Giới thiệu Arbitrum

Phạm Quang Minh, 21020359@vnu.edu.vn

Giới thiệu về Cryptocurrency

Một cryptocurrency (tiền dựa trên mật mã học, hay còn biết đến ở Việt Nam với tên gọi "tiền điện tử" hoặc "tiền ảo"; viết ngắn gọn là crypto) là một phương tiện *số* cho trao đổi và giao dịch sử dụng *mật mã học mạnh* để đảm bảo an toàn cho các *giao dịch* tài chính, kiểm soát *quá trình tạo mới* các đơn vị tiền và *xác nhận* việc chuyển giao tài sản mà không phụ thuộc vào bất kỳ cơ quan trung ương nào, chẳng hạn như chính phủ hoặc ngân hàng, để duy trì nó.

Tổng quan của tiền dựa trên mật mã học:

- Các loại tiền dựa trên mật mã học được xây dựng trên một công nghệ gọi là Blockchain. Một blockchain là một sổ cái (ledger) phi tập trung chứa các giao dịch được thực hiện trên một mạng ngang hàng. Công nghệ này cho phép những người tham gia xác nhận giao dịch mà không cần đến một cơ quan tập trung; và cũng cung cấp một mức độ ẩn danh cho các bên tham gia giao dịch.
- Các loại tiền dựa trên mật mã học sử dụng các kỹ thuật mật mã học mạnh để đảm bảo an toàn cho các giao dịch và kiểm soát sự tạo mới các đơn vị tiền. Mật mã học làm cho nó an toàn và bảo vệ nó khỏi lừa đảo và giả mạo.
- Không giống như các loại tiền tệ truyền thống do ngân hàng trung ương phát hành, tiền dựa trên mật mã học là phi tập trung. Điều này có nghĩa là chúng không bị kiểm soát bởi bất kỳ chính phủ hoặc tổ chức tài chính nào.
- Các ví điện tử được sử dụng để lưu trữ, gửi và nhận tiền crypto. Nó có thể là một thiết bị, chương trình hoặc một dịch vụ.
- Khóa công khai và khóa bí mật: Khóa công khai là một giá trị mật mã cho phép người dùng nhận tiền crypto vào tài khoản của mình và cho phép những người dùng khác kiểm tra chữ ký số của mình. Khóa bí mật được sử dụng để ký các giao dịch, cung cấp bằng chứng toán học cho thấy chúng đến từ chủ sở hữu ví.
- Các nền kinh tế crypto: Tổng nguồn cung được lưu hành và giá hiện tại của token (đơn vị tiền) được sử dụng để tính vốn hóa thị trường của một cryptocurrency.
- White paper: Hầu hết các dự án tiền điện tử đều cung cấp white paper, giúp xác định mục tiêu và chi tiết kỹ thuật của tiền điện tử. White paper xác định rõ ràng các mục tiêu của dự án, công nghệ của họ sẽ đạt được các mục tiêu đó như thế nào và loại tiền đó sẽ hoạt động như thế nào.

Giới thiệu về Blockchain

Tổng quan về Blockchain được sử dụng trong một cryptocurrency:

1. Cấu trúc của blockchain: Một blockchain là một loại database được chia sẻ trong đó lưu dữ liệu theo các khối được liên kết với nhau sử dụng mật mã học. Nó là một cơ sở dữ liệu hoặc sổ cái (ledger) phân tán được chia sẻ giữa các nút của một mạng máy tính.

a. “Block” (khối) là dữ liệu được lưu thành các nhóm liền tiếp nhau thành một chuỗi. Khi bạn gửi tiền crypto đến ai đó, dữ liệu giao dịch cần được thêm vào một khối để giao dịch đó thành công.
b. “Chain” (chuỗi, xâu chuỗi, xích) ở đây đề cập đến việc mỗi block tham chiếu đến block trước nó sử dụng mật mã học. Nói cách khác, các block được xâu chuỗi lại với nhau. Dữ liệu trong một block không thể bị thay đổi nếu không thay đổi tất cả các khối tiếp theo, một thay đổi như vậy đòi hỏi sự đồng thuận của toàn bộ mạng.
c. Mỗi máy tính trong mạng cần phải đồng ý với nhau về từng khối mới và cả toàn bộ chuỗi. Những máy tính này được gọi là các node (nút). Các node đảm bảo mọi người tương tác với blockchain đều có cùng một dữ liệu. Để đạt được sự đồng nhất trên mạng phân tán này, blockchain cần có một cơ chế đồng thuận (consensus mechanisim). Hai cơ chế đồng thuận phổ biến được dùng bởi các loại tiền crypto là proof-of-work và proof-of-stake.

2. Lưu trữ và truy cập dữ liệu: Sự khác biệt chính giữa cơ sở dữ liệu hoặc bảng tính truyền thống và blockchain là cách dữ liệu được cấu trúc và truy cập. Blockchain bao gồm các chương trình máy tính phụ trách việc thực hiện tự động các tác vụ bạn thường làm trong cơ sở dữ liệu: Nhập và truy cập thông tin cũng như lưu và lưu trữ nó ở đâu đó.
3. Bản chất phân tán: Một blockchain được phân tán, có nghĩa là các bản sao được lưu trên nhiều máy và tất cả chúng phải khớp nhau để blockchain đó hợp lệ.
4. Tạo chuỗi: Blockchain thu thập thông tin giao dịch và nhập nó vào một block, giống như một ô trong bảng tính chứa thông tin. Một khi block đã đầy, thông tin được chạy qua một thuật toán mật mã học để tạo ra mã hash. Hash của block đó sau đó được đưa vào header của block tiếp theo và sẽ được đưa vào thuật toán mật mã học cùng với các thông tin khác của block tiếp theo đó để sinh mã hash cho block tiếp theo đó. Quá trình này tạo một chuỗi các block được xâu chuỗi (chained) lại với nhau.
5. Quá trình giao dịch: Các giao dịch tuân theo một quá trình cụ thể, dựa trên loại blockchain mà trên đó chúng được thực hiện.
    a. Ví dụ, trên blockchain của Bitcoin, khi bạn thực hiện một giao dịch sử dụng ví tiền crypto của bạn, giao dịch đó được gửi đến tất các các node. Một số node sẽ thực hiện việc cho giao dịch này vào sổ cái và được gọi là miner (máy đào “tiền ảo”). Các máy tính này đầu tiên sẽ xác minh tính hợp lệ của giao dịch (xác minh chữ ký trên giao dịch đó sử dụng khóa công khai của người trả). Một khi đã được xác nhận là hợp lệ, các giao dịch được nhóm lại thành các block, và các miner sẽ thực hiện proof-of-work: tăng dần một giá trị nonce cho đến khi nó kèm với các giá khác trong block tạo ra hash bắt đầu với một số lượng bit 0 được yêu cầu. Quá trình này tiếp tục cho đến khi một miner tính ra một giá trị hash hợp lệ, thắng cuộc đua và nhận phần thưởng. Block được tính ra sẽ được truyền ra khắp mạng để các máy trên mạng cập nhật blockchain của chúng, bằng cách được xâu chuỗi với block trước. Để chắc chắn block mới này là hợp lệ, block này sẽ không được coi là xác nhận cho đến khi năm khối khác sau nó được xác thực. Quá trình này mất khoảng một giờ để mạng hoàn thành vì trung bình mất dưới 10 phút cho mỗi khối. Các node luôn coi chuỗi dài nhất là chính xác và sẽ tiếp tục mở rộng nó. Nếu hai node phát đồng thời các phiên bản khác nhau của block tiếp theo, một số node có thể nhận được một trong hai block đó trước cái còn lại. Trong trường hợp đó, những node đó làm việc trên nhánh đầu tiên chúng nhận được, nhưng lưu nhánh còn lại trong trường hợp nó dài

hơn. Sau khi một số proof-of-work tiếp theo được tạo ra, và một nhánh trở nên dài hơn; các node đang làm việc trên nhánh còn lại sẽ chuyển sang nhánh dài hơn. Nếu một trong hai block là không hợp lệ, nhánh của block không hợp lệ, được thực hiện bởi một (số) bên độc hại, sẽ không theo kịp nhanh của block hợp lệ, được thực hiện bởi đa số các nút hợp lệ trong mạng.

   b. Không phải blockchain nào cũng tuân theo quy trình này. Ví dụ, mạng Ethereum (sẽ được giới thiệu tiếp theo) chọn ngẫu nhiên một *người xác thực (validator)* từ một người dùng bất kỳ đã cọc trước (stake) Ether, sau đó được xác nhận bởi mạng. Quá trình này nhanh hơn và tốn ít năng lượng hơn quá trình của Bitcoin.

6. Tính phi tập trung: Một blockchain cho phép dữ liệu trong cơ sở dữ liệu được tỏa ra giữa nhiều node trong mạng ở các địa điểm khác nhau. Do đó không riêng một người hay một nhóm nào có quyền kiểm soát tuyệt đối, thay vào đó, tất cả người dùng kết hợp lại mới giữ quyền kiểm soát. Điều này cũng đảm bảo tính nhất quán của dữ liệu. Nếu ai đó muốn thay đổi một bản ghi của dữ liệu ở một node hoặc một vài node, số đông các node còn lại sẽ giữ nguyên bản ghi đúng và ngăn điều đó xảy ra. Tính phi tập trung cũng làm cho dữ liệu trong blockchain là bất biến, tức là, dữ liệu đã được đưa vào thì không thể đảo ngược được.
7. Tính minh bạch (transparency): Nhờ bản chất phi tập trung của blockchain, tất cả các giao dịch có thể được xem một cách minh bạch qua một node mà một người sở hữu hoặc thông qua các blockchain explorer cho phép bất kỳ ai có thể xem các giao dịch diễn ra trực tiếp. Mỗi node có một bản sao của blockchain mà được cập nhật khi các block mới được xác nhận và thêm vào chuỗi. Điều này nghĩa là, nếu bạn muốn, bạn có thể theo dõi lịch sử giao dịch của một đơn vị tiền crypto (xem nó đã từng đến tay những ai…).
8. Tính ẩn danh (anonymity): Blockchain không lưu lại thông tin chủ nhân của một ví. Do đó, mặc dù mọi giao dịch trong blockchain hiển thị địa chỉ ví của mỗi bên tham gia vào giao dịch, các chủ nhân của các ví đó là ẩn danh.
9. Đào tiền (Mining): Khi một node thực hiện thành công việc xác minh và xử lý một giao dịch để thêm nó vào blockchain, node đó sẽ được thưởng crypto cho các tài nguyên tính toán node đó đã bỏ ra trong toàn bộ quá trình tạo block.
10. An ninh: Công nghệ blockchain đạt được an ninh theo một số cách.
    a. Thứ nhất các block được lưu trữ tuyến tính và theo trình tự thời gian. Các block mới luôn được thêm vào cuối blockchain. Sau khi một block đã được thêm vào blockchain, các block trước đó không thể bị thay đổi. Bất kỳ thay đổi nào trong dữ liệu của một block đều dẫn đến thay đổi trong hash của block đó. Vì mỗi block đều chữa hash của block trước nó, thay đổi trong một block sẽ yêu cầu thay đổi cả chuỗi block đằng sau nó. Mạng sẽ từ chối một block đơn lẻ bị thay đổi vì các mã hash sẽ không trùng khớp nhau.
    b. Blockchain sử dụng các kỹ thuật mật mã để ngăn chặn tấn công can thiệp.
        i. Sử dụng hàm hash mật mã học (như SHA256). Các hàm hash như vậy có tính một chiều, tức là có thể dễ dàng tính giá trị hash của một khối nhưng từ một giá trị hash rất khó để tìm ra được một khối thỏa mãn hash đó. Vì vậy, chi phí tính toán bỏ ra để tạo ra một block giả và tương ứng là một blockchain giả là rất lớn.
        ii. Sử dụng mô hình chữ ký điện tử (như ECDSA) để xác thực giao dịch. Nếu một giao dịch bị thay đổi, chữ kỹ điện tử sẽ không còn hợp lệ và mạng sẽ phát hiện ra ngay.

c. Cơ chế đồng thuận: Tất cả giao dịch trong một block được xác thực và chấp thuận thống nhất bởi một cơ chế đồng thuận, đảm bảo mỗi giao dịch được thêm vào blockchain là đúng và chính xác.
d. Blockchain là phi tập trung và được phân tán trên một mạng ngang hàng mà liên tục được cập nhật và giữ đồng bộ. Vì blockchain không được xử lý và lưu trữ ở một nơi tập trung, blockchain không có một single-point-of-failure và không thể bị thay đổi từ chỉ một máy tính. Nếu một kẻ tấn công muốn thay đổi một blockchain, người đó sẽ cần phải kiểm soát phần đa số mạng. Đây được biết tới là tấn công 51% vì cần chiếm hơn 50% mạng để thực hiện nó. Thời gian sẽ là yếu tố quan trọng trong kiểu tấn công này—vào thời điểm tin tặc thực hiện bất kỳ hành động nào, mạng có thể đã vượt qua các khối mà chúng đang cố gắng thay đổi. Điều này là do tốc độ băm của các mạng này cực kỳ nhanh—ví dụ, mạng Bitcoin được băm ở mức 348,1 exahash mỗi giây (18 chữ số 0) vào ngày 21/4/23.

Giới thiệu về Ethereum

Ethereum Logo by Unknown Author is licensed under CC BY-ND

Ethereum là một mạng các máy tính trên thế giới tuân theo một tập các quy tắc gọi là giao thức Ethereum. Mạng Ethereum đóng vai trò là *nền tảng* cho các cộng đồng, ứng dụng, tổ chức và tài sản số mà bất kỳ ai cũng có thể xây dựng và sử dụng. Đây là một số khía cạnh chính của Ethereum:

1. Blockchain: Ethereum là một blockchain với một máy tính được nhúng vào trong đó. Nó là nền tảng cho việc xây dựng các ứng dụng và tổ chức theo một cách phi tập trung, không cần cấp phép (permissionless) và chống kiểm duyệt. Trong vũ trụ Ethereum, có một máy tính chuẩn duy nhất (được gọi là Máy Ảo Ethereum hoặc EVM) mà trạng thái của nó được mọi người trên mạng Ethereum đồng ý. Mọi người tham gia vào mạng Ethereum (tất cả các nút Ethereum) đều giữ

một bản sao của trạng thái của máy tính này. Ngoài ra, bất kỳ thành viên nào cũng có thể phát một yêu cầu cho máy tính này thực hiện một tính toán nào đấy. Bất cứ khi nào một yêu cầu như vậy được phát đi, các thành viên khác trong mạng sẽ chấp nhận, xác thực và thực thi tính toán đó. Việc thực thi này thay đổi trạng thái của EVM, thay đổi này sau đó được áp dụng (commit) và truyền bá trên toàn bộ mạng. Các yêu cầu tính toán như vậy được gọi là các yêu cầu giao dịch; bản ghi của tất cả giao dịch và trạng thái hiện tại của EVM được lưu trữ trên blockchain, blockchain này được lưu trữ và đồng ý bởi tất cả các node.

2. Cơ chế đồng thuận: Ethereum sử dụng cơ chế đồng thuận dựa trên proof-of-stake. Bất kỳ ai muốn thêm các block mới vào chuỗi đều phải đặt cược Ether – tiền native trong Ethereum – làm thế chấp và chạy phần mềm xác thực. Những người này được gọi là người xác thực ("validator"), và được chọn ngẫu nhiên để đề xuất các khối mới mà sau đó được kiểm tra và thêm vào blockchain bởi các validator khác. Có một hệ thống thưởng và phạt mà khuyến khích mạnh mẽ những người tham gia phải trung thực và trực tuyến nhiều nhất có thể.
3. Phi tập trung: Không chính phủ hay công ty nào có quyền kiểm soát hoàn toàn Ethereum. Tính phi tập trung khiến gần như không ai có thể ngăn cản một người khác nhận một thanh toán hoặc sử dụng dịch vụ trên Ethereum.
4. Ether (ETH) là tiền crypto native của Ethereum. Mục đích của ETH là cho phép tạo ra một thị trường cho các tính toán. Một thị trường như vậy mang lại động lực kinh tế cho những người tham gia xác minh và thực thi các yêu cầu giao dịch cũng như cung cấp tài nguyên tính toán cho mạng.
    a. Bất kỳ thành viên nào mà gửi yêu cầu giao dịch cũng phải cung cấp một lượng ETH cho mạng dưới dạng tiền thưởng. Mạng sẽ trao phần thưởng này cho người mà cuối cùng sẽ làm công việc xác minh giao dịch, thực thi nó, đưa (commit) nó vào blockchain và phát block mới lên mạng.
    b. Lượng ETH được trả tỷ lệ với lượng tài nguyên cần thiết để thực hiện tính toán. Những tiền thưởng này cũng ngăn chặn những thành viên độc hại cố tình làm tắc nghẽn mạng bằng cách yêu cầu thực thi một lượng tính toán vô hạn hoặc thực thi các chương trình tiêu tốn tài nguyên khác, vì những thành viên này phải trả tiền cho tài nguyên tính toán cần sử dụng.
    c. ETH cũng được sử dụng để cung cấp an ninh cho mạng dựa trên nền kinh tế crypto trong 3 cách chính:
        i. Nó được sử dụng như một phương tiện để thưởng cho những người xác thực (validator) thực hiện một cách hợp lệ công việc đề xuất block của mình, hoặc để chỉ ra những hành vi không trung thực bởi các người xác thực khác.
        ii. Nó được dùng để cọc (stake) bởi những người xác thực, đóng vai trò là tài sản thế chấp chống lại hành vi không trung thực—nếu người xác thực làm sai thì ETH của họ có thể bị phá hủy.
        iii. Nó được dùng để cân nhắc các "phiếu bầu" cho các khối mới được đề xuất, khi các khối này được đưa vào quá trình lựa chọn của cơ chế đồng thuận.
5. Hợp đồng thông minh (smart contracts): Trong thực tế, các thành viên không viết code mới mỗi khi họ muốn yêu cầu một tính toán trên EVM. Thay vào đó, các nhà phát triển ứng dụng tải lên các chương trình máy tính vào trạng thái EVM, và người dùng tạo các yêu cầu thực thi những đoạn code với các tham số khác nhau. Những chương trình như vậy được gọi là các hợp đồng thông minh (smart contracts).

a. Bất kỳ nhà phát triển nào cũng có thể tạo ra một hợp đồng thông minh và công khai nó trên mạng, sử dụng blockchain làm lớp dữ liệu (data layer), với một khoản phí trả cho mạng. Sau đó, bất kỳ người dùng nào cũng có thể gọi hợp đồng thông minh đó để thực thi code của nó, cũng với một khoản phí nào đó được trả cho mạng.
b. Do đó, với hợp đồng thông minh, các nhà phát triển có thể xây dựng và triển khai các app và dịch vụ ở các độ phức tạp đa dạng như: marketplace, công cụ tài chính, games,…

Giới thiệu về Arbitrum

Arbitrum Logo by Unknown Author is licensed under CC BY

Khi số lượng người sử dụng Ethereum tăng lên, blockchain Ethereum đã đạt một số ngưỡng giới hạn về dung lượng nhất định. Điều này đã đẩy chi phí sử dụng mạng lên cao, tạo ra nhu cầu về các giải pháp mở rộng quy mô (scaling solutions). Có nhiều giải pháp đang được nghiên cứu, thử nghiệm và triển khai với các cách tiếp cận khác nhau để đạt các mục tiêu tương tự.

Mục đích chính của mở rộng quy mô là tăng tốc độ giao dịch (hoàn thành xử lý giao dịch nhanh hơn) và thông lượng giao dịch (nhiều giao dịch mỗi giây hơn), mà không phải hy sinh tính phi tập trung hoặc an ninh. Trên blockchain Ethereum, nhu cầu cao dẫn đến giao dịch chậm hơn và chi phí giao dịch quá cao. Do đó, tăng dung lượng mạng về mặt tốc độ và thông lượng là nền tảng cho việc thúc đẩy có ý nghĩa mọi người sử dụng Ethereum.

Arbitrum là một bộ công nghệ được thiết kế để mở rộng quy mô Ethereum. Nó là một bộ các giải pháp mở rộng quy mô Ethereum theo mô hình Layer-2 cho phép mọi người sử dụng để xây dựng các ứng dụng phi tập trung (decentrialized apps – dApps). Người dùng có thể sử dụng các chuỗi (chain) Arbitrum để làm mọi thứ có thể làm được trên Ethereum – sử dụng các ứng dụng Web3, triển khai các hợp đồng thông minh,… và các giao dịch sẽ được thực hiện nhanh và rẻ hơn. Sản phẩm chủ lực của họ là Arbitrum Rollup, một giao thức Rollup Optimistic mà kế thừa các cơ chế an ninh của Ethereum.

Tại sao Ethereum cần được mở rộng quy mô?

Ethereum là một nền tảng rất tốt. Tuy nhiên, nếu chỉ sử dụng riêng nó thôi thì cũng rất gặp nhiều hạn chế. Blockchain Ethereum chỉ cho phép khoảng 20-40 giao dịch mỗi dây (transactions per second – TPS) (đấy là đã tính tổng cộng, cho tất cả người người dùng Ethereum). Khi đạt đến giới hạn đó, các người dùng buộc phải cạnh tranh với nhau để giao dịch của họ được thêm vào, điều này khiến phí giao dịch tăng lên.

Tại sao Ethereum có TPS thấp như vậy?

Đây là một quyết định có chủ ý trong thiết kế của Ethereum. Ethereum yêu cầu các node của nó (máy tính chạy phần mềm Ethereum) phải có một cách đạt được sự đồng thuận về trạng thái hiện tại của blockchain. Cách họ làm điều này là xử lý tất cả các giao dịch trong lịch sử của Ethereum.

Một trong những nguyên tắc của cộng đồng Ethereum, khi muốn xây dựng Ethereum là một hệ thống mở, phi tập trung và ngang hàng, là cho phép ở một mức độ hợp lý bất kỳ ai cũng có thể chạy một node Ethereum và xác thực blockchain cho chính họ; tức là, nếu việc này trở nên quá đắt (về mặt yêu cầu phần cứng/tài nguyên tính toán) thì điều này sẽ gây ảnh hưởng xấu đến mục tiêu nền tảng của tính phi tập trung. Sự kết hợp của hai yếu tố này – mọi nút phải xử lý mọi giao dịch và chúng ta muốn việc chạy một nút là tương đối khả thi – dẫn tới thông lượng (throughput) giao dịch phải bị giới hạn ở mức khá thấp.

Optimistic Rollup

Khi nói đến mở rộng quy mô của Ethereum (hay các blockchain khác), người ta hay sử dụng thuật ngữ layer 1. Layer 1 (lớp 1, viết tắt là L1) được dùng để chỉ chính giao thức cơ sở và blockchain nền tảng mà ta muốn mở rộng quy mô, trong trường hợp này là mạng chính Ethereum.

Khái niêm mở rộng quy mô có thể phân ra làm hai loại: mở rộng trên chuỗi (on-chain) hay ngoài chuỗi (off-chain). Mở rộng quy mô trên chuỗi là tạo ra những thay đổi ngay trên mạng chính layer 1 (giao thức Ethereum). Mặt khác, các giải pháp mở rộng ngoài chuỗi được triển khai tách biệt khỏi mạng chính layer 1 – tức không yêu cầu tạo ra thay đổi trên giao thức Ethereum hiện thời. Trong số các giải pháp mở rộng ngoài chuỗi, có một nhóm cái giải pháp kế thừa an ninh trực tiếp từ quá trình đồng thuận trên layer 1 Ethereum, và được biết đến là các giải pháp “layer 2”.

Layer 2 là một thuật ngữ chung cho những giải pháp được thiết kế để giúp mở rộng quy mô bằng cách xử lý các giao dịch ở bên ngoài mạng chính layer 1, trong khi tận dụng mô hình an ninh phi tập trung mạnh mẽ của mạng chính. Hầu hết các giải pháp lớp 2 tập trung xung quanh một số server, mỗi server có thể được gọi là node, validator, operator, sequencer, block producer hay thuật ngữ tương tự. Nói chung, các giao dịch được gửi đến các node này ở layer 2 thay vì được gửi trực tiếp đến layer 1. Trong nhiều giải pháp, layer 2 sau đó nhóm các giao dịch thành các lô (batch) trước khi chuyển chúng vào layer 1, sau đó các giao dịch này được bảo vệ an ninh bởi layer 1 và không thể bị thay đổi.

Rollup (tổng hợp) là một loại giải pháp layer 2, trong đó các giao dịch được thực hiện bên ngoài lớp 1, sau đó dữ liệu được gửi cho lớp 1 khi đạt được đồng thuận. Có hai loại rollup với hai mô hình an ninh khác nhau:

- Optimistic rollup (tổng hợp lạc quan): theo mặc định sẽ giả định các giao dịch là hợp lệ và chỉ chạy các tính toán, thông qua một chứng minh gian lận (fraud proof), trong trường hợp xảy ra tranh cãi.

- Zero-knowledge rollup: chạy các tính toán ngoài chuỗi và gửi một chứng minh hợp lệ (validity proof) lên chuỗi.

Trong Optimistic rollup, các giao dịch được thực thi bên ngoài Ethereum, rồi sau đó được nhóm lại thành các lô lớn trước khi gửi tới Ethereum. Cách tiếp cận này cho phép phân bổ một chi phí cố định cho nhiều giao dịch trong mỗi đợt, từ đó giảm chi phí cho người dùng cuối. Optimistic rollup cũng sử dụng các kỹ thuật nén để giảm lượng dữ liệu được đưa lên Ethereum.

Được gọi là "lạc quan" (optimistic) như vậy là bởi Optimistic rollup giả định các giao dịch là hợp lệ và không tạo ra các chứng minh hợp lệ cho các lô giao dịch được gửi lên chuỗi chính. Đây là điểm khác biệt giữa Optimistic rollup và Zero-knowledge (ZK) rollup; ở ZK rollup, các giao dịch được gửi lên chuỗi chính kèm theo chứng minh hợp lệ mật mã học.

Optimistic rollup, thay vào đó, dựa trên một mô hình chứng minh gian lận (fraud-proving scheme) để phát hiện các trường hợp các giao dịch được tính toán không chính xác. Sau khi một lô rollup được gửi lên Ethereum, có một khoảng thời gian (được gọi là giai đoạn thử thách/thẩm tra – challenge period) trong đó bất kỳ ai cũng có thể thách thức kết quả của một giao dịch trong rollup bằng cách tính ra một chứng minh gian lận (fraud proof).

Nếu chứng minh gian lận thành công, giao thức rollup thực thi lại các giao dịch và cập nhật trạng thái của rollup tương ứng. Một tác động khác của một chứng minh gian lận thành công là sequencer (nút sắp xếp thứ tự các giao dịch để cho vào lô rollup) chịu trách nhiệm cho việc thêm giao dịch không hợp lệ đó sẽ nhận một khoản phạt.

Nếu một lô rollup không bị thách thức (tức là tất cả các giao dịch đều được thực thi chính xác) sau khi hết giai đoạn thử thách, nó được coi là hợp lệ và được chấp nhận trên Ethereum. Cũng có thể xây dựng trên một khối rollup chưa được xác nhận (chưa hoàn thành giai đoạn thử thách) nhưng với một lưu ý: các kết quả giao dịch sẽ bị đảo ngược nếu dựa trên một giao dịch không hợp lệ được đưa lên trước đó.

Arbitrum Rollup hoạt động như nào?

Ý tưởng cơ bản là: một chuỗi Arbitrum Rollup chạy như một mô đun con bên trong Ethereum. Không giống như các giao dịch Ethereum ở Layer 1 thông thường, nút Ethereum không phải xử lý mọi giao dịch Arbitrium. Thay vào đó, Ethereum sử dụng một thái độ "vô tội cho đến khi được chứng minh là có tội" đối với Arbitrum. Layer 1 ban đầu "giả định một cách lạc quan" rằng hoạt động trên Arbitrum đang tuân theo đúng các quy tắc. Nếu xảy ra vi phạm (ví dụ ai đó khẳng định "bây giờ tôi sở hữu tiền của tất cả mọi người"), khẳng định này có thể đưa lên L1 giải quyết tranh chấp; gian lận sẽ được chứng minh, khẳng định không hợp lệ sẽ bị bỏ qua, và bên có ác ý sẽ bị phạt tài chính.

Khả năng xét xử và chứng minh gian lận trên L1 là tính năng nền tảng, then chốt của Arbitrum, và đó là cách và lý do hệ thống kế thừa cơ chế an ninh của Ethereum.

Dữ liệu giao dịch được đưa vào chuỗi Arbitrum Rollup sẽ được đăng trực tiếp lên Ethereum. Do đó, bất kỳ ai quan tâm đều có thể nhìn thấy những gì đang diễn ra trong Arbitrum và có khả năng phát hiện và chứng minh gian lận.

Ai là người thực hiện công việc kiểm tra gian lận?

Các bên mà chuyển tiếp trạng thái chuỗi Arbitrum lên L1 – tức là, thực hiện việc đưa ra khẳng định về trạng thái của chuỗi, tranh cãi với các khẳng định khác,… – được gọi là validator (người xác thực). Trong

thực tế, những người dùng trung bình không được kỳ vọng phải quan tâm đến việc chạy một validator, cũng như việc những người dùng Ethereum trung bình cũng không phải chạy các nút validator của riêng họ ở Layer 1. Tuy nhiên, đặc tính quan trọng là bất kỳ ai cũng có thể làm điều đó: trở thành một validator cho Arbitrum không yêu cầu phải có sự cho phép đặc biệt nào (hiện tại đang trong quá trình phát triển thì có một danh sách những người được cho phép, nhưng sau này sẽ mở rộng cho phép tất mọi người), chỉ cần người dùng chạy phần mềm validator như ở trong mã nguồn mở (và đặt cược Ether khi họ cần thực hiện các công việc của validator).

Ngoài ra, chừng nào mà chỉ cần có ít nhất một validator trung thực, cả chuỗi Arbitrum sẽ vẫn an toàn; tức là, để bắt quả tang bất kỳ số lượng kẻ gây rối độc hại nào cũng chỉ cần đúng một người kiểm tra gian lận trung thực. Những thuộc tính này cùng nhau làm cho hệ thống trở nên "trustless" (không yêu cầu sự tin cậy vào một cơ quan tập trung): người dùng không cần phải phụ thuộc vào bất kỳ bên cụ thể nào để đảm bảo an toàn cho tiền của họ.

Cụ thể hơn, mỗi người xác thực (validator) có thể chọn cách tiếp cận của riêng họ, những ba chiến lược thông thường được kỳ vọng là:

- Chiến lược validator *chủ động* (active): trực tiếp phát triển trạng thái của chuỗi bằng cách đề xuất các khối rollup mới. Một validator chủ động luôn phải đặt cọc (stake), vì việc tạo một khối rollup yêu cầu đặt cọc. Một chuỗi chỉ cần một validator chủ động trung thực là đã có thể hoạt động bình thường; có nhiều hơn một là không cần thiết và là một cách sử dụng tài nguyên không hiệu quả.
- Chiến lược validator *phòng thủ* (defensive): theo dõi hoạt động của giao thức rollup. Nếu chỉ có các khối rollup hợp lệ được đề xuất, chiến lược này không làm gì cả. Nhưng nếu xuất hiện một khối không hợp lệ được đề xuất, chiến lược này can thiệp bằng cách đăng lên một khối hợp lệ hoặc đặt cọc vào một khối hợp lệ đã được đăng bởi một bên khác. Chiến lược này tránh việc phải đặt cược khi mọi thứ đang diễn ra suôn sẻ, nhưng nếu có ai đó thực hiện gian lận, chiến lược này sẽ đặt cọc để bảo vệ kết quả chính xác.
- Chiến lược validator *tháp canh* (watchtower): không cần đặt cọc. Chiến lược này chỉ đơn giản là theo dõi giao thức rollup và nếu một khối không hợp lệ được đề xuất, nó sẽ đưa ra cảnh báo (bằng bất kỳ phương tiện nào nó chọn) để người khác có thể can thiệp. Chiến lược này giả định rằng các bên khác mà sẵn lòng đặt cọc thì cũng sẽ sẵn sàng can thiệp để lấy một phần trong số tiền được đặt cọc bởi người đưa ra đề xuất không trung thực, và việc này có thể được thực hiện trước khi hết gian đoạn thử thách của khối không trung thực. (Trong thực tế, các bên này được cho phép vài ngày để đưa ra thách thức).

Thông thường chỉ có một validator chủ động ở một thời điểm. Không có gì ngăn cản việc có nhiều validator chủ động, và giao thức vẫn hoạt động bình thường trong trường hợp đó. Nhưng chỉ cần có một validator chủ động có hành vi tốt, thì những validator khác mà sẵn lòng làm validator chủ động có thể tránh việc đặt cọc bằng cách đi theo chiến lược phòng thủ. Chừng nào validator chủ động đó vẫn còn đăng các block hợp lệ, mọi người khác có thể giảm thiểu chi phí từ việc đặt cọc nhưng vẫn giữ an toàn bằng cách duy trì chiến lược phòng thủ. Nếu validator chủ động đó thực hiện gian lận, các validator phòng thủ sẽ chứng minh gian lận và validator chủ động sẽ mất tiền cọc. Sau đó, bất kỳ ai cũng có thể chuyển sang chiến lược chủ động và bắt đầu xác thực cho khối chính xác.

Trong điều kiện bình thường, những validator sử dụng chiến lược phòng thủ và tháp canh sẽ không làm gì ngoại trừ việc xem xét chuỗi và thực hiện ngầm việc kiểm tra (không thông báo cho người khác biết mình đang làm vậy) liệu mỗi block rollup được đề xuất có hợp lệ không. Một tác nhân độc hại đang cân nhắc có nên thử gian lận hay không sẽ không thể biết được có bao nhiêu validator phòng thủ và tháp canh đang hoạt động ngầm như vậy. Có thể có một vài validator phòng thủ có công khai chiến lược của mình, nhưng những validator còn lại thì không làm vậy. Vì vậy, kẻ tấn công sẽ luôn phải lo lắng rằng những validator phòng thủ đang thực hiện kiểm tra ngầm và sẽ "nổi lên" và đưa ra thách thức khi gặp khối không hợp lệ.

Những ai sẽ làm validator? Trong thực tế, mọi người sẽ muốn làm validator cho một số lý do như sau:

- Một số validator sẽ được trả tiền, bởi bên tạo ra chuỗi hoặc ai đấy khác. Trong trường hợp của Arbitrum, nhóm phát triển của Arbitrum có một danh sách các validator ban đầu cho Arbitrum One hoặc Nova và được trả tiền như vậy.
- Các bên có một lượng tài sản đáng kể trong một chuỗi, như các nhà phát triển dApp (ứng dụng phi tập trung), các sàn giao dịch… có thể chọn thực hiện công việc của validator để bảo vệ khoản đầu tư của họ.
- Bất kỳ ai khác muốn thì đều có thể làm được. Có thể một vài người dùng muốn thực hiện xác thực để bảo vệ tài sản của họ hoặc họ muốn làm công dân tốt. Nhưng những người dùng thông thường, như đã nói, không cần và không được mong đợi phải làm vậy.

Gian lận được chứng minh như nào?

Về bản chất: nếu hai validator bất đồng ý kiến thì chỉ (nhiều nhất) một trong số họ là đang nói sự thật. Trong một tranh chấp như vậy, hai validator sẽ thực hiện một "trò chơi" tương tác, gọi và phản hồi, trong đó họ thu hẹp tranh chấp của mình thành một bước tính toán duy nhất. Bước này được thực hiện trên L1 và sẽ chắc chắn chứng mình được rằng bên trung thực đang nói sự thật.

Trong số các giao thức optimistic rollup, quyết định thiết kế quan trọng nhất là cách giải quyết tranh cãi. Giả sử Alice khẳng định rằng chuỗi sẽ tạo ra một kết quả nhất định và Bob không đồng ý. Giao thức cần quyết định chấp nhận khẳng định nào.

Có hai lựa chọn cơ bản: interactive proving (chứng minh tương tác) và re-executing transations (thực thi lại các giao dịch). Arbitrum sử dụng chứng minh tương tác. Cách thiết kế này đang thể hiện là một cách hiệu quả và linh động hơn so với thực thi lại các giao dịch.

Ý tưởng chính của chứng minh tương tác là Alice và Bob sẽ tham gia vào một giao thức trao đổi qua lại, với một hợp đồng L1 đứng ra ở giữa làm trọng tài, để giải quyết tranh cãi sao cho sử dụng L1 một cách tối thiểu.

Phương pháp của Arbitrum là dựa trên chia nhỏ tranh cãi. Nếu khẳng định của Alice chiếm N bước thực thi, khẳng định đó được chia nhỏ thành 2 khẳng định kích cỡ N/2. Sau đó, Bob chọn một trong hai khẳng định kích cỡ N/2 bước đó để thách thức. Khi đó, kích cỡ của khẳng định cần thử thách đã giảm đi còn một nữa. Quá trình này tiếp tục, chia đôi tranh cãi ở mỗi giai đoạn, cho đến khi chỉ còn đúng một bước thực thi. Lưu ý rằng cho đến đây, trọng tài L1 vẫn chưa phải thực thi gì cả. Chỉ đến khi tranh cãi được thu nhỏ xuống chỉ còn một bước thì trọng tài L1 mới cần phải giải quyết tranh cãi đó bằng việc xem xét bước thực thi đó thực sự đưa ra kết quả gì và liệu tuyên bố của Alice về kết quả đó có đúng không.

Nguyên tắc chính đằng sau chứng minh tương tác là nếu Alice và Bob đang tranh cãi, Alice và Bob nên thực hiện các công việc giải quyết ở bên ngoài chuỗi chính (off-chain) nhiều nhất có thể, thay vì thực hiện công việc đó trên chuỗi chính L1. Chính nhờ vậy nên phương pháp này mới đạt được hiệu suất cao hơn so với phương pháp còn lại.

Chứng minh tranh chấp này rõ ràng phải mất một khoảng thời gian; điều này có gây ra bất kỳ sự chậm trễ nào đối với các giao dịch của người dùng Arbitrum không?

Sự chậm trễ duy nhất mà một người dùng cảm nhận được là khi họ "rút tiền" – chuyển tiền của họ từ Arbitrum trở lại Ethereum. Nếu người dùng rút tiền trực tiếp từ Arbitrum sang Ethereum, họ điển hình là phải đợi 1 tuần trước khi nhận được tiền trên L1. Tuy nhiên, nếu người dùng sử dụng một ứng dụng cầu nối nhanh (fast-bridge), họ có thể bỏ qua hoàn toàn khoảng thời gian trì hoãn này (thường là với một khoảng phí nhỏ). Bất kỳ điều gì khác mà một người dùng thực hiện – như gửi tiền từ Ethereum vào Arbitrum, hay sử dụng một dApp (ứng dụng phi tập trung) được triển khai trên một Arbitrum chain – đều không phát sinh khoảng thời gian trì hoãn này.

Như vậy, có phải cơ chế Optimistic Rollup chính là cách và lý do Arbitrum có thể cung cấp mức phí thấp?

Về cơ bản, đúng vậy, đây là cơ sở của việc giảm mức phí giao dịch. Tuy nhiên, có một số biện pháp khác giúp Arbitrum giảm bớt gánh nặng cho L1, tất cả đều dẫn đến giúp giảm chi phí giao dịch cho người dùng cuối. Thứ nhất, các giao dịch Arbitrum được gửi lên L1 theo các lô lớn, một lô điển hình sẽ chứa hàng trăm giao dịch L2. Việc nhóm thành các lô như vậy sẽ giảm bớt chi phí chung của việc tương tác với L1, và do đó mang lại khoản tiết kiệm đáng kể so với việc gửi từng giao dịch giao dịch riêng lẻ tại một thời điểm. Hơn nữa, dữ liệu giao dịch được đăng lên L1 ở dạng nén (và chỉ được giải nén trong môi trường L2) tiếp tục giảm tải cho L1.

Trải nghiệm sử dụng Arbitrum tương đồng với Ethereum

Các giao thức Layer 2 khác nhau nhấn mạnh và tối ưu hóa cho những mục đích khác nhau. Arbitrum được tạo ra với ưu tiên hàng đầu là tương thích với Ethereum. Điều này có nghĩa là người dùng có thể sử dụng Arbitrum với tất cả các ví Ethereum ưa thích của họ; các nhà phát triển có thể xây dựng và triển khai các hợp đồng thông minh với tất cả các thư viện và công cụ Ethereum ưa thích của họ. Trên thực tế, trong hầu hết các trường hợp, trải nghiệm sử dụng Arbitrum sẽ có cảm giác giống hệt với sử dụng Ethereum; với điểm khác biệt quan trọng là nó rẻ hơn và nhanh hơn.

Nhiều công sức đã được đổ vào việc phát triển để đạt được mức độ tương thích Ethereum này. Nhưng ở cốt lõi của nó: bản thân Arbitrum sử dụng một nhánh (fork) của Geth – cách triển khai Ethereum được sử dụng rộng rãi nhất – với các sửa đổi đến biến nó thành một giải pháp trustless (không yêu cầu tin cậy) Layer 2. Điều này có nghĩa là hầu hết code chạy trong Arbitrum là giống hệt với code chạy trong Ethereum. Nhóm phát triển Arbitrum gọi cách tiếp cận tiên tiến này là Nitro.

Ngoài những khả năng giống với trên Ethereum, những nhà phát triển còn có thể làm thêm nhiều điều nữa với Arbitrum. Ở phiên bản mới nhất của Arbitrum, được gọi là Stylus, ngoài duy trình khả năng tương thích với Ethereum của Nitro, còn bổ sung các tính năng mạnh mẽ mới, như tính năng cho phép viết các hợp đồng thông minh có hiệu suất chạy cao bằng các ngôn ngữ lập trình như Rust, C++, và nhiều hơn nữa. Stylus hiện đang có trên mạng thử nghiệm công khai.

Có vẻ như Arbitrum Rollup là một giải pháp lý tưởng mà có thể giải quyết mọi vấn đề mở rộng quy mô?

Arbitrum Rollup cung cấp những tính năng tuyệt vời. Nó được thiết kể chủ yếu hướng tới việc tránh tạo thêm bất kỳ sự tập trung hóa hay yêu cầu tin tưởng nào, và do đó, đây hoàn toàn là một thành công cho hệ sinh thái Ethereum. Tuy nhiên, việc phi tập trung hóa có cái giá của nó (cả theo nghĩa đen), và không phải tất cả các ứng dụng và người dùng đều muốn và cần phải trả cái giá đó. Đối với các trường hợp sử dụng dApp có các cân nhắc an ninh khác nhau, nhà phát triển có thể sử dụng công cụ thích hợp trong bộ Arbitrum. Một công cụ như vậy là các chuỗi (chain) Arbitrum AnyTrust.

AnyTrust Chain là gì?

Một Arbitrum AnyTrust chain không có cùng các sự đảm bảo an ninh về tính phi tập trung / tính không yêu cầu tin cậy / không cần cấp phép như một Rollup chain, và do đó có thể đưa ra các mức phí thấp hơn. Rollup và AnyTrust giống nhau về nhiều mặt, mặc dù có một điểm khác biệt chính: trong khi ở Rollup, tất cả dữ liệu được đăng lên L1 (cho phép mọi người được tham gia làm validator không cần đến sự cho phép), trong AnyTrust, dữ liệu được quản lý hoàn toàn (cho đến khi xảy tranh chấp) ngoài chuỗi (off-chain). Trong trường hợp có tranh chấp, chuỗi AnyTrust sẽ quay lại "chế độ rollup"; giả định ở đây là ít nhất 2 trong số các thành viên của ủy ban là trung thực (tức là họ sẽ cung cấp dữ liệu khi cần thiết). Giữ dữ liệu ngoài chuỗi trong trường hợp vui vẻ/thông thường giúp cho hệ thống có thể tính phí thấp hơn đáng kể cho người dùng. Với các ứng dụng yêu cầu thông lượng (throughput) giao dịch cao và không yêu cầu tính phi tập trung đầy đủ mà rollup cung cấp, AnyTrust có thể là một sự đánh đổi hợp lý.

Như vậy, có nhiều hơn một chuỗi Arbitrum tồn tại?

Đúng vậy. Việc nhiều chuỗi có thể chạy song song là một lợi ích quan trọng đối với công nghệ mở rộng quy mô ngoài chuỗi. Hiện tại, trên mạng chính Ethereum, có 2 chuỗi Arbitrum: một chuỗi Arbitrum Rollup, được gọi là "Arbitrum One", và một chuỗi AnyTrust, được gọi là "Nova". Người dùng và nhà phát triển có thể chọn bất cứ chuỗi nào phù hợp với nhu cầu an ninh/chi phí giao dịch của họ.

Các nhà phát triển còn có lựa chọn khởi chạy chuỗi Arbitrum của riêng họ bên trên chuỗi Arbitrum Layer 2. Những chuỗi như vậy được gọi là các chuỗi Orbit.

Ai đưa ra các quyết định về tương lai của Arbitrum One và Arbitrum Nova?

Các chuỗi Arbitrum One và Nova đang được sở hữu bởi hệ thống Quản trị (Governance) Arbitrum DAO.

Arbitrum là một công nghệ Web3. Các công nghệ Web3 thường được xây dựng ban đầu bởi các corporation (công ty/hội đồng) do một ban giám đốc điều hành. Một khi các công nghệ này đạt được sự phù hợp với thị trường và một cộng đồng các người dùng và các stakeholder (bên có liên quan tới nó, có trách nhiệm với nó và có lợi ích khi nó thành công) phát triển, quyền ra quyết định có thể được phi tập trung hóa dần dần. Đây được gọi là progressive decentralization (phi tập trung hóa lũy tiến/tăng dần) và đó là điều Arbitrum đang làm. Phi tập trung hóa lũy tiến thường được hỗ trợ bởi ba thành phần chính:

1. Thành lập DAO: Arbitrum DAO (Decentrialized Autonomous Organization – Tổ chức Tự trị Phi tập trung) là một thực thể với thẩm quyền ra quyết định trên các chuỗi Arbitrum One và Arbitrum Nova, cùng với các giao thức nền tảng của chúng. DAO được quản lý bởi The Constitution of Arbitrum DAO (Hiến pháp của Arbitrum DAO), là một bộ quy tắc mô tả cách DAO sẽ hoạt động. Hiến pháp đươc khắc ghi vào trong một số hợp đồng xã hội được Arbitrum DAO sử dụng để quản lý chính nó và các công nghệ của nó.

2. Phát hành token quản trị (governance token): Việc sở hữu token quản trị đại diện cho tư cách thành viên trong DAO. Những người nắm giữa token có thể bỏ phiếu cho các đề xuất DAO. Token quản trị của Arbitrum là ARB và vừa mới được phân phát đến các địa chỉ ví đủ điều kiện trong đợi airdrop kết thúc vào cuối tháng 9 năm nay.
3. Code: Việc quản trị của DAO thường được hỗ trợ bởi một loạt các hợp đồng thông minh mã nguồn mở thi hành một giao thức cho việc ra quyết định được nêu lên trong Hiến pháp của Arbitrum DAO.