Mở rộng Ethereum với rollups

Do sự phổ biến của blockchain Ethereum, mạng lưới Ethereum thường xuyên bị tắc nghẽn. Với không gian hạn chế ở lớp cơ sở, phí giao dịch trở nên cực kỳ đắt đỏ do nhiều người cùng tranh giành block space khan hiếm. L2 rollups hoạt động thay vì gửi từng giao dịch riêng lẻ lên mạng Ethereum để xử lý theo thời gian thực, chúng gộp nhiều giao dịch thành một lô (batch) và gửi lên Ethereum theo chu kỳ cố định, nhờ đó phí giao dịch trung bình thấp hơn đáng kể. Tùy vào công nghệ, block space cần thiết cho mỗi lô cũng được tối ưu.

Hiện có hai loại L2 rollups:

1. Rollups lạc quan (Optimistic rollups): Giả định mọi giao dịch đều hợp lệ và chỉ cung cấp bằng chứng gian lận (fraud proof) khi có tranh chấp, nhờ đó người kiểm tra có thể phát hiện giao dịch không hợp lệ.
2. ZK rollups: Sử dụng bằng chứng hợp lệ (validity proof), yêu cầu người đề xuất khối chứng minh giao dịch đã được xác thực.

Cả hai phương pháp đều chuyển phần lớn việc xử lý sang L2 và chỉ giữ lại tính toán tối thiểu trên L1, đồng thời vẫn dựa vào L1 để đảm bảo an ninh và dữ liệu. Mỗi loại đã có nhiều triển khai thực tế trên thị trường

Optimistic rollups

Optimistic rollups, đúng như tên gọi, sử dụng chiến lược "lạc quan" để gom các giao dịch lại. Chúng giả định rằng các giao dịch trong lô là hợp lệ và cho phép một khoảng thời gian để mạng lưới cung cấp bằng chứng gian lận (fraud proof) nhằm hoàn tác (rollback) các giao dịch nếu cần. Cơ chế này cho rằng mạng lưới vẫn an toàn miễn là có ít nhất một trình xác minh trung thực sẵn sàng cung cấp bằng chứng gian lận đúng lúc. Tuy nhiên, vì cho phép cung cấp bằng chứng gian lận và tranh chấp, việc hoàn tất giao dịch có thể mất nhiều thời gian hơn.Thông thường, để vận hành mạng L2, người ta thiết lập một hệ thống cầu hai chiều (two-way bridges) để nạp ether từ mạng Ethereum lớp 1 (L1) nhằm tài trợ cho các giao dịch trên L2. Cầu nối (bridge) là một mô hình thiết kế phổ biến trong blockchain, giúp trao đổi hai loại token gốc từ hai blockchain khác nhau. Quá trình này bao gồm việc khóa ether trên L1 và đúc (mint) token mới trên L2.

Tùy theo loại L2, một số optimistic rollups như Optimism có token riêng để dùng cho giao dịch tài sản và phí gas trên L2. Trong khi đó, một số rollup khác như Arbitrum chỉ đúc token để thanh toán phí gas trên L2.

Ở phía L1 (Ethereum), toàn bộ batch (lô giao dịch) từ L2 rollup được xử lý như một giao dịch duy nhất và tương tác với hợp đồng rollup – nơi lưu trữ trạng thái (state) của L2 trên L1.

- Với Optimistic rollups (ví dụ: Optimism), batch mới được thêm vào danh sách đã sắp xếp trong hợp đồng.
- Sau khi gửi lên L1, có một khoảng thời gian chờ (thường 1-2 tuần) để bất kỳ ai cũng có thể nộp bằng chứng gian lận (fraud proof) nếu phát hiện batch chứa giao dịch không hợp lệ.
- Nếu không có thách thức nào, batch được coi là hợp lệ; ngược lại, L1 sẽ kiểm tra và xử lý tranh chấp.

- Cơ Chế Fraud Proof:
    - Khi phát hiện gian lận, hợp đồng L1 kiểm tra lại giao dịch L2 để xác minh.
    - Nếu đúng có lỗi, khôi phục trạng thái đúng trên cả L1 & L2, thưởng cho người báo cáo.
    - Chỉ cần một người trung thực gửi bằng chứng là đủ đảm bảo an ninh.
- Optimistic Rollups Hoạt Động:
    - Optimism: Phải xử lý lại cả batch + giao dịch sau nếu có lỗi.
    - Arbitrum: Chỉ hoàn lại giao dịch lỗi, tiết kiệm gas.
- Rút Tiền & Thời Gian Chờ:
    - Khi rút từ L2, phải đợi 1-2 tuần (thời gian chống gian lận) trước khi nhận ETH trên L1.
- Ưu Điểm Chính:
    - Phí rẻ hơn (gộp nhiều giao dịch vào một batch).
    - Tốc độ cao (hàng nghìn giao dịch/giây).
    - Bảo mật: Kế thừa an ninh từ Ethereum.

ZK rollups

Bằng chứng không tiết lộ(zero knowledge proof) hoặc giao thức bằng chứng không tiết lộ (zero knowledge protocol) không phải là một khái niệm mới. Nó là 1 phương thức mà 1 bên (người chứng minh -prover) thuyết phục 1 bên khác (người xác minh - verifier) về 1 tuyên bố mà thông tin bí mật là chính xác mà không tiết lộ nó.
Giao thức bằng chứng không tiết lộ (ZKP) có thể là tương tác hoặc không tương tác. Nó đạt được nhiều thành công trong công nghệ blockchain chủ yếu qua hai trường hợp sử dụng riêng biệt ; một là như một cơ chế bảo vệ quyền riêng tư để giải quyết các mối lo ngại về quyền riêng tư dữ liệu trên blockchain, và một cái khác là ZK rollups.

Tương tự như optimistic rollups, ZK rollups gom các giao dịch lại thành lô và công bố lên blockchain lớp 1 theo định kỳ. Thay vì giả định rằng các giao dịch là hợp lệ, ZK rollups tạo ra ZKP bằng cách sử

dụng công nghệ zk-SNARK hoặc zk-STARK cho các giao dịch theo lô, và gửi các giao dịch, trạng thái trước và trạng thái sau cùng với ZKP như một bằng chứng xác thực lên Ethereum mainnet lớp 1.

Hợp đồng rollup trên L1 sẽ xác minh ZKP, và đăng lô đó như một giao dịch duy nhất lên blockchain lớp 1.

Tương tự như optimistic rollups, đều dựa vào hợp đồng bridge để khóa tài sản trên L1 và đúc L2 token. Phí giao dịch thấp hơn, vì 1 lô giao dịch đưa lên L1 và được xem là 1 giao dịch.

Tuy nhiên, với ZK rollups, một bộ tổng hợp cấp sẽ thu thập tất cả các giao dịch , thực thi chúng, tạo ra gốc trạng thái Merkle trước và sau , và chạy zk-SNARKS để tạo ZKP.

Việc tính toán cho bằng chứng này khá phức tạp, và yêu cầu nhiều năng lực tính toán hơn ở nút tổng hợp.

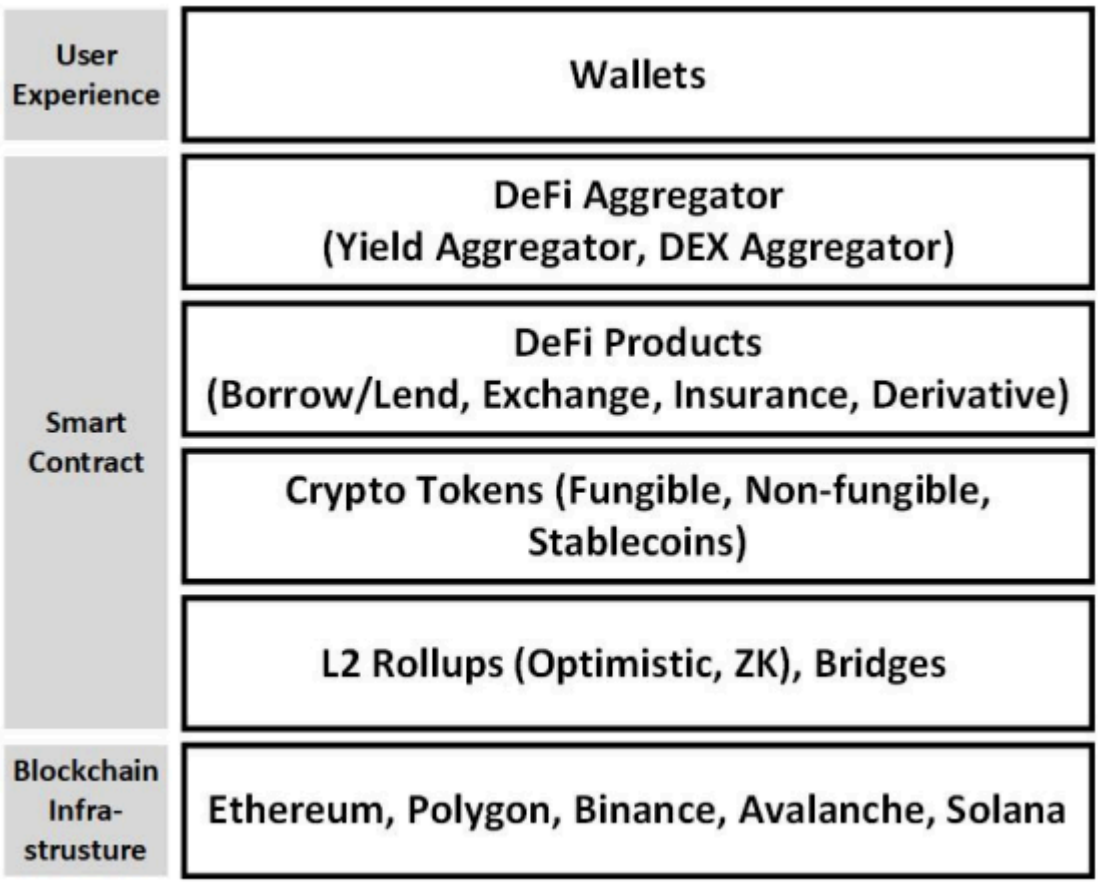
Một vấn đề khác của ZKP là hiện tại nó không thể chạy các hợp đồng thông minh phức tạp.

Tài chính phi tập trung (DeFi)

DeFi là một phiên bản phi tập trung của các sản phẩm và dịch vụ tài chính mà chúng ta thường thấy và giao dịch trong cuộc sống hàng ngày trước khi có blockchain và Bitcoin.

Nó là một tập hợp các sản phẩm và dịch vụ kỹ thuật số gốc blockchain được vận hành bởi công nghệ blockchain và một mạng lưới phi tập trung

Hình ảnh mô tả các lớp công nghệ



- Ở lớp nền là hạ tầng blockchain, cung cấp sức mạnh cho hợp đồng thông minh và ứng dụng DeFi. Đây là lớp quyết toán cuối cùng của tất cả tài sản tiền mã hóa trong DeFi.
- Hợp đồng thông minh cho phép sử dụng rollups lớp 2 để cải thiện khả năng mở rộng và tốc độ xử lý trên hạ tầng blockchain lớp 1 , đồng thời cung cấp kết nối giữa các blockchain khác nhau.
- Các yếu tố cơ bản của tiền mã hóa như token thay thế được , token không thể thay thế (NFTs) và stablecoin được hỗ trợ một cách gốc thông qua hợp đồng thông minh.
- Khả năng tổ hợp trong hợp đồng thông minh giúp xây dựng các giao thức và sản phẩm DeFi hàng đầu, ví dụ như các lĩnh vực: cho vay và vay mượn, sàn giao dịch phi tập trung , phái sinh tiền mã hóa, bảo hiểm và quản lý rủi ro.

Các tiêu chuẩn token của Ethereum

Token trên Ethereum là các hợp đồng thông minh tuân thủ các tiêu chuẩn cụ thể (như ERC-20), được triển khai dưới dạng các smart contract độc lập. Mỗi hợp đồng token xác định các quy tắc về phát hành, chuyển nhượng và quản lý token đó trong hệ sinh thái Ethereum và các mạng tương thích EVM

Cũng giống như tiền pháp định, các coin (đồng tiền mã hóa) như Bitcoin hoặc Ether là tiền mã hóa gốc được đúc ra/phát hành thông qua L1 blockchain protocol và được lưu thông trên blockchain network để thúc đẩy nền kinh tế tiền mã hóa trong hệ sinh thái của nó. Bitcoin đôi khi được gọi là coin bởi vì nó là loại đồng tiền mã hóa đầu tiên được tạo ra. Tất cả các coin được phát hành từ L1 khác, bao gồm Ether và những đồng tiền khác được gọi là Altcoins (đồng thay thế).

Ngược lại, tokens (mã thông báo) là một dạng cryptocurrency và đóng vai trò như một đại diện kỹ thuật số hoặc mã hóa của toàn bộ hoặc một phần tài sản có thể giao dịch trong hệ sinh thái blockchain. Chúng được tạo ra bên ngoài L1, thường thông qua hợp đồng thông minh hoặc các cấu trúc thuộc L2.

Tài sản mã hóa là các tài sản kỹ thuật số có thể giao dịch dưới dạng coin hoặc token trên blockchain. Chúng là một loại tài sản mới xuất hiện nhờ công nghệ tiền mã hóa và blockchain. Những tài sản này được quản lý một cách tự động thông qua mạng ngang hàng và được bảo mật bằng công nghệ mã hóa.

Tokens thường thuộc các loại sau:

- Utility tokens
- Security tokens (mã thông báo chứng khoán): Được tạo ra và điều chỉnh theo các quy định tài chính.
- Payment tokens (mã thông báo thanh toán): Dùng để thanh toán, bao gồm đồng gốc hoặc các token được phát hành để thanh toán như stablecoins
- Fungible tokens (mã thông báo có thể thay thế): Một loại token có thể chuyển nhượng, giống như Bitcoin. Một token bằng một Bitcoin, hoạt động như một Bitcoin, và có giá trị tương đương một Bitcoin.
- NFTs (mã thông báo không thể thay thế): Một loại token đại diện cho tài sản độc nhất – ví dụ, một tác phẩm nghệ thuật gốc.

Fungible tokens and NFTs

Giống như tiền pháp định (fiat), các loại tiền mã hóa như Bitcoin, Ether và Altcoin đều là token fungible (có thể thay thế), nghĩa là chúng có thể hoán đổi với nhau cùng loại. Ví dụ: 1 Bitcoin luôn bằng 1 Bitcoin, chỉ số lượng quan trọng.

Bên cạnh đó, còn có NFT (Non-Fungible Token) – token không thể thay thế, đại diện cho các tài sản độc nhất như:

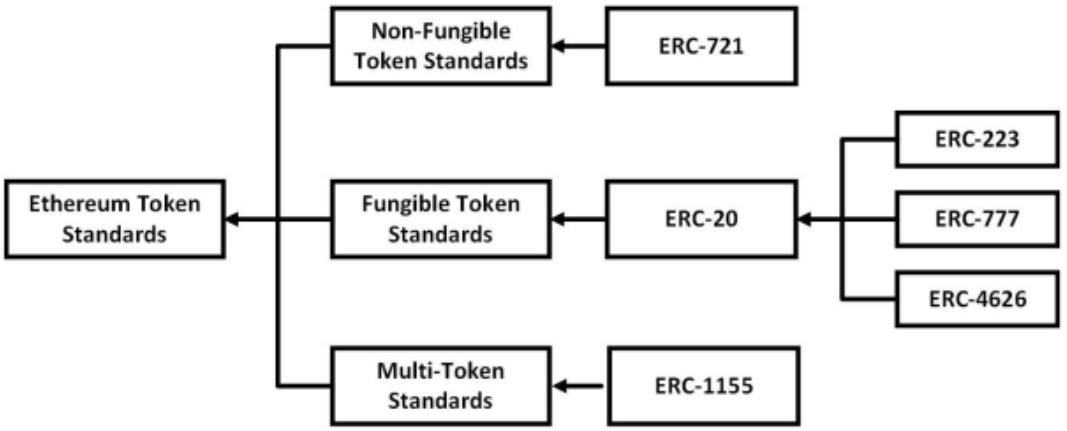
- Tác phẩm nghệ thuật số
- Vật phẩm sưu tầm
- Bản quyền kỹ thuật số
- Royalty (tiền bản quyền)

Ethereum & Tiêu Chuẩn Token

Ethereum cung cấp nền tảng và các tiêu chuẩn token thông qua smart contract, giúp các dự án phát hành token mới. Smart contract đóng vai trò như hợp đồng kỹ thuật số giữa nhà phát hành và nhà đầu tư.

Các tiêu chuẩn phổ biến:

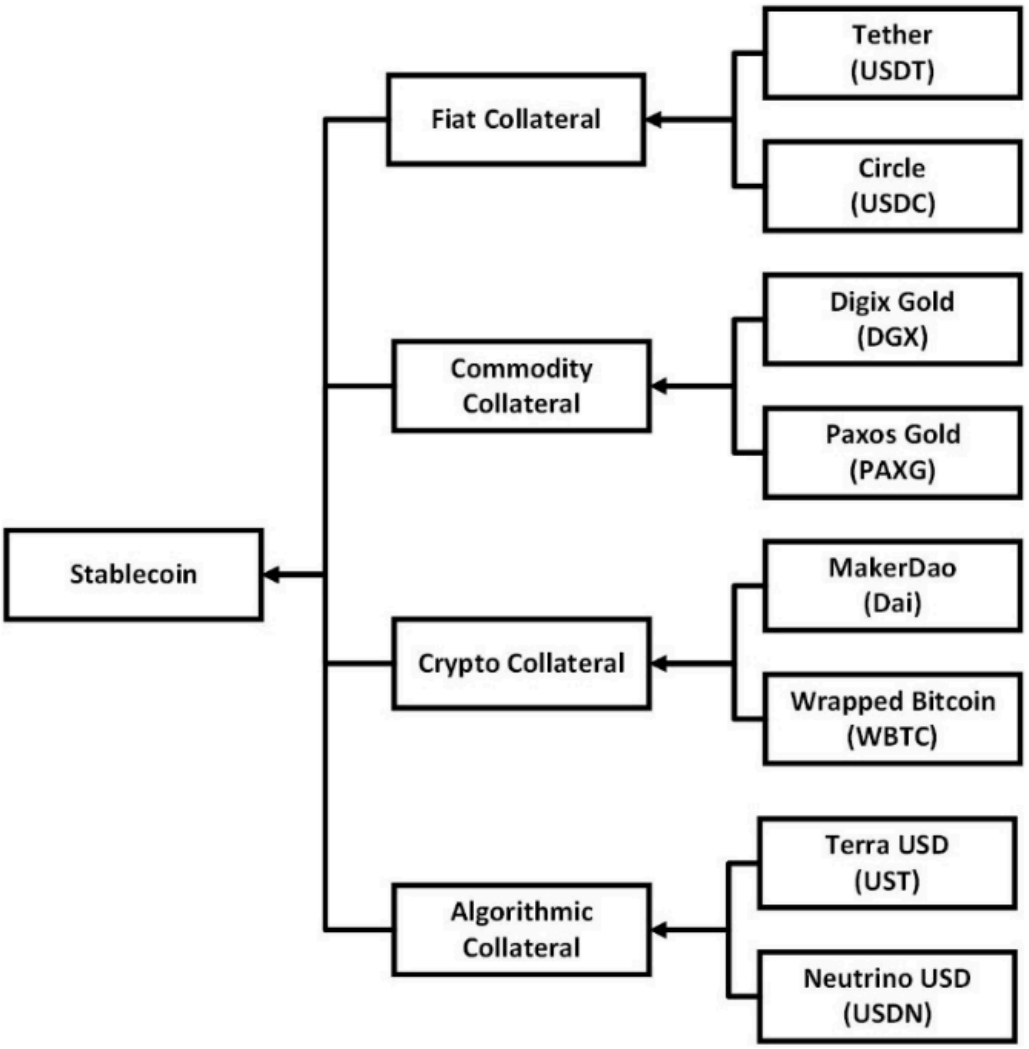
- ERC-20: Chuẩn cho fungible token (tiền mã hóa thông thường).
- ERC-721: Chuẩn cho NFT (token không thể thay thế).
- ERC-1155: Chuẩn đa token, cho phép giao dịch cả fungible và NFT trong một giao dịch.



Stablecoin

Stablecoin là các token tiền mã hóa được sử dụng để cung cấp cho nhà đầu tư các lựa chọn tương đối ổn định thay thế cho việc neo giá trị vào các tài sản cụ thể, chẳng hạn như tiền tệ fiat, hàng hóa, hoặc tiền mã hóa chủ chốt. Cung cấp stablecoin được điều chỉnh dựa trên nhu cầu sử dụng các quy tắc quản trị đã được xác định trước

Có 4 loại stablecoin được xác định như hình ảnh dưới đây



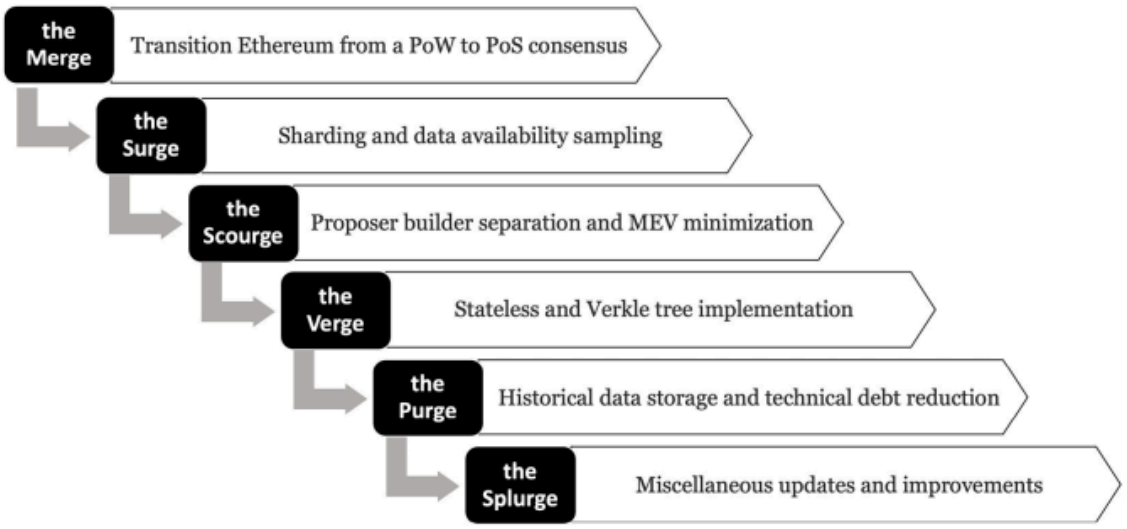
Stablecoin có tài sản bảo chứng bằng tiền fiat: Loại stablecoin này được neo giá trị vào tiền tệ fiat như đồng USD hoặc euro. Nó được bảo chứng bởi một quỹ dự trữ với một lượng tiền fiat nhất định. Một trong những stablecoin phổ biến nhất là Tether (USDT), được neo giá trị vào đồng USD với tỷ lệ 1:1. Circle USDC là một ví dụ khác của loại stablecoin này.

Stablecoin có tài sản bảo chứng bằng hàng hóa: Loại stablecoin này được neo giá trị vào một hàng hóa phổ biến, như vàng. Nó được bảo chứng bởi một giá trị nhất định của hàng hóa đó. Một ví dụ là Digix Gold (DGX), một đồng coin ERC-20 được neo giá trị vào vàng với tỷ lệ mục tiêu là 1 DGX tương ứng với 1 gram vàng. Paxos Gold (PAXG) là một ví dụ khác của loại stablecoin này.

Stablecoin có tài sản bảo chứng bằng tiền mã hóa: Loại stablecoin này được bảo chứng bởi một loại tiền mã hóa chính, như Bitcoin hoặc Ether. Các stablecoin trong nhóm này thường được bảo chứng bằng một lượng nhất định Ether hoặc Bitcoin. Một ví dụ phổ biến là Dai, được tạo ra bởi MakerDAO, được neo vào đồng USD với tỷ lệ mục tiêu là 1:1.

Stablecoin bảo chứng bằng thuật toán: Loại stablecoin này còn được gọi là coin theo phong cách thặng dư (seigniorage). Nó sử dụng thuật toán để kiểm soát nguồn cung của stablecoin. Không có tài sản bảo chứng cho các stablecoin này, và giá trị của chúng hoàn toàn được kiểm soát bởi cung cầu và được ổn định bởi các thuật toán khác nhau.

Lộ trình của ethereum sau khi hợp nhất



- The Merge (Hợp nhất): Hợp nhất Ethereum 1.0 và 2.0, chuyển từ PoW sang PoS. Một số nhiệm vụ còn lại như rút stake và finality trong một slot vẫn chưa hoàn tất.
- The Surge (Bùng nổ): Tập trung mở rộng mạng lưới thông qua rollup L2 và sharding dữ liệu (Danksharding). EIP-4844 (Proto-Danksharding) là bước đầu tiên, hướng đến hơn 100.000 TPS.
- The Scourge (Tai họa): Giới thiệu PBS để giảm rủi ro MEV và tăng tính phi tập trung bằng cách tách vai trò người xây dựng khối và người đề xuất khối.
- The Verge (Cạnh ranh): Triển khai cây Verkle để đơn giản hóa lưu trữ trạng thái và hỗ trợ Ethereum sử dụng SNARK hoàn toàn thông qua zkEVM.
- The Purge (Thanh lọc): Giảm gánh nặng kỹ thuật bằng cách xóa dữ liệu cũ (EIP-4444) và đơn giản hóa EVM, bao gồm cơ chế hết hạn trạng thái.
- The Splurge (Tối ưu hóa): Giai đoạn tổng hợp để cải tiến thêm, bao gồm trừu tượng hóa tài khoản (EIP-4337), cải cách phí (EIP-1559), và hàm trì hoãn xác minh (VDF).

Sharding và tính khả dụng dữ liệu (data availability sampling)

Sharding (phân mảnh dữ liệu) là giải pháp mở rộng quan trọng của Ethereum sau The Merge, tập trung vào phân mảnh dữ liệu thay vì cả dữ liệu và thực thi.

Sharding là kỹ thuật phân vùng dữ liệu ngang, chia cơ sở dữ liệu lớn thành các shard nhỏ hơn. Trong blockchain, sharding giúp giảm tải cho từng nút bằng cách phân phối dữ liệu trên

các nút con thay vì yêu cầu mọi nút lưu trữ toàn bộ chuỗi. Ban đầu, Ethereum dự kiến chia dữ liệu thành 64 shard, liên kết với Beacon Chain.

Tuy nhiên, sharding truyền thống gặp phải một số thách thức. Việc xử lý giao dịch liên shard (cross-shard transactions) khá phức tạp. Ngoài ra, có nguy cơ tập trung hóa do yêu cầu lưu trữ dữ liệu lớn trên chuỗi.

Để giải quyết những vấn đề này, Ethereum đã chuyển hướng sang giải pháp đơn giản hơn là Proto-Danksharding và Danksharding. Proto-Danksharding (EIP-4844) là bước đầu tiên, cung cấp 1MB dung lượng tạm thời cho dữ liệu L2 dưới dạng blobs, không cần lưu trữ vĩnh viễn. Trong tương lai, Danksharding hoàn chỉnh sẽ mở rộng lên 16-32MB, tăng khả năng mở rộng gấp khoảng 16 lần so với hiện tại.

Rollup L2 đóng vai trò quan trọng trong kiến trúc này. Các giải pháp Rollup (Optimistic/ZK) xử lý giao dịch ngoài chuỗi, chỉ gửi dữ liệu lên L1 để đảm bảo tính khả dụng. Ethereum L1 chỉ cần kiểm tra tính khả dụng của dữ liệu chứ không xác thực nội dung.

Về mặt bảo mật và phi tập trung, dữ liệu lịch sử không cần được lưu trữ trên mọi nút. Cơ chế mã hóa và kinh tế game theory đảm bảo tính toàn vẹn của hệ thống. Ngay cả khi có tác nhân độc hại cố gắng che giấu hoặc thao túng dữ liệu cũ, việc này cũng khó thực hiện do các bằng chứng gian lận dễ dàng bị phát hiện.

Tóm lại, sharding đơn giản hóa (Proto-Danksharding) là bước tiến quan trọng giúp Ethereum mở rộng thông lượng giao dịch. Cùng với sự hỗ trợ từ các giải pháp Rollup L2, Ethereum có thể đạt được khả năng mở rộng cao trong khi vẫn duy trì được tính phi tập trung và bảo mật vốn có. Kiến trúc này cho phép Ethereum hướng tới mục tiêu trở thành nền tảng blockchain có khả năng xử lý hàng trăm nghìn giao dịch mỗi giây, đủ sức cạnh tranh với các hệ thống thanh toán truyền thống như Visa hay Mastercard.