi Nakamoto là bút danh của người sáng tạo ra đồng Bitcoin. Vẫn chưa ai chắc chắn rằng liệu đó là một người hay một nhóm. Có nhiều giả thuyết về cá nhân và số người thực hiện Bitcoin, về quốc tịch hay độ tuổi, nhưng không ai có bằng chứng xác đáng về danh tính của họ.

Vào thời điểm cuốn sách này được viết ra, Satoshi Nakamoto vẫn là một ẩn số.

**SHA (Thuật toán mã hóa an toàn sử dụng hàm băm)**

Thuật toán mã hóa an toàn sử dụng hàm băm là một loại hàm băm mật mã học được Viện Tiêu chuẩn và Kĩ thuật Quốc gia Mỹ (NIST) tạo ra như một Tiêu chuẩn Xử lý Thông tin Liên bang Mỹ (FIPS).

Thuật toán mã hóa an toàn sử dụng hàm băm là một cách trong đó ngay khi dữ liệu được mã hóa, nó gần như bất khả giải đối với những ai không có quyền truy cập.

Xem "Hàm băm mật mã học" và "SHA256".

**SHA 256**

SHA 256 là thuật toán mã hóa an toàn sử dụng hàm băm được sử dụng trong hệ thống bằng chứng xử lý của Bitcoin.

Thuật giải SHA 256 sinh ra các mã băm ổn định (32 byte) 256 bit độc nhất.

**Chữ ký**

Một chữ ký trong tiền ảo là một cách thức toán học dùng để chứng minh quyền sở hữu, quyền truy cập quỹ tiền và thực hiện giao dịch.

Trong Bitcoin, một khóa cá nhân buộc phải tương thích với một khóa công khai để đánh dấu một giao dịch. Mạng Bitcoin có thể xác nhận khóa cá nhân và khóa công khai tương thích trên một chữ ký giao dịch nhưng khóa cá nhân vẫn được ẩn khỏi mạng lưới.

Bitcoin sử dụng giải thuật Ký Số Hệ Mật Đường Cong Elliptic (ECDSA) để đánh dấu giao dịch.

**Hợp đồng thông minh**

Hợp đồng thông minh là những hợp đồng được viết bằng mã máy tính và vận hành trên một Blockchain hoặc sổ cái phân tán.

Chúng tự động xác nhận, xử lý và ép buộc thực hiện các hợp đồng căn cứ theo thuật ngữ được viết bằng mã.

Các hợp đồng thông minh có thể tự xử lý hoặc tự ép buộc thực hiện một phần hoặc toàn phần.

**Solidity**

Solidity là ngôn ngữ lập trình được sử dụng để lập trình mã được Máy ảo Ethereum thông dịch, để dùng trong hợp đồng thông minh hoặc các ứng dụng phi tập trung trên mạng Ethereum. Nó là một cấu trúc cú pháp tương tự như JavaScript.

**Giao dịch không được xác nhận**

Đây là các giao dịch không được đưa vào bất cứ khối nào, được gọi là giao dịch "xác nhận 0". Các giao dịch không được xác nhận sẽ tiếp tục ở trạng thái không được xác nhận cho đến khi mạng lưới quyết định bỏ đi, có thể thấy nó trên Blockchain hoặc tự gắn mình vào Blockchain. Xem thêm Số xác nhận.

**Tấn Công Quá Bán**

Tấn Công Quá Bán, hay còn gọi là tấn công trên 50% hoặc tấn công giao dịch lặp chi. Tình huống này xảy ra khi có trên 50% công suất tính toán trên một mạng lưới tiền ảo bị một cá nhân hoặc nhóm người kiểm soát.

Bằng cách kiểm soát trên 50% công suất tính toán trên mạng lưới, họ có thể thay đổi mạng lưới và Blockchain thông qua việc chấp nhận giao dịch lặp chi, ngụy tạo giao dịch và khiến các giao dịch không được xác nhận.

Ngay cả khi lý thuyết này khả thi, số lượng các thợ đào và công suất tính toán ngày càng tăng trên mạng lưới sẽ khiến Tấn Công Quá Bán càng khó xảy ra.

Tấn Công Quá Bán gần như không có khả năng xảy ra trên mạng lưới Bitcoin, nhưng xác suất xảy ra cao hơn đối với những đồng tiền ảo nhỏ hơn và mới ra đời.

# Phụ lục

**Bitcoin: Hệ thống tiền ảo mô hình ngang cấp**

*Satoshi Nakamoto*

*satoshin@gmx.com*

*www.bitcoin.org*

**Tổng quan**

Phiên bản tiền điện tử ngang cấp cho phép thực hiện hoạt động thanh toán trực tuyến trực tiếp giữa các bên mà không cần thông qua tổ chức tài chính nào. Chữ ký điện tử có một phần vai trò trong giải pháp này, tuy nhiên những lợi ích chính sẽ không còn nếu vẫn cần tới một bên thứ ba đáng tin cậy để ngăn chặn tình trạng giao dịch lặp chi. Chúng tôi đề xuất một giải pháp ứng phó với vấn nạn giao dịch lặp chi nhờ sử dụng mạng lưới theo mô hình ngang cấp. Mạng lưới này sẽ dán nhãn thời gian cho các giao dịch bằng cách băm chúng vào một chuỗi liên tục gồm các bằng chứng xử lý dựa theo hàm băm, từ đó hình thành một hồ sơ không thể thay đổi trừ phi tái tạo bằng chứng xử lý. Chuỗi dài nhất không chỉ hoạt động như một minh chứng cho các sự kiện nối tiếp nhau mà còn cho thấy rằng nó bắt nguồn từ vùng trữ công suất CPU lớn nhất. Chỉ cần đa số công suất CPU được kiểm soát bởi các nút không thông đồng tấn công mạng lưới, chúng sẽ sản sinh ra chuỗi dài nhất và vượt thoát khỏi những kẻ tấn công. Bản thân mạng lưới chỉ yêu cầu một cấu trúc rất đơn giản. Các thông điệp được truyền trên cơ sở thỏa thuận nỗ lực tối đa, các nút có thể rời bỏ và tái gia nhập mạng lưới tùy ý,

chấp nhận chuỗi bằng chứng xử lý dài nhất như một minh chứng cho những gì đã diễn ra khi chúng không có mặt.

## 1. Giới thiệu

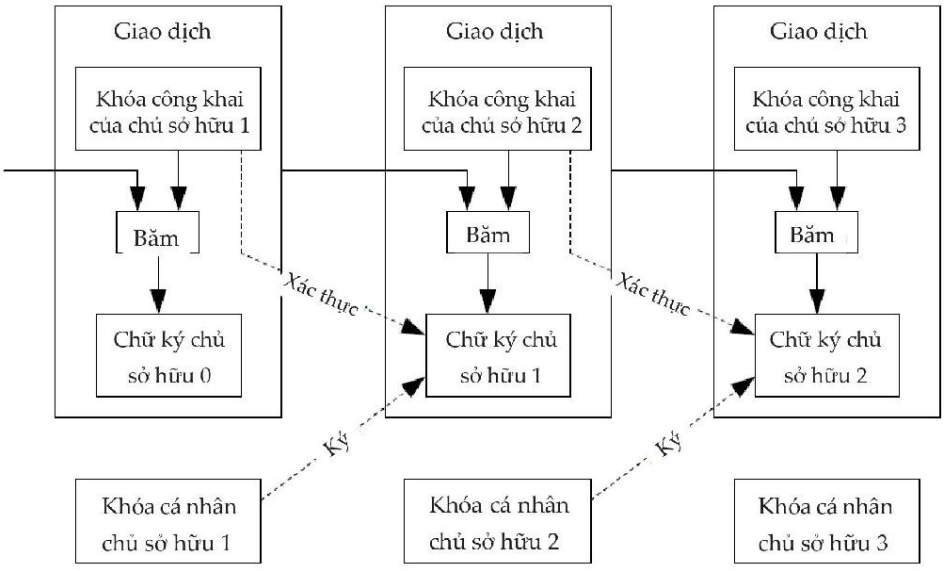
Hoạt động giao dịch trên mạng Internet đã trở nên phụ thuộc quá mức vào các tổ chức tài chính đóng vai trò bên thứ ba đáng tin cậy trong việc xử lý các khoản thanh toán điện tử. Mặc dù hệ thống hoạt động thích đáng với mọi giao dịch, nó vẫn chịu ảnh hưởng từ những nhược điểm cố hữu trong mô hình thiết lập dựa trên niềm tin. Không thực sự tồn tại các giao dịch hoàn toàn bất khả đảo ngược trong mô hình này, vì các tổ chức tài chính không thể tránh khỏi việc phải dàn xếp các vụ tranh chấp. Chi phí dàn xếp làm tăng chi phí giao dịch, giới hạn kích thước tối thiểu của giao dịch thực tế và xóa bỏ tiềm năng thực hiện các giao dịch nhỏ thông thường, còn có khoản phí phát sinh do không có khả năng thực hiện các giao dịch một chiều cho các dịch vụ bất khả thay đổi. Yêu cầu về lòng tin tăng lên cùng với nguy cơ giao dịch bị đảo ngược. Các doanh nghiệp phải rất cẩn thận với khách hàng của mình, đòi hỏi họ nhiều thông tin hơn họ cần cung cấp. Họ buộc phải chấp nhận phần trăm nguy cơ gian lận nào đó vì không thể tránh khỏi. Rủi ro thanh toán và các loại chi phí này có thể tránh được khi mọi người chi tiêu bằng tiền giấy, nhưng không máy móc nào có thể thực hiện thanh toán trên các kênh giao dịch mà thiếu đi bên thứ ba.

Cần phải có một hệ thống thanh toán điện tử dựa trên các bằng chứng mã hóa thay vì các hệ thống dựa trên niềm tin, cho phép hai bên bất kỳ giao dịch trực tiếp với nhau mà không cần tới bên thứ ba đóng vai trò trung gian. Các giao dịch không thể đảo chiều sẽ bảo vệ người mua khỏi tình trạng gian dối, các hệ thống chứng từ thông

thường có thể dễ dàng được thực hiện để bảo vệ người mua. Trong chuyên đề này, chúng tôi đề xuất một giải pháp ứng phó với nạn giao dịch lặp chi bằng cách sử dụng một hệ thống nhãn thời gian phân tán ngang cấp để tạo ra các bằng chứng tính toán về trình tự giao dịch theo thời gian. Hệ thống còn an toàn chừng nào các nút trung thực còn tập trung kiểm soát lượng công suất CPU nhiều hơn nhóm các nút tấn công hợp lại.

**2. Giao dịch**

Chúng ta coi một đồng tiền điện tử là một chuỗi các chữ ký số. Mỗi chủ sở hữu chuyển tiền tới chủ sở hữu tiếp theo bằng cách ký một băm của giao dịch trước và khóa công khai của chủ sở hữu sau rồi bổ sung vào cuối đồng tiền. Người thụ hưởng có thể kiểm nhận các chữ ký để xác thực chuỗi quyền sở hữu.



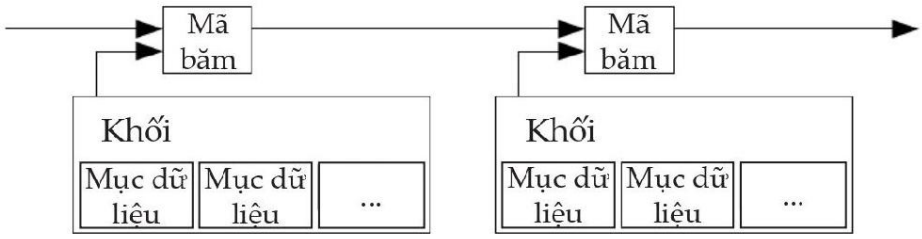
Vấn đề của quá trình này là người thụ hưởng không thể xác thực xem liệu một trong số các chủ sở hữu có tiền giao dịch lặp chi hay không. Cách xử lý phổ biến là đưa vào một tổ chức trung tâm đáng tin cậy, hoặc xưởng phát hành, để thẩm tra mọi giao dịch xem có giao dịch lặp chi không. Sau mỗi giao dịch, đồng tiền phải quay về xưởng để được phát hành đồng tiền mới, và chỉ những đồng được xưởng phát hành mới được coi là không bị lặp chi. Vấn đề của giải pháp này là số phận của toàn bộ hệ thống tiền tệ trên đều phụ thuộc vào tổ chức chủ quản xưởng phát hành, và mọi giao dịch đều phải thông qua tổ chức đó, tương tự như một ngân hàng.

Chúng ta cần một giải pháp làm sao để người thụ hưởng biết được chủ sở hữu trước đã không ký bất kỳ giao dịch nào trước đó. Với mục tiêu giao dịch sớm nhất là giao dịch được công nhận, chúng ta không quan tâm tới những cố gắng thực hiện lặp chi sau đó. Cách duy nhất để xác định giao dịch nào thiếu là nhận thức được toàn bộ các giao dịch. Trong mô hình xưởng phát hành, xưởng sẽ nhận thức tất cả các giao dịch và quyết định xem giao dịch nào tới đầu tiên. Để quyết định được điều này khi không có bên thứ ba đáng tin cậy, các giao dịch phải được thông báo công khai [1], và chúng ta cần một hệ thống để người tham gia có thể tán thành một bản ghi chép trình tự những gì họ đã nhận được. Người thụ hưởng cần bằng chứng rằng vào thời điểm mỗi giao dịch diễn ra, đa số các nút đều đồng thuận giao dịch đó được nhận đầu tiên.

**3. Hệ thống nhãn thời gian**

Giải pháp mà chúng tôi đưa ra bắt đầu với một hệ thống nhãn thời gian. Một hệ thống nhãn thời gian hoạt động bằng cách lấy mã băm của một khối các mục dữ liệu để gắn nhãn thời gian rồi công bố

rộng rãi mã băm đó, chẳng hạn qua báo hoặc các trạm Usenet [2-5]. Rõ ràng là, nhãn thời gian cho thấy rằng dữ liệu đã tồn tại vào thời điểm nào đó mới lấy được mã băm. Mỗi nhãn thời gian bao hàm nhãn thời gian liền trước trong mã băm, hình thành một chuỗi, với mỗi nhãn thời gian bổ sung lại góp phần củng cố thêm cho các nhãn trước đó.

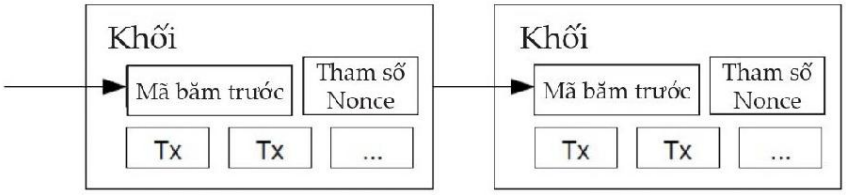



**4. Bằng Chứng Xử Lý**

Để triển khai hệ thống nhãn thời gian phân tán trên một nền tảng ngang cấp, chúng ta sẽ cần sử dụng một hệ thống bằng chứng xử lý tương tự như Hashcash của Adam Back [6], thay vì báo hoặc các trạm Usenet. Bằng Chứng Xử Lý chịu trách nhiệm quét một giá trị mà khi giá trị đó được băm, chẳng hạn như SHA-256, mã băm sinh ra bắt đầu bằng nhiều số nhị phân 0. Hoạt động xử lý yêu cầu thông thường là hàm mũ của một lượng số nhị phân 0 cần thiết, và có thể được xác thực thông qua việc chạy một mã băm.

Trong mạng lưới nhãn thời gian, chúng ta thực hiện Bằng Chứng Xử Lý bằng cách tăng lần lượt một tham số Nonce trong khối cho đến khi tìm ra giá trị để đưa các số nhị phân 0 cần thiết vào mã băm

của khối đó. Ngay khi công suất CPU được sử dụng để khối đó thỏa mãn bằng chứng xử lý, khối sẽ không thể bị thay đổi mà không trải qua quá trình tái xử lý. Vì các khối sau sẽ gắn thành chuỗi vào khối đó, hoạt động thay đổi khối đó sẽ bao hàm việc tái xử lý toàn bộ các khối sau nó.




Bằng Chứng Xử Lý còn giải quyết được vấn đề xác minh kết quả đa số trong quá trình ra quyết định. Nếu đa số được dựa trên mỗi-địa- chỉ-IP-một-phiếu-bầu, nó có thể bị thao túng nếu ai đó có thể kiểm soát được nhiều địa chỉ IP. Bằng Chứng Xử Lý về cơ bản là mỗi-CPU-một- phiếu-bầu. Quyết định của đa số được thể hiện qua chuỗi dài nhất, đây là kết quả Bằng Chứng Xử Lý lớn nhất đầu tư vào đó. Nếu đa số công suất CPU được các nút trung thực kiểm soát, chuỗi trung thực sẽ phát triển nhanh nhất và bỏ xa những chuỗi cạnh tranh. Để sửa đổi một khối cũ, kẻ tấn công sẽ phải sửa lại bằng chứng xử lý của khối đó và tất cả các khối sau nó rồi mới có thể bắt kịp và vượt qua thành quả của các nút trung thực. Trong phần sau, chúng ta sẽ thấy rằng xác suất để một kẻ tấn công chậm chạp bắt kịp được các nút trung thực giảm theo hàm số mũ khi các khối tiếp sau được bổ sung vào chuỗi.

Để bù đắp cho việc gia tăng tốc độ phần cứng và biến đổi lợi ích khi vận hành các nút theo thời gian, độ khó của Bằng Chứng Xử Lý được xác định bằng cách thay đổi định mức trung bình một số trung bình các khối mỗi giờ. Nếu các khối sinh ra quá nhanh, độ khó sẽ tăng lên.

**5. Mạng lưới**

Các bước vận hành mạng lưới như sau:

1) Các giao dịch mới được truyền tới tất cả các nút.

2) Mỗi nút tập hợp các giao dịch mới vào một khối.

3) Mỗi nút đi tìm một bằng chứng xử lý khó khăn cho khối của nó.

4) Khi một nút tìm ra một bằng chứng xử lý, nó truyền khối tới tất cả các nút.

5) Các nút chấp nhận khối đó chỉ khi toàn bộ các giao dịch trong khối hợp lệ.

6) Các nút thể hiện sự chấp thuận khối đó bằng cách thực hiện khởi tạo khối tiếp theo trong chuỗi, sử dụng mã băm của khối đã được chấp nhận với tư cách mã băm liền trước.

Các nút luôn luôn coi chuỗi dài nhất là chuỗi chính xác và sẽ tiếp tục hoạt động mở rộng chuỗi đó. Nếu hai nút đồng thời truyền hai phiên bản khối kế tiếp khác nhau, một số nút có thể nhận được bản này hoặc bản kia trước. Trong trường hợp đó, chúng hoạt động trên phiên bản đầu tiên chúng nhận được, nhưng vẫn dành ra một nhánh khác phòng trường hợp nó trở nên dài hơn. Mối liên kết sẽ bị phá vỡ khi bằng chứng xử lý tiếp theo được tìm ra và một nhánh dài hơn hẳn; các nút đang hoạt động trên nhánh kia sẽ chuyển sang nhánh dài hơn đó.

Giao dịch mới truyền đi không nhất thiết phải đi tới tất cả các nút. Chỉ cần chúng tới được nhiều nút, chúng sẽ ngay lập tức được đưa vào khối. Khối truyền đi cũng có thể gặp tình trạng thất lạc. Nếu một nút không nhận được một khối, nó sẽ yêu cầu khối đó khi nó nhận được khối liền sau và phát hiện ra nó bị lỡ mất một khối.

**6. Động lực**

Thông thường, giao dịch đầu tiên trong một khối là một giao dịch đặc biệt tạo ra một đồng tiền mới thuộc sở hữu của người khởi tạo khối. Điều này tăng thêm động lực để các nút hỗ trợ mạng lưới, và đưa ra cách thức để bắt đầu lưu hành đồng tiền, vì không tồn tại tổ chức trung tâm phát hành tiền tệ. Phần thêm ổn định của một số lượng tiền mới không đổi cũng tương tự như những người thợ mỏ đào vàng vận dụng các nguồn lực để đưa thêm vàng vào lưu hành. Trong trường hợp của chúng ta, nguồn lực sử dụng là thời gian và điện năng CPU.

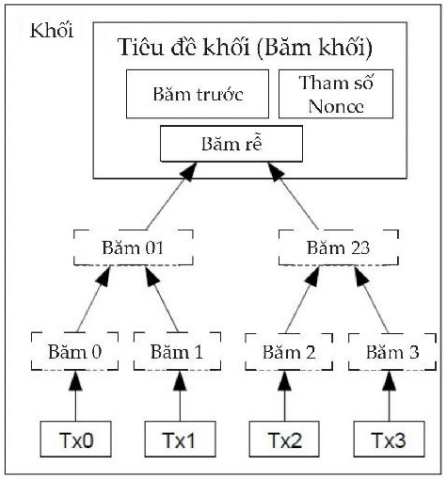
Sự khích lệ còn bao gồm cả phí giao dịch. Nếu giá trị xuất của một giao dịch nhỏ hơn giá trị nhập, sự chênh lệch này là phí giao dịch được thêm vào giá trị khích lệ của khối hàm chứa giao dịch đó. Khi một lượng tiền dự tính được đưa vào lưu hành, phần khích lệ có thể chuyển toàn bộ thành phí giao dịch và hoàn toàn không có lạm phát.

Phần khích lệ có thể giúp khuyến khích các nút duy trì tính trung thực. Nếu một kẻ tấn công tham lam có khả năng tập hợp nhiều công suất CPU hơn tất cả các nút trung thực, hắn ta sẽ phải lựa chọn sử dụng lợi thế này để lừa gạt mọi người bằng cách trộm lại các khoản thanh toán hoặc tạo ra các đồng tiền mới. Anh ta hẳn nên thấy tuân thủ quy định sẽ có lợi hơn nhiều, những quy định đó mang

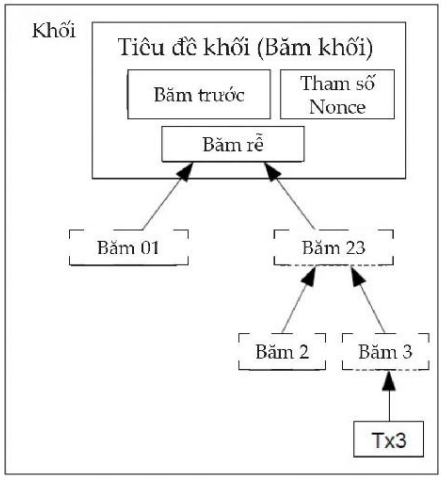
đến cho anh ta nhiều đồng tiền mới hơn những người khác cộng lại, hơn hẳn việc phá hoại hệ thống và sự giàu có hợp thức của anh ta.

**7. Thu hồi không gian lưu trữ**

Khi giao dịch cuối trong một đồng tiền có đủ số khối thêm vào phía trên, các giao dịch đã dùng trước nó có thể được loại bỏ để tiết kiệm không gian lưu trữ. Để làm được việc này mà không làm ảnh hưởng tới mã băm của khối, các giao dịch được băm trong một Cây Merkle [7] [2][5], với duy nhất rễ cây là một phần trong mã băm của khối. Các khối cũ sau đó có thể được thu gọn bằng cách cắt bỏ các cành cây. Những băm nội bộ không cần phải lưu trữ.




Các giao dịch được băm trong một cây Merkle



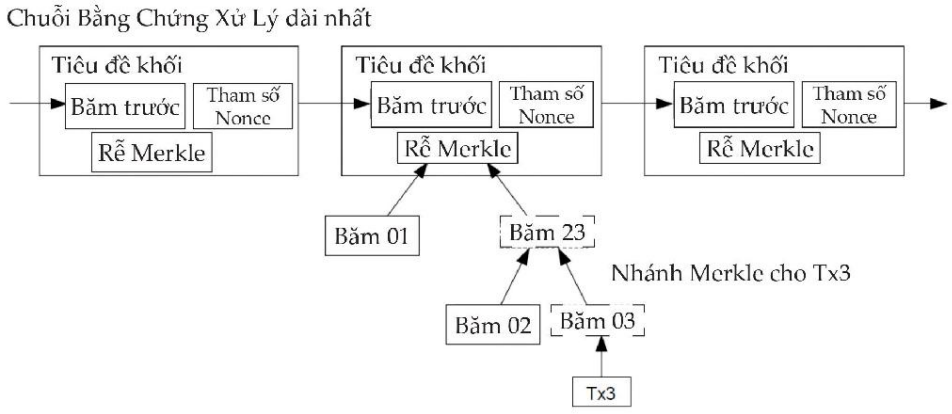

Sau khi cắt bỏ Tx0-2 từ khối

Một tiêu đề khối không có giao dịch sẽ vào khoảng 80 byte. Nếu chúng ta giả định rằng các khối được sinh ra cứ mỗi 10 phút, 80 byte * 6 * 24 * 365 = 4.2MB mỗi năm. Với hệ thống máy tính bán ra tiêu chuẩn RAM 2GB vào năm 2008, và định luật Moore dự đoán tốc

độ tăng trưởng hiện thời 1.2GB mỗi năm, việc lưu trữ sẽ không phải vấn đề ngay cả khi các tiêu đề khối cần được lưu trong bộ nhớ.

**8. Xác thực thanh toán đơn giản hóa**

Có thể xác thực các khoản thanh toán mà không cần vận hành toàn bộ các nút trong mạng lưới. Người dùng chỉ cần giữ bản lưu các tiêu đề khối của chuỗi bằng chứng công việc dài nhất, điều này anh ta có thể thực hiện được bằng cách truy vấn các nút trong mạng lưới cho tới khi anh ta bảo đảm được rằng anh ta sở hữu chuỗi dài nhất, và có được nhánh cây Merkle liên kết giao dịch với khối mà nó được gắn nhãn thời gian vào. Anh ta không thể tự kiểm tra giao dịch, nhưng bằng cách liên kết giao dịch đó vào một vị trí trên chuỗi, anh ta có thể thấy một nút trong mạng lưới đã chấp nhận hay chưa, và các khối được thêm vào sau đó sẽ xác nhận thêm rằng mạng lưới đã chấp nhận nó.

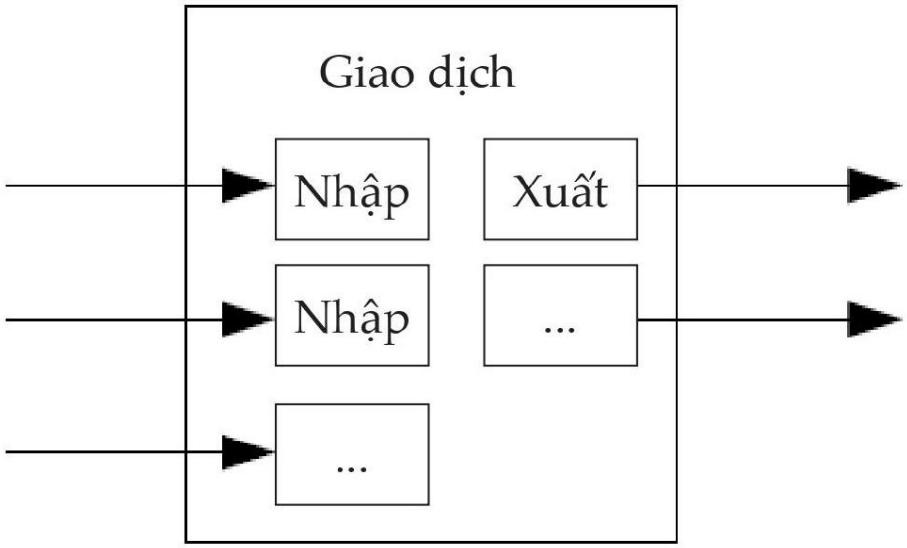



Như thế, việc xác thực được coi là đáng tin cậy khi các nút trung thực kiểm soát mạng lưới, nhưng dễ bị phá hoại nếu mạng lưới bị

một kẻ tấn công thao túng. Mặc dù các nút trong mạng lưới có thể tự xác thực giao dịch, phương thức đơn giản hóa có thể bị các giao dịch ngụy tạo của kẻ tấn công lừa gạt để kẻ này có thể tiếp tục thao túng mạng lưới. Chiến lược chống lại nguy cơ này là cho phép các nút trong mạng lưới báo lỗi khi chúng phát hiện ra một khối bất hợp lệ, thúc đẩy phần mềm của người dùng tải xuống khối trọn vẹn và các giao dịch bị cảnh báo để xác thực tính thống nhất. Các doanh nghiệp nhận thanh toán thường xuyên có lẽ sẽ vẫn muốn vận hành các nút riêng của họ để xác thực nhanh hơn và bảo mật chắc chắn hơn.

**9. Kết hợp và phân chia giá trị**

Mặc dù hoàn toàn có thể xử lý riêng rẽ các đồng tiền, nhưng thực hiện phân tách giao dịch với mỗi xu trong một lần chuyển giao là rất khó khăn. Để giá trị có thể được phân chia và kết hợp, các giao dịch bao gồm nhiều dữ liệu nhập và xuất. Thông thường, sẽ có hoặc một dữ liệu nhập đơn từ giao dịch lớn hơn trước đó hoặc nhiều dữ liệu nhập kết hợp các khoản nhỏ hơn, và có tối đa hai dữ liệu xuất: một để thanh toán, và một trả tiền thừa cho người gửi, nếu có.

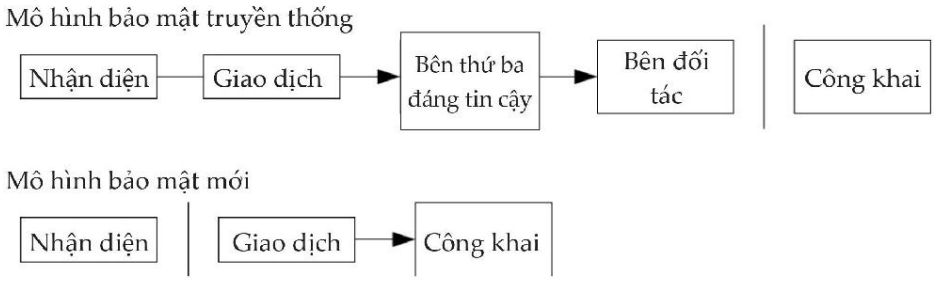



Cần chú ý rằng, tín hiệu ra, khi một giao dịch phụ thuộc vào nhiều giao dịch, và các giao dịch đó lại phụ thuộc nhiều giao dịch khác, không phải vấn đề trong trường hợp này. Không cần phải trích xuất một bản sao lưu hoàn toàn riêng biệt về lịch sử của một giao dịch.

**10. Độ bảo mật**

Mô hình hoạt động của ngân hàng truyền thống đạt được mức độ bảo mật nào đó nhờ hạn chế được khả năng truy cập thông tin tới các bên liên quan và bên thứ ba đáng tin cậy. Sự cần thiết phải thông báo công khai toàn bộ các giao dịch đã chặn đứng đà phát triển của phương thức này, nhưng độ bảo mật vẫn được duy trì nhờ cách tiếp cận dòng thông tin theo một hướng khác: sử dụng các khóa công khai vô danh. Mọi người có thể thấy ai đó đang truyền gửi một khoản chi tới người khác, nhưng không có thông tin liên kết giao dịch với bất kỳ ai. Điều này cũng tương tự như mức độ thông

tin mà các sàn giao dịch chứng khoán cung cấp, tại đây thời gian và kích thước của các giao dịch cá nhân, hay "băng truyền thông tin" được công khai, nhưng không cho biết các bên tham gia là ai.




Với tư cách một tường lửa bổ sung, cặp khóa mới nên được sử dụng cho mỗi giao dịch để đảm bảo rằng các giao dịch đều liên kết với một chủ sở hữu chung. Một số kết nối vẫn không thể tránh khỏi các giao dịch đa đầu vào, điều này chắc chắn cho thấy rằng dữ liệu nhập của chúng thuộc cùng chủ sở hữu. Rủi ro là, nếu chủ sở hữu của một khóa bị lộ, các liên kết có thể tiết lộ các giao dịch khác cũng thuộc chủ sở hữu đó.

**11. Thao tác điện toán**

Chúng ta giả định một tình huống trong đó kẻ tấn công cố gắng tạo ra một chuỗi thay thế nhanh hơn hẳn chuỗi trung thực. Ngay cả khi điều này thành hiện thực, nó cũng không khiến hệ thống gặp phải những biến đổi bất thường, chẳng hạn như đột nhiên tạo ra một giá trị hoặc chiếm lấy tiền bạc không thuộc sở hữu của kẻ tấn công. Các nút sẽ không coi một giao dịch bất hợp lệ là một khoản thanh toán, và các nút trung thực sẽ không bao giờ đồng thuận một khối

có chứa giao dịch như thế. Kẻ tấn công chỉ có thể thay đổi được một trong số các giao dịch của chính hắn để lấy lại tiền hắn vừa chi.

Cuộc đua giữa chuỗi trung thực và chuỗi của kẻ tấn công có thể được diễn tả như một Bước Đi Nhị Thức Ngẫu Nhiên trong lý thuyết xác suất. Sự kiện thành công là chuỗi trung thực mở rộng thêm một khối, tăng vị trí lên +1, còn sự kiện thất bại là chuỗi tấn công mở rộng thêm một khối, giảm đi khoảng cách bằng -1.

Xác suất để một kẻ tấn công bắt kịp độ hụt cho trước cũng tương tự như vấn đề Gambler's Ruin (Bài toán Sạt nghiệp của Con bạc) trong lý thuyết xác suất thống kê. Giả định một con bạc với khoản nợ vô hạn bắt đầu từ điểm thâm hụt và có thể chơi vô số ván bài để đạt tới điểm hòa vốn. Chúng ta có thể tính ra xác suất để hắn hòa vốn, nói cách khác, để một kẻ tấn công bắt kịp chuỗi trung thực, như sau [8]:

p = xác suất để một nút trung thực tìm ra khối tiếp theo

q = xác suất để kẻ tấn công tìm ra khối tiếp theo

$q_z$ = xác suất để kẻ tấn công bắt kịp từ z khối phía sau

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

Giả định cho trước của chúng ta p > q, xác suất giảm theo số mũ vì số khối mà kẻ tấn công phải bắt kịp gia tăng. Nếu anh ta xui xẻo, nếu anh ta không thể may mắn tiến lên từ sớm, cơ hội của anh ta sẽ trở nên càng lúc càng nhỏ đến gần bằng 0 vì anh ta bị bỏ xa lại phía sau. Lúc này, chúng ta xem xét liệu người nhận một giao dịch mới cần chờ bao lâu trước khi đảm bảo được rằng người gửi không thay đổi giao dịch. Chúng ta giả định người gửi là một kẻ tấn công đang muốn người nhận tin rằng anh ta sẽ trả tiền trong chốc lát, sau đó lại chuyển ngược trả về cho anh ta. Người nhận sẽ được cảnh báo chuyện gì đang diễn ra, nhưng người nhận hy vọng rằng sẽ không quá trễ.

Người nhận tạo một cặp khóa mới và giao khóa công khai cho người gửi ngay trước khi ký. Điều này giúp ngăn chặn người gửi không chuẩn bị được một chuỗi các khối trước thời hạn bằng cách liên tục hoạt động trên đó cho tới khi anh ta đủ may mắn để vượt lên đủ xa, sau đó xử lý giao dịch tại thời điểm đó. Ngay khi giao dịch được gửi đi, người gửi gian lận bắt đầu bí mật hoạt động trên một chuỗi song song có chứa phiên bản giao dịch thay thế của anh ta.

Người nhận chờ tới khi giao dịch được đưa vào một khối và z khối đã được kết nối sau khối đó. Người này không biết chính xác tiến độ mà kẻ tấn công đã tạo ra, nhưng giả sử các khối trung thực đã tính trung bình thời gian dự kiến cho mỗi khối, tiến độ khả dĩ của kẻ tấn công sẽ là một Phân phối Poisson với giá trị dự kiến:

$$\lambda = z\frac{q}{p}$$

Lúc này, để thu được xác suất sao cho kẻ tấn công có thể bắt kịp, chúng ta nhân mật độ Poisson cho mỗi mức tiến độ mà anh ta có thể thực hiện bằng xác suất bắt kịp của anh ta vào thời điểm đó:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{cases}$$

Tái sắp xếp để tránh cộng phần dư vô hạn của phân phối...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Chuyển sang mã C…

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
double p = 1.0 - q;
double lambda = z * (q / p);
double sum = 1.0;
int i, k;
for (k = 0; k <= z; k++)
{
double poisson = exp(-lambda);
for (i = 1; i <= k; i++)
poisson *= lambda / i;
sum -= poisson * (1 - pow(q / p, z - k));
}
return sum;
}
```

Chạy một số kết quả, chúng ta có thể thấy xác suất giảm dần theo hàm số mũ với z.

```
q=0.1
z=0 P=1.0000000
z=1 P=0.2045873
z=2 P=0.0509779
z=3 P=0.0131722
z=4 P=0.0034552
z=5 P=0.0009137
z=6 P=0.0002428
```

z=7 P=0.0000647

z=8 P=0.0000173

z=9 P=0.0000046

z=10 P=0.0000012

q=0.3

z=0 P=1.0000000

z=5 P=0.1773523

z=10 P=0.0416605

z=15 P=0.0101008

z=20 P=0.0024804

z=25 P=0.0006132

z=30 P=0.0001522

z=35 P=0.0000379

z=40 P=0.0000095

z=45 P=0.0000024

z=50 P=0.0000006

Giải với P nhỏ hơn 0,1%... P < 0.001

q=0.10 z=5

q=0.15 z=8

q=0.20 z=11

q=0.25 z=15

q=0.30 z=24

q=0.35 z=41

q=0.40 z=89

q=0.45 z=340

**12. Kết luận**

Chúng ta đã đưa ra một hệ thống giao dịch điện tử không phụ thuộc vào niềm tin. Chúng ta đã bắt đầu từ khung tiền tệ thông thường được tạo ra từ chữ ký kỹ thuật số, loại công nghệ cho phép quản lý sát sao quyền sở hữu, nhưng còn thiếu cách ngăn chặn tình trạng giao dịch lặp chi. Để giải quyết vấn đề này, chúng tôi đề xuất một hệ thống ngang cấp sử dụng bằng chứng xử lý để ghi chép một lịch sử giao dịch công khai sẽ nhanh chóng khiến một kẻ tấn công không thể sửa đổi về phương diện tính toán nếu các nút trung thực kiểm soát đa số công suất CPU. Mạng lưới hoạt động mạnh mẽ nhờ tính đơn giản bất cấu trúc của nó. Các nút hoạt động đồng thời mà chỉ cần phối hợp một chút. Chúng không cần phải nhận dạng, vì các thông điệp không được truyền tới một điểm cụ thể bất kỳ nào mà chỉ được phân phối trên cơ sở thỏa thuận nỗ lực tối đa. Các nút có thể rời bỏ rồi tái gia nhập mạng lưới tùy ý, chấp nhận chuỗi bằng chứng xử lý như một minh chứng những gì đã diễn ra trong lúc vắng mặt. Chúng biểu quyết bằng công suất CPU, thể hiện sự chấp thuận các khối hợp lệ bằng cách hoạt động mở rộng các khối đó và bác bỏ các khối bất hợp lệ bằng cách từ chối hoạt động trên đó. Mọi quy định và động lực cần thiết đều có thể được thực hiện nhờ cơ chế đồng thuận này.

# Nguồn tham khảo

[1] W. Dai, "b-money," http://www.weidai. com/bmoney.txt, năm 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," trong 20th Symposium on Information Theory in the Benelux, tháng Năm năm 1999.

[3] S. Haber, W.S. Stornetta, "How to time- stamp a digital document," trong Journal of Cryptology, tập 3, số 2, trang 99-111, năm 1991. [4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," trong Sequences II: Methods in Communication, Security and Computer Science, trang 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," trong Proceedings of the 4th ACM Conference on Computer and Communications Security, trang 28-35, tháng Tư năm 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure,"http://www.hashcash.org/ papers/hashcash.pdf, năm 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, trang 122-133, tháng Tư năm 1980.

[8] W. Feller, "An introduction to probability theory and its applications," năm 1957.