CHƯƠNG 5: CÁC THÁCH THỨC VÀ XU HƯỚNG MỚI CỦA BLOCKCHAIN

5.1. Các thách thức của Blockchain

Để Bitcoin có thể trở thành *"tài sản số kiểu mới"* như (và có thể là hơn) cách mà vàng đã từng làm được trong thế giới thực, hay Ethereum đóng vai trò *máy tính của thế giới* (Vitalik Buterin, đồng sáng lập Ethereum), hoặc Cardano là *nền tảng Blockchain công cộng phục vụ hàng tỷ người* (Charles Hoskinson, nhà sáng lập Cardano) ... các nền tảng Blockchain cần vượt qua một loạt các thách thức. Chương này sẽ phân tích từ những thách thức kỹ thuật cơ bản, được gọi là "bộ ba tam giác bất khả thi" (Blockchain Trilemmas), đến các thách thức liên quan đến ứng dụng đại trà của các nền tảng Blockchain trong cuộc sống.

"Bộ ba tam giác bất khả thi" lần đầu được đề cập đến trong một bài viết của Vitalik Buterin năm 2017, đề cập đến ba yếu tố quan trọng mà bất kỳ nền tảng Blockchain nào cũng phải cân bằng: sự phân tán (decentralization), mức độ bảo mật (security), và khả năng mở rộng (scalability). Theo lý thuyết, rất khó để một Blockchain tối ưu hóa cả ba yếu tố này cùng lúc. Ví dụ, nếu tập trung vào khả năng mở rộng để xử lý nhiều giao dịch hơn trong thời gian ngắn, nền tảng có thể phải hy sinh một phần mức độ phân tán hoặc bảo mật. Ngược lại, khi ưu tiên bảo mật hoặc phân tán, khả năng mở rộng thường bị giảm đi. Thách thức này buộc các nhà phát triển phải đưa ra những giải pháp sáng tạo để đạt được sự cân bằng hợp lý giữa các yếu tố mà không làm suy giảm mục tiêu cốt lõi của Blockchain.

Ngoài các thách thức về mặt kỹ thuật, các nền tảng Blockchain cũng phải đối mặt với nhiều vấn đề khác. Thách thức pháp lý là một trong số đó, xuất phát từ tính mới mẻ của công nghệ và việc một số cá nhân hoặc tổ chức lợi dụng Blockchain để thực hiện các hành vi bất hợp pháp như rửa tiền, lừa đảo, hoặc kinh doanh đa cấp. Những vấn đề này không chỉ làm giảm lòng tin của công chúng mà còn khiến các cơ quan quản lý phải ban hành nhiều chính sách kiểm soát chặt chẽ hơn, đôi khi làm chậm lại quá trình phát triển của ngành.

Bên cạnh đó, độ phức tạp của các ứng dụng Blockchain cũng là một rào cản lớn. Việc hiểu và sử dụng công nghệ này đòi hỏi một mức độ kiến thức nhất định, khiến nó khó tiếp cận với đại đa số người dùng. Nhận thức của xã hội về Blockchain vẫn còn hạn chế, và nhiều người thậm chí vẫn coi đây là một công nghệ không thực tế hoặc mang tính đầu cơ cao. Hơn nữa, sự thiếu hụt các chuyên gia có kinh nghiệm trong lĩnh vực này cũng cản trở khả năng ứng dụng

Blockchain vào các lĩnh vực thực tiễn, làm giảm tốc độ mà công nghệ này có thể tích hợp vào cuộc sống hàng ngày.

Chúng ta sẽ cùng nhau tìm hiểu về các thách thức trong phần dưới đây

5.1.1. Thách thức về mặt kỹ thuật

5.1.1.1. Khả năng mở rộng (Scalability)

Một trong những thách thức lớn nhất của blockchain là khả năng mở rộng. Vấn đề này thể hiện qua các khía cạnh sau:

• **Giới hạn kích thước block**: Mỗi block trên blockchain có kích thước cố định, giới hạn số lượng giao dịch có thể xử lý trong một thời gian nhất định. Ví dụ, Bitcoin với giới hạn block 1 MB thường gặp tắc nghẽn khi số lượng giao dịch tăng cao, khiến thời gian xác nhận kéo dài. Ethereum cũng gặp vấn đề tương tự trong quá khứ do phụ thuộc vào gas limit cho mỗi block, đặc biệt khi có nhiều ứng dụng phi tập trung (dApps) hoạt động trên nền tảng này.

• **Thời gian xử lý giao dịch**: Với các cơ chế đồng thuận như đã nêu ở chương trước, thời gian xác nhận giao dịch có thể kéo dài từ vài phút đến hàng giờ trong thời điểm mạng tắc nghẽn. Ví dụ, Bitcoin sử dụng cơ chế Proof of Work (PoW), khiến thời gian trung bình để thêm một block mới mất khoảng 10 phút. Trong khi đó, Ethereum, sau khi chuyển sang cơ chế Proof of Stake (PoS) vào năm 2022 thông qua sự kiện "The Merge," đã cải thiện hiệu suất và giảm mức tiêu thụ năng lượng. Tuy nhiên, thời gian chờ xử lý giao dịch vẫn có thể kéo dài trong các giai đoạn cao điểm.

• **Chi phí giao dịch**: Khi lưu lượng tăng cao, cả Bitcoin và Ethereum đều từng chứng kiến chi phí giao dịch tăng vọt. Trên Ethereum, chi phí gas đã giảm nhờ các giải pháp Layer-2 như Optimistic Rollup và zk-Rollups, nhưng tình trạng phí tăng đột biến vẫn có thể xảy ra khi có nhiều hợp đồng thông minh hoặc dApps hoạt động đồng thời.

Để giải quyết các vấn đề về khả năng mở rộng, nhiều phương án đã được triển khai và tiếp tục phát triển:

1. **Chuyển đổi cơ chế đồng thuận**: Ethereum đã hoàn tất chuyển đổi từ cơ chế Proof of Work (PoW) – chậm chạp và tốn kém năng lượng - sang Proof of Stake (PoS) – nhanh chóng và giảm tối đa năng lượng tiêu thụ- vào năm 2022 thông qua sự kiện lịch sử "The Merge." Đây là bước quan trọng trong lộ trình Ethereum 2.0 nhằm nâng cao khả năng mở rộng và giảm tác động môi trường. Trước "The Merge," mạng Ethereum vận hành song song hai chuỗi: chuỗi chính (Mainnet) dựa trên PoW và Beacon Chain dựa

trên PoS. Khi "The Merge" xảy ra, hai chuỗi này được hợp nhất, loại bỏ PoW hoàn toàn và Ethereum chính thức hoạt động hoàn toàn dựa trên PoS. Sau khi chuyển sang POS, mạng Ethreum đã đạt được những kết quả ấn tượng ban đầu:

- **Hiệu quả năng lượng**: PoS giảm tới 99.95% lượng năng lượng tiêu thụ so với PoW.
- **Bảo mật cao hơn**: PoS yêu cầu người xác thực khóa một lượng lớn ETH để tham gia, làm tăng chi phí tấn công mạng.
- **Nền tảng cho các cải tiến tiếp theo**: Việc chuyển sang PoS mở đường cho các giải pháp mở rộng như sharding.

2. **Sharding**: Đây là một trong những giải pháp quan trọng trong lộ trình phát triển của Ethereum. Sharding chia mạng lưới blockchain thành nhiều phân đoạn nhỏ hơn, gọi là "shards." Mỗi shard có thể xử lý các giao dịch và hợp đồng thông minh một cách độc lập, giúp mạng lưới xử lý nhiều giao dịch song song thay vì tuần tự trên một chuỗi duy nhất. Ví dụ, một ngân hàng phải xử lý 1.000 giao dịch cùng lúc. Nếu ngân hàng có 10 chi nhánh (tương tự như các shard), mỗi chi nhánh chỉ cần xử lý 100 giao dịch thay vì toàn bộ 1.000 giao dịch. Điều này giúp tiết kiệm thời gian và giảm tải cho hệ thống chính. Trên Ethereum, sharding sẽ làm giảm áp lực lên mạng lưới chính (Layer-1), giúp tăng tốc độ giao dịch và giảm chi phí.

   Tính đến 2025, sharding vẫn đang trong giai đoạn triển khai, dự kiến sẽ trở thành một phần quan trọng của Ethereum trong các năm tới với những cải tiến phù hợp. Đây là bước tiếp theo sau sự kiện "The Merge," giúp Ethereum đạt được mục tiêu khả năng mở rộng và tương thích tốt hơn với các ứng dụng phi tập trung.

3. **Layer-2**: Các giải pháp Layer-2 như Lightning Network cho Bitcoin, Optimistic Rollup, zk-Rollups, và Polygon trên Ethereum đã được áp dụng rộng rãi. Chúng giúp giảm tải mạng lưới chính (Layer-1) và cải thiện tốc độ xử lý cũng như giảm chi phí giao dịch.

4. **Blockchain thế hệ mới**: Các dự án như Solana, Avalanche, Cardano, Sui, Aptos… đã đưa ra các cải tiến mới về khả năng mở rộng và tương tác giữa các blockchain. Solana nổi bật với tốc độ xử lý giao dịch cao, trong khi Aptos và Sui tập trung vào hiệu quả lập trình và khả năng xử lý dữ liệu song song.

Nhờ những cải tiến này, hệ sinh thái blockchain đã dần khắc phục được nhiều hạn chế về khả năng mở rộng, tạo nền tảng cho sự phát triển bền vững và mở rộng ứng dụng trong thực tế.

5.1.1.2 Vấn đề về bảo mật

Mặc dù blockchain được thiết kế với tính bảo mật cao nhờ các cơ chế mã hóa và phi tập trung, vẫn tồn tại một số điểm yếu tiềm tàng mà nếu không được quản lý tốt, có thể gây ảnh hưởng nghiêm trọng đến hệ thống.

- **Tấn công 51%**: Đây là một trong những rủi ro lớn nhất đối với các blockchain sử dụng cơ chế đồng thuận Proof of Work (PoW). Một cuộc tấn công 51% xảy ra khi một thực thể hoặc nhóm kiểm soát hơn 50% sức mạnh tính toán (hash power) của toàn bộ mạng. Với quyền lực này, kẻ tấn công có thể thao túng mạng lưới bằng cách tạo ra các khối giả mạo, đảo ngược giao dịch đã xác nhận, hoặc ngăn chặn các giao dịch mới. Điều này làm mất đi tính toàn vẹn và đáng tin cậy của mạng blockchain. Tuy nhiên, tấn công này thường khó xảy ra với các blockchain lớn như Bitcoin do chi phí và tài nguyên cần thiết là rất lớn.
- **Lỗ hổng trong hợp đồng thông minh**: Smart Contract là những đoạn mã tự động hóa các quy tắc và giao dịch trên blockchain, nhưng chúng không tránh khỏi lỗi lập trình hoặc thiết kế. Các lỗ hổng trong mã nguồn có thể bị khai thác bởi các hacker để trộm tiền hoặc phá hủy dữ liệu. Một ví dụ điển hình là vụ tấn công DAO trên Ethereum vào năm 2016, khi hacker tận dụng lỗi trong mã hợp đồng thông minh để rút hàng triệu đô la từ quỹ. Vì vậy, việc kiểm tra và kiểm toán mã nguồn (auditing) kỹ lưỡng là cực kỳ quan trọng để giảm thiểu rủi ro này.
- **Nguy cơ từ máy tính lượng tử**: Với sức mạnh tính toán vượt trội, máy tính lượng tử có thể đe dọa phá vỡ các thuật toán mã hóa hiện tại của blockchain như SHA-256 (Bitcoin) hoặc ECDSA (Ethereum). Các thuật toán này vốn được thiết kế để chống lại các cuộc tấn công từ máy tính cổ điển, nhưng không đủ khả năng chống lại sự tiến bộ của máy tính lượng tử. Nếu các thuật toán mã hóa bị phá vỡ, toàn bộ dữ liệu trên blockchain có thể bị giải mã, dẫn đến nguy cơ mất an toàn thông tin và tài sản. Chúng ta tạm thời yên tâm rằng ở thời điểm hiện tại, các nhà nghiên cứu và nhà phát triển đang tích cực làm việc để tạo ra các thuật toán mã hóa kháng lượng tử nhằm bảo vệ blockchain trong tương lai.

Những điểm yếu này nhấn mạnh rằng, mặc dù blockchain là một công nghệ tiên tiến và bảo mật cao, nó không phải là bất khả xâm phạm. Việc nâng cấp liên tục, kết hợp với các biện

pháp bảo vệ như kiểm toán mã nguồn, tăng cường phi tập trung, và nghiên cứu công nghệ kháng lượng tử, là cần thiết để duy trì sự an toàn và phát triển bền vững của blockchain.

5.1.1.3. Tiêu thụ năng lượng và tác động môi trường

Các mạng lưới blockchain, đặc biệt là những hệ thống sử dụng cơ chế đồng thuận Proof of Work (PoW) như Bitcoin và Ethereum trước khi chuyển đổi sang Proof of Stake (PoS), đã bị chỉ trích vì mức tiêu thụ năng lượng cao và tác động tiêu cực đến môi trường.

Tiêu thụ năng lượng của các mạng lưới Blockchain

PoW yêu cầu các "thợ đào" giải quyết các bài toán mật mã phức tạp để xác minh giao dịch và tạo ra khối mới. Quá trình này sử dụng một lượng lớn tài nguyên tính toán, dẫn đến mức tiêu thụ năng lượng khổng lồ. Theo các ước tính:

- Mạng lưới Bitcoin tiêu thụ khoảng 110 TWh mỗi năm (tương đương mức tiêu thụ của một quốc gia nhỏ như Hà Lan).
- Ethereum trước khi chuyển đổi sang PoS tiêu thụ khoảng 70 TWh/năm.

Việc tiêu thụ năng lượng chủ yếu đến từ các trung tâm dữ liệu và thiết bị chuyên dụng (ASIC, GPU), thường được vận hành 24/7 tại các quốc gia có giá điện thấp.

Tác động môi trường

Nguồn điện cho các mạng lưới blockchain thường đến từ năng lượng hóa thạch như than đá hoặc khí tự nhiên, dẫn đến lượng lớn khí CO2 thải vào môi trường. Các nghiên cứu chỉ ra rằng:

- Hoạt động khai thác Bitcoin thải ra khoảng 60-70 triệu tấn CO2 mỗi năm.
- Tình trạng nóng lên toàn cầu và cạn kiệt tài nguyên năng lượng là những hậu quả đáng kể.

Ngoài ra, việc sản xuất và vận hành các thiết bị đào cũng tạo ra chất thải điện tử khổng lồ, gây thêm áp lực lên môi trường.

Cách thức vận hành giảm tác động

Các giải pháp được đề xuất và triển khai nhằm giảm thiểu tác động môi trường của blockchain bao gồm:

- **Chuyển đổi sang Proof of Stake (PoS):** Ethereum đã thành công chuyển đổi sang PoS vào năm 2022, giảm mức tiêu thụ năng lượng xuống hơn 99,9%. PoS không yêu

cầu các bài toán mật mã phức tạp, thay vào đó, các trình xác thực được chọn dựa trên số lượng tài sản nắm giữ.

- **Sử dụng năng lượng tái tạo:** Các trung tâm dữ liệu khai thác đang hướng đến việc sử dụng năng lượng mặt trời, gió và thủy điện để giảm lượng phát thải carbon. Ví dụ, tại Iceland và Canada, các công ty khai thác tận dụng nguồn năng lượng địa nhiệt và thủy điện dồi dào.
- **Off-chain và Layer 2:** Các giải pháp mở rộng như Lightning Network hoặc Optimistic Rollup giúp giảm tải giao dịch trực tiếp trên blockchain, từ đó giảm tiêu thụ năng lượng tổng thể.
- **Quy định và chính sách:** Một số quốc gia đang áp dụng các chính sách hạn chế khai thác PoW hoặc ưu tiên các dự án blockchain thân thiện với môi trường.

Ví dụ thực tế

Ethereum sau khi chuyển sang PoS đã trở thành một minh chứng rõ ràng về việc blockchain có thể duy trì tính phi tập trung và bảo mật mà không tiêu tốn quá nhiều năng lượng. Bên cạnh đó, các mạng lưới blockchain mới như Algorand, Cardano, và Polkadot cũng sử dụng các cơ chế đồng thuận tiết kiệm năng lượng ngay từ khi thiết kế, để tối ưu hóa hiệu suất và giảm tác động môi trường.

Tóm lại, mặc dù blockchain mang lại nhiều lợi ích cho xã hội và kinh tế, nhưng vấn đề năng lượng và môi trường vẫn cần được quản lý chặt chẽ để đảm bảo tính bền vững lâu dài

5.1.2. Thách thức về quản trị và khả năng tương tác

5.1.2.1. Thách thức về quản trị của các mạng lưới Blockchain

Quản trị blockchain đề cập đến cách thức các quyết định được đưa ra và thực thi trong hệ thống, bao gồm việc quản lý các cập nhật, thay đổi trong giao thức và cách giải quyết các tranh chấp. Các thách thức lớn về quản trị blockchain bao gồm:

a. Quyết định tập trung vs. phi tập trung

Mặc dù blockchain thường được thiết kế để phi tập trung, nhiều dự án lại gặp phải vấn đề về sự tập trung quyền lực trong tay một số ít người. Điều này xảy ra khi các nhóm phát triển, các "lãnh đạo" của dự án hoặc những người nắm giữ phần lớn token có thể kiểm soát các quyết định quan trọng, chẳng hạn như thay đổi giao thức hoặc cập nhật phần mềm.

Ví dụ, trong trường hợp của Bitcoin, sự kiểm soát của các thợ đào hoặc các tổ chức lớn về việc thay đổi giao thức hoặc nâng cấp mạng có thể gây ra sự chia rẽ trong cộng đồng, như đã xảy ra với việc chia tách thành Bitcoin và Bitcoin Cash vào năm 2017.

b. Thiếu sự đồng thuận trong cộng đồng

Mặc dù blockchain là hệ thống phân tán, nhưng việc đạt được sự đồng thuận giữa các bên liên quan trong cộng đồng lại rất khó khăn. Các thay đổi trong giao thức hoặc các nâng cấp mạng có thể gặp phải sự phản đối từ một bộ phận người dùng hoặc các nhà phát triển. Điều này có thể dẫn đến các phân mảnh mạng (hard forks) hoặc các vấn đề lớn trong việc duy trì tính thống nhất của mạng. Ví dụ, việc nâng cấp Ethereum từ Proof of Work (PoW) sang Proof of Stake (PoS) đã gặp phải rất nhiều tranh cãi trước khi thành công.

c. Khả năng quyết định của cộng đồng

Một số blockchain, chẳng hạn như Ethereum, đã áp dụng cơ chế quản trị phi tập trung thông qua các DAO (Decentralized Autonomous Organizations), nơi các quyết định được đưa ra thông qua việc bỏ phiếu của cộng đồng. Tuy nhiên, việc này vẫn gặp phải nhiều vấn đề như sự tham gia của cộng đồng hạn chế, sự thiếu vắng các cơ chế kiểm soát và những rủi ro về việc bị thao túng bởi các nhóm có ảnh hưởng lớn.

5.1.2.2. Thách thức về khả năng tương tác của các mạng lưới Blockchain

Khả năng tương tác giữa các blockchain (cross-chain interoperability) là một trong những yếu tố quan trọng để tạo ra một hệ sinh thái blockchain toàn diện, nơi các mạng lưới có thể giao tiếp và trao đổi dữ liệu hoặc tài sản với nhau. Tuy nhiên, vấn đề này gặp phải một số thách thức lớn:

a. Thiếu tiêu chuẩn chung

Mỗi blockchain đều có các đặc điểm và giao thức riêng biệt, điều này tạo ra sự phân mảnh lớn trong không gian blockchain. Các mạng lưới khác nhau có thể sử dụng các hệ thống đồng thuận, cách thức mã hóa và mô hình kinh tế hoàn toàn khác nhau. Việc này làm cho việc kết nối và tương tác giữa các blockchain trở nên phức tạp và đòi hỏi sự phát triển các công nghệ và tiêu chuẩn chung. Hiện tại, không có một tiêu chuẩn chung duy nhất cho khả năng tương tác của các mạng blockchain.

b. Cầu nối và trung gian

Một trong những phương pháp hiện tại để giải quyết vấn đề tương tác giữa các blockchain là thông qua các cầu nối (bridges), cho phép chuyển tài sản và dữ liệu giữa các mạng lưới khác

nhau. Tuy nhiên, cầu nối cũng mang lại những rủi ro, đặc biệt là vấn đề bảo mật. Các vụ tấn công nhằm vào các cầu nối blockchain, chẳng hạn như hack Poly Network năm 2021, đã làm lộ ra những lỗ hổng trong hệ thống, gây thiệt hại hàng trăm triệu đô la.

c. Các giải pháp Layer 2 và giao thức liên chuỗi

Các giải pháp Layer 2 như Lightning Network (cho Bitcoin) và các giao thức liên chuỗi như Polkadot, Cosmos, hay Avalanche được phát triển để giải quyết vấn đề khả năng tương tác. Các giải pháp này cho phép nhiều blockchain giao tiếp và tương tác với nhau mà không cần phải thay đổi cấu trúc bên trong của từng mạng lưới. Tuy nhiên, các giải pháp này vẫn đang trong giai đoạn phát triển và không phải lúc nào cũng dễ dàng triển khai và duy trì.

5.1.2.3. Ví dụ thực tế

- **Ethereum và Bitcoin:** Mặc dù Ethereum và Bitcoin đều là hai blockchain lớn và phổ biến nhất, chúng không thể giao tiếp trực tiếp với nhau. Các giải pháp như wrapped Bitcoin (WBTC) trên Ethereum giúp giải quyết vấn đề này, nhưng vẫn có những hạn chế và không phải là một giải pháp tối ưu.
- **Polkadot:** Polkadot là một ví dụ về một blockchain được thiết kế từ đầu để hỗ trợ khả năng tương tác giữa các blockchain. Mạng Polkadot sử dụng một cơ chế gọi là parachains để kết nối các blockchain với nhau, giúp các ứng dụng và tài sản có thể chuyển giao giữa các mạng.

5.1.2.4. Tương lai của quản trị và khả năng tương tác

Mặc dù quản trị và khả năng tương tác của blockchain hiện tại còn nhiều thách thức, nhưng sự phát triển của các giao thức và nền tảng mới đang mở ra những cơ hội lớn. Các cơ chế quản trị phi tập trung đang ngày càng được hoàn thiện và phổ biến, đồng thời các giải pháp Layer 2 và giao thức liên chuỗi hứa hẹn sẽ giúp tạo ra một hệ sinh thái blockchain mạnh mẽ và liên kết chặt chẽ hơn trong tương lai.

Tóm lại, thách thức về quản trị và khả năng tương tác là những vấn đề quan trọng cần phải giải quyết để blockchain có thể trở thành một công nghệ thực sự phát triển và ứng dụng rộng rãi trong xã hội.

5.1.3. Thách thức về pháp lý và tuân thủ

5.1.3.1. Khung pháp lý chưa hoàn thiện

Một trong những thách thức lớn nhất trong việc áp dụng blockchain và cryptocurrency là khung pháp lý chưa hoàn thiện. Mặc dù blockchain đã tồn tại trong nhiều năm, các cơ quan pháp lý vẫn chưa hoàn thiện được các quy định cần thiết để điều chỉnh hoạt động của các mạng lưới này. Những vấn đề liên quan đến khung pháp lý bao gồm:

a. Thiếu các quy định rõ ràng về cryptocurrency và blockchain

Trong khi một số quốc gia đã bắt đầu xây dựng các quy định liên quan đến cryptocurrency và blockchain, phần lớn các quy định này còn thiếu rõ ràng và đầy đủ. Các quốc gia như Mỹ, Trung Quốc, và Liên minh Châu Âu đều đã bắt đầu thử nghiệm và đưa ra một số quy định, nhưng nhiều khía cạnh vẫn chưa được giải quyết, như cách thức phân loại các cryptocurrency, thuế đối với các giao dịch blockchain, hoặc các quy định về bảo vệ người tiêu dùng.

Ví dụ, tại Mỹ, Cơ quan Chứng khoán và Giao dịch (SEC) chưa đưa ra một định nghĩa rõ ràng về cryptocurrency và đối tượng quản lý đối với từng loại tiền kỹ thuật số. Điều này dẫn đến sự bất ổn trong các giao dịch và các quyết định đầu tư liên quan đến cryptocurrency.

b. Khác biệt trong quy định giữa các quốc gia

Một thách thức lớn khác là sự khác biệt trong quy định giữa các quốc gia. Mỗi quốc gia có một cách tiếp cận khác nhau đối với blockchain và cryptocurrency, tạo ra một môi trường pháp lý phức tạp. Một số quốc gia như Nhật Bản và Thụy Sĩ đã chấp nhận cryptocurrency và blockchain, coi chúng như một phần của nền kinh tế chính thống, trong khi các quốc gia khác như Trung Quốc và Ấn Độ đã đưa ra các biện pháp cấm hoặc hạn chế nghiêm ngặt đối với các hoạt động liên quan đến blockchain và cryptocurrency.

Sự khác biệt này không chỉ tạo ra sự thiếu đồng bộ trong các quy định mà còn làm cho các doanh nghiệp và cá nhân gặp khó khăn trong việc hoạt động xuyên quốc gia. Việc không có một hệ thống pháp lý thống nhất có thể khiến các công ty blockchain gặp khó khăn trong việc mở rộng và tuân thủ các quy định quốc tế.

Điều đáng mừng là trong năm 2024, Việt Nam đã ban hành Quyết định số 1236/QĐ-TTg của Thủ tướng Chính phủ về Chiến lược quốc gia ứng dụng và phát triển công nghệ chuỗi khối (blockchain) đến năm 2025, định hướng đến năm 2030. Quyết định này xác định Blockchain là một công nghệ trọng tâm cần được ưu tiên phát triển, với tầm nhìn đưa Việt Nam trở thành quốc gia dẫn đầu khu vực và có vị thế quốc tế trong nghiên cứu, triển khai công nghệ Blockchain vào năm 2030. Đây là nền tảng pháp lý quan trọng, góp phần thúc đẩy chuyển đổi

số toàn diện, đồng thời mở ra cơ hội phát triển mạnh mẽ cho công nghệ Blockchain tại Việt Nam hiện tại và trong tương lai.

c. Thách thức trong việc áp dụng luật hiện hành với công nghệ mới

Một trong những vấn đề lớn là việc áp dụng các luật hiện hành vào blockchain và cryptocurrency. Các luật hiện tại được thiết kế cho các hệ thống tài chính truyền thống và không phù hợp với các đặc điểm riêng biệt của blockchain như tính phi tập trung, sự ẩn danh và khả năng tự động hóa thông qua smart contracts. Điều này gây khó khăn cho các cơ quan quản lý trong việc điều chỉnh và áp dụng các quy định hiện hành đối với các công nghệ mới này.

5.1.3.2. Bảo vệ người dùng trong hệ sinh thái Blockchain

Một trong những yếu tố quan trọng cần được xem xét trong các mạng blockchain là bảo vệ người dùng. Mặc dù blockchain mang lại sự minh bạch và bảo mật, nhưng các vấn đề bảo vệ người dùng lại rất phức tạp, đặc biệt là trong môi trường phi tập trung và không có trung gian. Các thách thức lớn về bảo vệ người dùng bao gồm:

a. Thiếu cơ chế bảo vệ người dùng khi xảy ra sự cố

Trong hệ thống blockchain, các giao dịch là không thể thay đổi và không có một cơ chế rõ ràng để giải quyết khi có sự cố xảy ra, chẳng hạn như khi tài sản của người dùng bị đánh cắp hoặc mất. Việc thiếu các cơ chế pháp lý hoặc cơ chế bảo vệ người tiêu dùng khiến người dùng gặp nhiều rủi ro khi tham gia vào các mạng lưới blockchain.

Một ví dụ điển hình là các vụ hack các sàn giao dịch tiền mã hóa, nơi người dùng có thể mất tài sản mà không có cơ hội khôi phục hoặc bảo vệ quyền lợi của mình. Vì không có một cơ quan giám sát hoặc bảo vệ pháp lý như các ngân hàng truyền thống, việc yêu cầu bồi thường hoặc giải quyết tranh chấp trở nên khó khăn.

b. Khó khăn trong việc khôi phục tài sản số bị mất hoặc đánh cắp

Một vấn đề lớn khác trong blockchain là việc khôi phục tài sản số bị mất hoặc đánh cắp. Với tính chất phi tập trung và không có cơ chế giám sát trung gian, khi người dùng mất quyền truy cập vào ví của mình hoặc tài sản bị đánh cắp, rất khó để khôi phục hoặc có được sự hỗ trợ pháp lý. Các thợ đào hoặc hacker có thể lấy cắp tiền từ các ví điện tử mà không có cơ chế dễ dàng để lấy lại tài sản.

Một số sàn giao dịch hoặc dịch vụ ví điện tử cung cấp các giải pháp khôi phục mật khẩu hoặc tài khoản, nhưng chúng lại có hạn chế và không phải lúc nào cũng hiệu quả.

c. Vấn đề về quyền riêng tư và bảo mật thông tin

Blockchain cung cấp một mức độ bảo mật cao nhờ vào cơ chế mã hóa và phân tán, nhưng vấn đề bảo vệ quyền riêng tư vẫn là một thách thức. Các giao dịch trên blockchain, mặc dù được bảo vệ bởi các mã hóa phức tạp, vẫn có thể được theo dõi và phân tích nếu không sử dụng các biện pháp bảo vệ bổ sung như coin mixers hoặc các blockchain chuyên dụng cho quyền riêng tư như Monero và Zcash.

Ngoài ra, việc quản lý và bảo vệ dữ liệu cá nhân của người dùng trên các nền tảng blockchain vẫn chưa được quy định rõ ràng, đặc biệt khi blockchain là một công nghệ không thay đổi và lưu trữ dữ liệu vĩnh viễn. Việc lưu trữ dữ liệu nhạy cảm trên blockchain mà không có cơ chế bảo mật hợp lý có thể tạo ra nguy cơ rò rỉ thông tin và vi phạm quyền riêng tư của người dùng.

5.1.3.3. Tương lai của pháp lý và bảo vệ người dùng trong Blockchain

Để giải quyết các thách thức pháp lý và bảo vệ người dùng, các quốc gia và tổ chức quốc tế cần hợp tác để xây dựng các khuôn khổ pháp lý rõ ràng và phù hợp với công nghệ blockchain. Điều này có thể bao gồm việc xây dựng các tiêu chuẩn toàn cầu cho việc bảo vệ người tiêu dùng, tăng cường các quy định về bảo mật và quyền riêng tư, và phát triển các cơ chế bảo vệ người dùng trong trường hợp xảy ra sự cố.

5.1.4. Thách thức về xã hội và chấp nhận

5.1.4.1. Rào cản về nhận thức

Mặc dù công nghệ blockchain có tiềm năng lớn trong nhiều lĩnh vực, nhưng vẫn còn một số rào cản về nhận thức mà các tổ chức và người dùng cần phải vượt qua. Dưới đây là những vấn đề quan trọng liên quan đến nhận thức xã hội về blockchain:

1. **Thiếu hiểu biết về công nghệ blockchain**: Một trong những rào cản lớn nhất trong việc áp dụng blockchain là sự thiếu hiểu biết chung về công nghệ này. Rất nhiều người và doanh nghiệp vẫn chưa hiểu rõ về cách blockchain hoạt động, cũng như các ứng dụng tiềm năng của nó. Việc thiếu thông tin và sự giáo dục về blockchain khiến cho nhiều người không dám thử nghiệm hoặc đầu tư vào công nghệ này, mặc dù nó có thể mang lại nhiều lợi ích.
2. **Lo ngại về tính bảo mật và độ tin cậy**: Mặc dù blockchain có thể mang lại sự bảo mật cao, nhưng các lỗ hổng trong phần mềm, các cuộc tấn công mạng và việc sử dụng không đúng cách có thể làm dấy lên lo ngại về tính bảo mật. Cộng đồng vẫn còn lo

ngại về các vấn đề như gian lận, mất tiền, và các vụ hack đã xảy ra trước đây. Điều này gây ảnh hưởng đến lòng tin của người dùng vào blockchain, đặc biệt trong các ứng dụng như tiền điện tử và các hợp đồng thông minh.

3. **Thói quen sử dụng hệ thống truyền thống**: Người tiêu dùng và các tổ chức đã quen với các hệ thống tài chính truyền thống và các mô hình kinh doanh cũ. Việc chuyển sang các hệ thống phân quyền mới đòi hỏi thời gian và sự thay đổi trong tư duy. Việc thay đổi này không chỉ khó khăn về mặt kỹ thuật mà còn đụng phải các thói quen lâu dài trong việc sử dụng các dịch vụ tài chính, thanh toán, và quản lý dữ liệu.

5.1.4.2. Chi phí triển khai

Dù blockchain mang lại nhiều lợi ích, nhưng việc triển khai và áp dụng công nghệ này cũng đụng phải những vấn đề về chi phí, đặc biệt là đối với các doanh nghiệp vừa và nhỏ.

1. **Chi phí đầu tư ban đầu cao**: Để triển khai blockchain, các doanh nghiệp phải đối mặt với chi phí đầu tư ban đầu rất lớn. Điều này bao gồm việc xây dựng hạ tầng, tuyển dụng nhân lực chuyên môn, và phát triển các ứng dụng blockchain. Các chi phí này có thể khiến cho việc triển khai blockchain trở nên khó khăn đối với các doanh nghiệp có nguồn lực hạn chế.
2. **Thiếu nguồn nhân lực có chuyên môn**: Blockchain là một công nghệ mới, và việc tìm kiếm nhân lực có chuyên môn về blockchain hiện nay vẫn là một vấn đề lớn. Các kỹ sư blockchain và các chuyên gia trong lĩnh vực này rất hiếm và đắt đỏ, gây khó khăn cho các doanh nghiệp khi muốn triển khai các giải pháp blockchain. Bên cạnh đó, việc đào tạo nhân viên cũng đụng phải thách thức lớn vì kiến thức chuyên sâu về blockchain không được dạy phổ biến trong các trường đại học.
3. **Chi phí vận hành và bảo trì**: Sau khi triển khai, các doanh nghiệp còn phải đối mặt với chi phí vận hành và bảo trì. Các nền tảng blockchain yêu cầu bảo trì hệ thống, nâng cấp phần mềm, và giám sát bảo mật liên tục. Đặc biệt đối với các ứng dụng lớn, chi phí này có thể trở thành gánh nặng lâu dài.

5.2. Blockchain 3.0: Các Đột Phá Mới trong Công Nghệ Blockchain

Blockchain 3.0 đại diện cho sự tiến hóa của công nghệ blockchain, giải quyết những hạn chế và vấn đề tồn tại trong các phiên bản trước đó (Blockchain 1.0 và 2.0). Nó tập trung vào những yếu tố như hiệu suất, khả năng mở rộng, bảo mật, và đặc biệt là tính bền vững. Ba yếu

tố nổi bật trong Blockchain 3.0 là **Blockchain xanh**, **Zero-Knowledge Proof (ZKP)**, và **Layer 2 và Rollups**.

1. Blockchain Xanh

Một trong những vấn đề lớn của các nền tảng blockchain hiện tại là tiêu thụ năng lượng cao, đặc biệt là các mạng lưới sử dụng cơ chế đồng thuận Proof of Work (PoW), như Bitcoin. Trong khi Blockchain 2.0 (Ethereum) đang chuyển sang Proof of Stake (PoS) để giảm tiêu thụ năng lượng, Blockchain 3.0 tiếp tục tiến xa hơn với khái niệm **Blockchain xanh**.

- **Blockchain xanh** là những hệ thống blockchain được thiết kế để giảm thiểu tác động đến môi trường. Các nền tảng này sử dụng các cơ chế đồng thuận tiết kiệm năng lượng, như PoS, hoặc các công nghệ thay thế khác để giúp giảm lượng năng lượng cần thiết cho việc vận hành mạng lưới.
- Một ví dụ điển hình là **Algorand**, một nền tảng blockchain sử dụng PoS và cam kết duy trì một mức phát thải carbon cực thấp. Điều này giúp các blockchain xanh không chỉ có thể mở rộng và thực hiện các giao dịch nhanh chóng mà còn giảm thiểu tác động tiêu cực tới môi trường.
- **Cardano và Tezos** cũng là những ví dụ của các nền tảng chú trọng vào tính bền vững và hiệu quả năng lượng trong khi duy trì các tính năng bảo mật và khả năng mở rộng.

2. Zero-Knowledge Proof (ZKP)

Zero-Knowledge Proof (ZKP) là một trong những công nghệ quan trọng trong Blockchain 3.0 giúp nâng cao bảo mật và quyền riêng tư của người dùng mà không cần tiết lộ dữ liệu nhạy cảm. ZKP là một kỹ thuật trong đó một bên (người chứng minh) có thể chứng minh với một bên khác (người xác minh) rằng một tuyên bố là đúng mà không cần tiết lộ bất kỳ thông tin nào ngoài tính đúng đắn của tuyên bố đó.

Giả sử Peggy cần chứng minh với Victor rằng cô ấy đang sở hữu một bí mật mà không tiết lộ bí mật đó. Cô ấy có thể làm vậy một cách thuyết phục Victor rằng cô ấy thực sự biết bí mật đó không? Đây là câu hỏi nằm ở trung tâm của một trong những quy trình mật mã mạnh mẽ nhất mà chúng ta có thể sử dụng trong các hệ thống nhận dạng: bằng chứng không có kiến thức (ZKP). Giả sử ví dụ rằng Peggy có một giấy phép lái xe kỹ thuật số và muốn chứng minh với Victor, người phục vụ tại quầy bar, rằng cô ấy trên 21 tuổi mà không cần đưa giấy phép lái xe của mình hoặc thậm chí không cần cho anh ta xem ngày sinh của cô. ZKPs cho

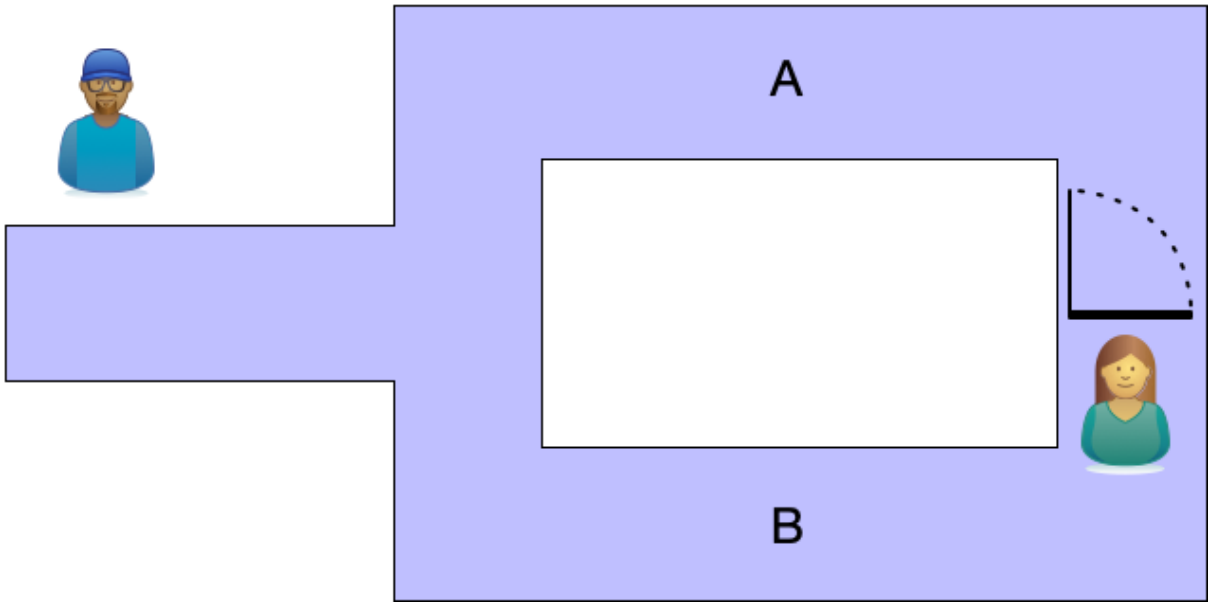
phép Peggy chứng minh rằng giấy phép lái xe của cô nói rằng cô ấy ít nhất 21 tuổi mà không cần tiết lộ bất kỳ thông tin nào khác (tức là không có kiến thức dư thừa).

Vấn đề này lần đầu tiên được các nhà nghiên cứu MIT Shafi Goldwasser, Silvio Micali và Charles Rackoff khám phá vào những năm 1980 như một cách để chống lại sự rò rỉ thông tin. Mục tiêu là giảm bớt lượng thông tin thừa mà người xác minh, Victor, có thể biết về người chứng minh, Peggy.

Một cách để hiểu cách thức hoạt động của ZKP là câu chuyện về Hang động Alibaba, lần đầu tiên được các nhà mật mã học Quisquater, Guillou và Berson công bố. Sơ đồ sau đây cung cấp một minh họa.

Peggy và Victor trong "Hang động Alibaba"

Hang động Alibaba có hai lối đi, được đánh dấu là A và B, chia ra từ một hành lang duy nhất nối với cửa ra vào. Peggy sở hữu một mã bí mật cho phép cô mở khóa một cánh cửa nối A và B. Victor muốn mua mã này nhưng sẽ không trả tiền cho đến khi anh ấy chắc chắn rằng Peggy biết mã này. Peggy sẽ không chia sẻ nó với Victor cho đến khi anh ấy trả tiền.



Thuật toán để Peggy chứng minh rằng cô ấy biết mã tiến hành như sau:

1. Victor đứng ngoài hang động trong khi Peggy vào và chọn một trong các lối đi. Victor không được phép nhìn thấy lối đi nào mà Peggy chọn.
2. Victor vào hang và gọi ra "A" hoặc "B" một cách ngẫu nhiên.
3. Peggy xuất hiện từ đúng lối đi vì cô có thể dễ dàng mở cửa dù chọn lối đi nào khi vào.

4. Tất nhiên, Peggy có thể chỉ đoán đúng và may mắn, vì vậy Peggy và Victor sẽ thử lại thí nghiệm nhiều lần.
5. Nếu Peggy luôn có thể trở lại từ lối đi mà Victor chọn, thì xác suất Peggy thực sự biết mã sẽ tăng dần. Sau 20 lần thử, có ít hơn một cơ hội trong triệu lần rằng Peggy chỉ đơn giản là đoán đúng chữ mà Victor sẽ gọi. Đây là một bằng chứng xác suất cho thấy Peggy biết bí mật.

Thuật toán này không chỉ cho phép Peggy thuyết phục Victor rằng cô ấy biết mã mà còn làm điều đó theo cách đảm bảo Victor không thể thuyết phục ai khác rằng Peggy biết mã. Giả sử Victor ghi lại toàn bộ giao dịch. Điều duy nhất mà người quan sát thấy là Victor gọi các chữ cái và Peggy xuất hiện từ đúng đường hầm. Người quan sát không thể chắc chắn rằng Victor và Peggy không đã thỏa thuận trước một chuỗi các chữ cái để lừa người quan sát. Lưu ý rằng tính chất này phụ thuộc vào việc thuật toán sử dụng một bộ sinh số giả ngẫu nhiên tốt với một hạt giống có độ ngẫu nhiên cao để Peggy và người quan sát thứ ba không thể dự đoán các lựa chọn của Victor.

Do đó, trong khi Peggy không thể từ chối với Victor rằng cô ấy biết bí mật, cô ấy có thể từ chối rằng cô ấy biết bí mật với những bên thứ ba khác. Điều này đảm bảo rằng bất cứ điều gì cô ấy chứng minh cho Victor sẽ chỉ giữa họ và Victor không thể tiết lộ nó - ít nhất là theo cách mật mã chứng minh rằng nó đến từ Peggy. Peggy giữ quyền kiểm soát cả bí mật của mình và việc cô ấy biết bí mật đó.

Khi chúng ta nói "không có kiến thức" và nói về việc Victor không học được gì ngoài tuyên bố đang được kiểm tra, điều đó không hoàn toàn chính xác. Trong hang động Alibaba, Peggy chứng minh trong không có kiến thức rằng cô ấy biết bí mật. Nhưng có rất nhiều điều khác mà Victor học về Peggy mà ZKP không thể làm gì được. Ví dụ, Victor biết rằng Peggy có thể nghe thấy anh ta, nói cùng ngôn ngữ, đi bộ, và hợp tác. Anh ta cũng có thể học được những điều về hang động, như mất bao lâu để mở cửa. Peggy học được những điều tương tự về Victor. Vì vậy, thực tế là bằng chứng là kiến thức gần như không có chứ không phải là hoàn toàn không có kiến thức.

Hệ thống ZKP

Ví dụ về Hang động Alibaba là một ứng dụng rất cụ thể của ZKPs, gọi là bằng chứng không có kiến thức về kiến thức (zero-knowledge proof of knowledge). Peggy đang chứng minh rằng cô ấy biết (hoặc sở hữu một thứ gì đó). Nói chung, Peggy có thể muốn chứng minh

nhiều sự thật với Victor. Những sự thật này có thể bao gồm các mệnh đề hoặc thậm chí các giá trị. ZKP có thể làm được điều này.

Để hiểu cách chúng ta có thể chứng minh các mệnh đề trong không có kiến thức, hãy xem một ví dụ khác, đôi khi được gọi là Vấn đề Triệu phú Xã hội chủ nghĩa. Giả sử Peggy và Victor muốn biết liệu họ có được trả lương công bằng không. Cụ thể, họ muốn biết liệu họ có được trả cùng một mức lương hay không, nhưng không muốn tiết lộ mức lương cụ thể của mình cho nhau hoặc thậm chí cho một bên thứ ba đáng tin cậy. Trong trường hợp này, Peggy không chứng minh cô ấy biết một bí mật, mà cô ấy chứng minh một mệnh đề về sự bình đẳng (hoặc không bình đẳng).

Để đơn giản, giả sử Peggy và Victor được trả một trong các mức lương $10, $20, $30 hoặc $40 mỗi giờ. Thuật toán hoạt động như sau:

1. Peggy mua bốn hộp khóa và gắn nhãn $10, $20, $30, và $40.
2. Cô ấy vứt đi chìa khóa của mọi hộp trừ hộp có nhãn mức lương của cô.
3. Peggy đưa tất cả các hộp khóa cho Victor, người sẽ bí mật bỏ một mẩu giấy có dấu "+" vào khe trên hộp có mức lương của anh ta. Anh ấy sẽ bỏ mẩu giấy có dấu "-" vào tất cả các hộp còn lại.
4. Victor trả lại các hộp cho Peggy, người sẽ sử dụng chìa khóa của mình để mở hộp có mức lương của cô.
5. Nếu cô tìm thấy dấu "+", điều đó có nghĩa là họ có mức lương giống nhau. Nếu không, họ có mức lương khác nhau. Cô ấy có thể sử dụng điều này để chứng minh sự thật cho Victor.

Đây được gọi là chuyển giao không biết và chứng minh mệnh đề "VictorSalary = PeggySalary" là đúng hay sai trong không có kiến thức (tức là, mà không tiết lộ bất kỳ thông tin nào khác).

Để điều này hoạt động, Peggy và Victor phải tin tưởng vào việc đối phương sẽ minh bạch và khai báo mức lương thật của mình. Victor cần tin rằng Peggy sẽ vứt đi ba chìa khóa còn lại. Peggy phải tin rằng Victor sẽ chỉ bỏ một mẩu giấy có dấu "+" vào các hộp.

Cũng giống như chứng chỉ kỹ thuật số cần có một hệ thống PKI để tạo dựng sự tin tưởng vượt ra ngoài những gì có thể có chỉ với chứng chỉ tự phát hành, ZKPs mạnh mẽ hơn trong một hệ thống cho phép Peggy và Victor chứng minh các sự thật từ những điều mà người khác nói về họ, không chỉ từ những gì họ nói về chính họ. Ví dụ, thay vì Peggy và Victor tự khẳng

định mức lương của họ, giả sử họ có thể dựa vào một tài liệu đã được ký từ phòng nhân sự để đưa ra khẳng định, để cả hai đều biết rằng người kia đang khai báo mức lương thật của mình. **Chứng chỉ có thể xác minh (Verifiable Credentials)** cung cấp một hệ thống để sử dụng ZKPs nhằm chứng minh nhiều sự thật khác nhau, riêng lẻ hoặc kết hợp, theo cách tạo ra sự tin tưởng vào phương pháp và niềm tin vào dữ liệu.

ZKP không tương tác (Non-Interactive ZKPs)

Trong các ví dụ trước, Peggy đã có thể chứng minh những điều cho Victor thông qua một loạt các tương tác. Để ZKP trở nên thực tế, các tương tác giữa người chứng minh và người xác minh nên được giảm thiểu tối đa. May mắn thay, một kỹ thuật gọi là SNARK cho phép chứng minh không có kiến thức không tương tác.

SNARKs có các đặc điểm sau (từ đó tên gọi của chúng được sinh ra):

- **Ngắn gọn**: kích thước của các thông điệp là nhỏ so với độ dài của chứng minh thực tế.
- **Không tương tác**: ngoài một số thiết lập ban đầu, người chứng minh chỉ gửi một thông điệp duy nhất tới người xác minh.
- **Lập luận**: đây thực sự là một lập luận cho rằng cái gì đó là đúng, không phải là một chứng minh như chúng ta hiểu về mặt toán học. Cụ thể, người chứng minh lý thuyết có thể chứng minh các phát biểu sai nếu có đủ sức mạnh tính toán. Vì vậy, SNARKs là "chắc chắn về mặt tính toán" thay vì "chắc chắn tuyệt đối".
- **Kiến thức**: người chứng minh biết sự thật đang được nói đến.

Thông thường, bạn sẽ thấy "zk" (từ viết tắt của zero-knowledge) được thêm vào phía trước để chỉ rằng trong quá trình này, người xác minh không học được gì ngoài các sự kiện được chứng minh.

Toán học cơ bản của zkSNARKs liên quan đến tính toán đồng hình trên các đa thức bậc cao. Tuy nhiên, chúng ta có thể hiểu cách thức hoạt động của zkSNARKs mà không cần biết toán học cơ sở đảm bảo rằng chúng là chắc chắn. Nếu bạn muốn tìm hiểu thêm chi tiết về toán học, tôi khuyên bạn nên tham khảo "zkSNARKs in a Nutshell" của Christian Reitwiessner.

Lấy một ví dụ đơn giản, giả sử Victor được cung cấp một giá trị băm sha256, H, của một giá trị nào đó. Peggy muốn chứng minh rằng cô ấy biết một giá trị s sao cho sha256(s) == H mà không tiết lộ s cho Victor. Chúng ta có thể định nghĩa một hàm C mô tả mối quan hệ này:

C(x, w) = (sha256(w) == x)

Vậy C(H, s) == true, trong khi các giá trị khác cho w sẽ trả về false.

Việc tính toán một zkSNARK yêu cầu ba hàm G, P và V. G là hàm tạo khóa nhận đầu vào một tham số bí mật gọi là lambda và hàm C, rồi tạo ra hai khóa công khai, khóa chứng minh pk và khóa xác minh vk. Chúng chỉ cần được tạo ra một lần cho một hàm C nhất định. Tham số lambda phải bị hủy sau bước này vì nó không còn cần thiết và bất kỳ ai có nó đều có thể tạo ra các chứng minh giả.

Hàm chứng minh P nhận đầu vào là khóa chứng minh pk, một giá trị công khai x, và một chứng cứ (bí mật) w. Kết quả của việc thực thi P(pk,x,w) là một chứng minh, prf, rằng người chứng minh biết giá trị w thỏa mãn C.

Hàm xác minh V tính toán V(vk, x, prf), và kết quả là true nếu chứng minh prf là đúng và false nếu không phải.

Trở lại với Peggy và Victor, Victor chọn một hàm C đại diện cho điều anh ta muốn Peggy chứng minh, tạo ra một số ngẫu nhiên lambda, và chạy G để tạo ra khóa chứng minh và khóa xác minh:

(pk, vk) = G(C, lambda)

Peggy không được phép biết giá trị của lambda. Victor chia sẻ C, pk và vk với Peggy.

Peggy muốn chứng minh cô ấy biết giá trị s thỏa mãn C cho x = H. Cô ấy chạy hàm chứng minh P sử dụng các giá trị này làm đầu vào:

prf = P(pk, H, s)

Peggy đưa chứng minh prf cho Victor, người chạy hàm xác minh:

V(vk, H, prf)

Nếu kết quả là true, Victor có thể yên tâm rằng Peggy biết giá trị s.

Hàm C không cần phải giới hạn chỉ là một băm như trong ví dụ này. Trong giới hạn của toán học cơ sở, C có thể rất phức tạp và liên quan đến bất kỳ số lượng giá trị nào mà Victor muốn Peggy chứng minh, tất cả trong một lần.

Ứng dụng ZKP trong blockchain giúp bảo vệ quyền riêng tư của người dùng, vì các thông tin giao dịch không cần phải công khai nhưng vẫn đảm bảo rằng giao dịch đó là hợp lệ. Điều

này có thể giúp giải quyết các vấn đề về bảo mật và quyền riêng tư trên các mạng lưới blockchain công khai như Ethereum.

- **Zcash** là một ví dụ về đồng tiền điện tử sử dụng ZKP. Nó cho phép người dùng thực hiện giao dịch mà không tiết lộ số tiền hoặc người nhận, qua đó bảo vệ quyền riêng tư của họ.
- **zk-SNARKs** (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) là một dạng cụ thể của ZKP, đã được áp dụng trên Ethereum để cải thiện khả năng bảo mật và tối ưu hiệu suất các hợp đồng thông minh.

3. Layer 2 và Rollups

Trong bối cảnh Blockchain 3.0, **Layer 2** và **Rollups** là các giải pháp nâng cao khả năng mở rộng và hiệu suất của các blockchain, đặc biệt là Ethereum, mà không làm giảm tính bảo mật hoặc phi tập trung.

Layer 2

Layer 2 (L2) là một giải pháp giúp cải thiện khả năng mở rộng và hiệu suất của các mạng blockchain mà không làm giảm tính bảo mật hoặc phi tập trung. Để hiểu rõ hơn về Layer 2, hãy tưởng tượng blockchain giống như một con đường giao thông, nơi tất cả các giao dịch đều phải di chuyển qua con đường chính (Layer 1). Nếu con đường này quá đông đúc, việc giao dịch sẽ rất chậm và tốn kém. Layer 2 giống như việc xây dựng thêm những con đường phụ, giúp các giao dịch có thể di chuyển nhanh hơn mà không làm tắc nghẽn con đường chính.

Cách thực Layer 2 hoạt động?

Layer 2 hoạt động bằng cách xử lý các giao dịch ngoài chuỗi chính (Layer 1) và chỉ gửi dữ liệu quan trọng hoặc kết quả của giao dịch đó vào blockchain chính. Việc này giúp giảm tải cho Layer 1, tăng tốc độ giao dịch và giảm chi phí giao dịch mà không cần phải ghi tất cả mọi giao dịch vào blockchain chính.

Có hai loại giải pháp Layer 2 phổ biến:

1. **State Channels**:
    - Là một kênh giao tiếp giữa hai bên (hoặc nhiều bên) mà các giao dịch diễn ra bên ngoài blockchain chính. Sau khi các giao dịch hoàn tất, kết quả cuối cùng được ghi vào blockchain chính.

- Ví dụ: Giả sử bạn và tôi muốn trao đổi tiền trong một khoảng thời gian dài. Thay vì mỗi lần trao đổi lại ghi vào blockchain (mất thời gian và chi phí), chúng ta có thể giao dịch ngoài chuỗi qua một state channel và chỉ ghi kết quả cuối cùng vào blockchain.

2. **Rollups**:
    - Rollups hoạt động bằng cách chuyển các giao dịch và tính toán ra ngoài blockchain chính (Layer 1), nhưng các kết quả này vẫn được xác minh và công nhận trên blockchain chính. Điều này giúp giảm thiểu sự tắc nghẽn và chi phí giao dịch của blockchain chính, đồng thời vẫn đảm bảo tính bảo mật và phi tập trung. Các giao dịch được thực hiện trên Layer 2 và sau đó "cuộn" lại thành một giao dịch duy nhất hoặc một nhóm giao dịch để ghi vào blockchain chính. Kết quả là chỉ có dữ liệu tổng hợp của các giao dịch mới được lưu trữ trên blockchain chính, không cần lưu trữ tất cả các giao dịch chi tiết. Có hai loại Rollups chính:
        - **Optimistic Rollups**: Giả định rằng các giao dịch là hợp lệ và không kiểm tra ngay lập tức, nhưng có thể yêu cầu chứng minh nếu có nghi ngờ về tính hợp lệ của giao dịch.
        - **zk-Rollups**: Sử dụng công nghệ Zero-Knowledge Proof (ZKP) để xác minh tính chính xác của các giao dịch mà không cần phải tiết lộ toàn bộ dữ liệu giao dịch, giúp tăng cường bảo mật và hiệu suất.

Lợi ích của Layer 2

- **Tăng tốc giao dịch**: Layer 2 giúp giao dịch diễn ra nhanh hơn vì nó giảm bớt sự tắc nghẽn trên blockchain chính.
- **Giảm chi phí**: Bằng cách xử lý các giao dịch ngoài chuỗi, chi phí giao dịch giảm đáng kể so với khi phải thực hiện tất cả trên blockchain chính.
- **Mở rộng quy mô**: Các giải pháp Layer 2 giúp blockchain có thể xử lý nhiều giao dịch hơn mà không gặp phải các vấn đề về tắc nghẽn hoặc chi phí cao.

Ví dụ về Layer 2

- **Lightning Network** trên Bitcoin là một ví dụ nổi bật về Layer 2. Nó cho phép người dùng thực hiện giao dịch nhanh chóng và rẻ hơn mà không cần phải ghi tất cả vào blockchain chính của Bitcoin.

- **Optimism và Arbitrum** trên Ethereum là hai giải pháp Layer 2 đang giúp Ethereum giải quyết vấn đề tắc nghẽn và chi phí giao dịch cao.

Layer 2 là một công nghệ quan trọng giúp blockchain có thể mở rộng và xử lý nhiều giao dịch hơn mà không làm giảm tính bảo mật hoặc phi tập trung. Các giải pháp như State Channels và Rollups sẽ giúp cải thiện hiệu suất của blockchain và giảm chi phí giao dịch, tạo ra một hệ sinh thái blockchain mạnh mẽ và hiệu quả hơn trong tương lai.

Như vậy, việc phát triển các giải pháp cho mạng lưới Blockchain thế hệ 3.0 và xa hơn nữa không chỉ đơn thuần là những cải tiến về công nghệ mà còn tập trung vào những yếu tố quan trọng như bảo mật, hiệu suất, khả năng mở rộng và tính bền vững. Những công nghệ mới như Blockchain xanh, Zero-Knowledge Proofs và Layer 2, Rollups là những yếu tố giúp blockchain giải quyết các vấn đề còn tồn tại trong các phiên bản trước đó, đồng thời mở ra nhiều cơ hội cho việc ứng dụng blockchain trong nhiều lĩnh vực khác nhau trong tương lai.

5.3. Tổng kết

Blockchain là một công nghệ đầy tiềm năng nhưng đang phải đối mặt với nhiều thách thức phức tạp. Việc giải quyết các thách thức này đòi hỏi sự nỗ lực của toàn bộ cộng đồng blockchain, từ các nhà phát triển, doanh nghiệp đến các cơ quan quản lý. Sự phát triển của công nghệ và các giải pháp mới đang dần giải quyết những thách thức này, mở ra triển vọng cho việc ứng dụng blockchain rộng rãi hơn trong tương lai.

Câu hỏi ôn tập

1. Phân tích các thách thức chính về khả năng mở rộng của blockchain và đề xuất giải pháp khắc phục.
2. Tại sao vấn đề tiêu thụ năng lượng lại là một thách thức lớn đối với blockchain? Các giải pháp nào đang được phát triển để giải quyết vấn đề này?
3. So sánh các thách thức về mặt kỹ thuật và thách thức về mặt quản trị trong việc triển khai blockchain.
4. Thảo luận về vai trò của khung pháp lý trong việc phát triển và ứng dụng công nghệ blockchain.
5. Đánh giá tác động của các thách thức xã hội đối với việc chấp nhận và áp dụng rộng rãi công nghệ blockchain.

Tài liệu tham khảo

1. Antonopoulos, A. M. (2017). Mastering Bitcoin: Programming the Open Blockchain
2. Zheng, Z., et al. (2018). Blockchain challenges and opportunities: A survey
3. Swan, M. (2015). Blockchain: Blueprint for a New Economy
4. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution
5. https://www.windley.com/archives/2021/11/zero_knowledge_proofs.shtml?form=MG0AV3