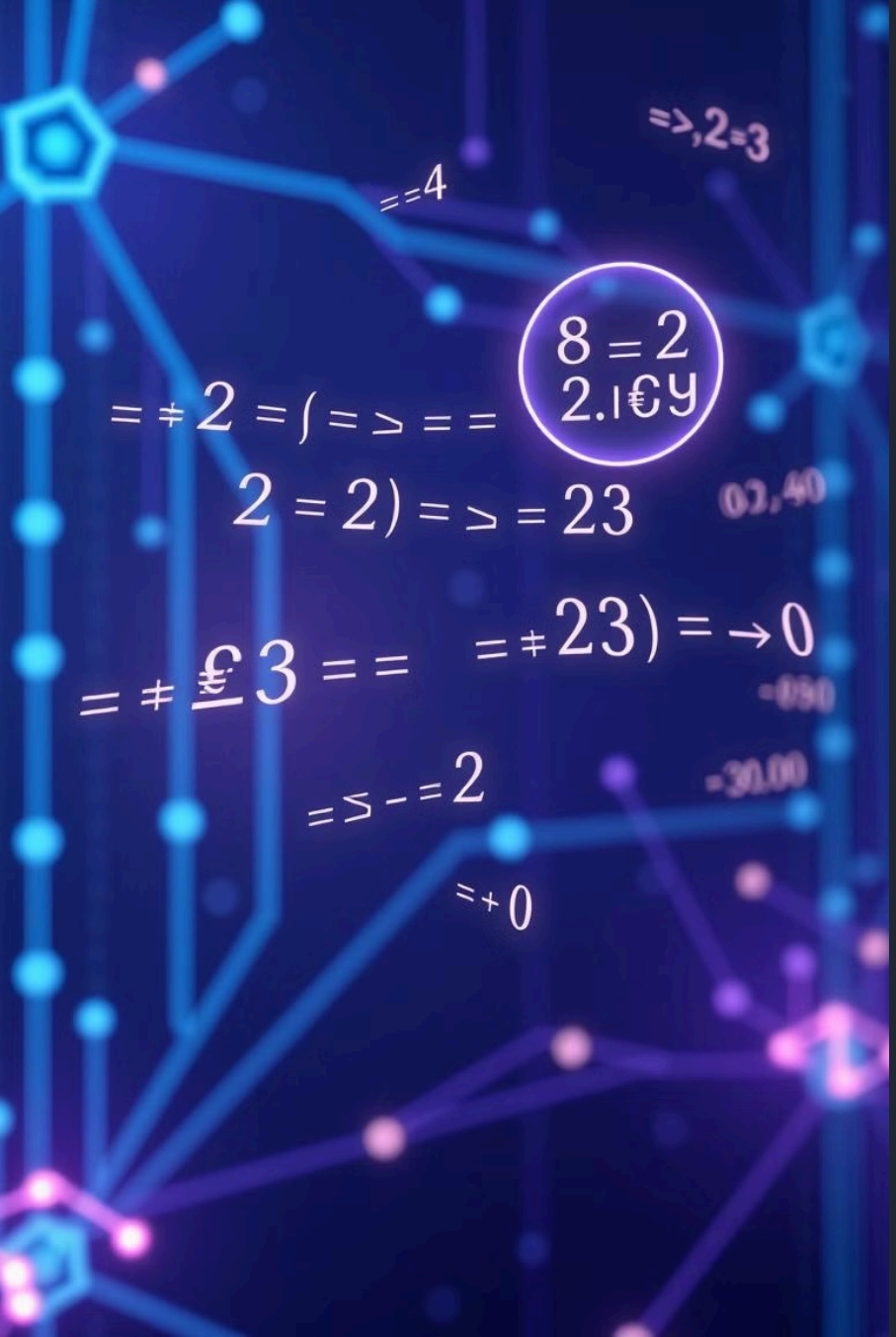


Polynomial Commitments: Nền Tảng Của SNARKs & STARKs

Trong hệ thống Zero-Knowledge Proofs (ZKP), Polynomial Commitment Schemes là một giải pháp quan trọng, được sử dụng trong zk-SNARKs và zk-STARKs, giúp đảm bảo tính bảo mật và hiệu quả của các bằng chứng. Bài viết này sẽ khám phá chi tiết về Polynomial Commitment Scheme, so sánh KZG Commitment và FRI Commitment, và ứng dụng của KZG Commitment trong Ethereum EIP-4844 (Proto-Danksharding).

Polynomial Commitment Scheme Là Gì?

Nguyên lý hoạt động

Polynomial Commitment Scheme cho phép cam kết với một đa thức mà không tiết lộ nội dung, sau đó chứng minh giá trị đánh giá tại một điểm cụ thể. Nó bao gồm ba thuật toán chính: Commit, Prove, và Verify.

Tính chất bảo mật

Tính chất bảo mật của Polynomial Commitment Scheme bao gồm Hiding (cam kết không tiết lộ thông tin) và Binding (người gửi không thể tạo hai đa thức khác nhau có cùng cam kết). Ứng dụng chính là trong SNARKs và STARKs để chứng minh tính đúng đắn của các tính toán phức tạp.

So Sánh KZG Commitment vs. FRI Commitment

KZG Commitment

Sử dụng cặp ghép elliptic curve để tạo cam kết nhỏ gọn, phù hợp với zk-SNARKs. Kích thước cam kết và bằng chứng nhỏ, xác minh nhanh, nhưng yêu cầu thiết lập tin cậy (Trusted Setup).

FRI Commitment

Sử dụng cây Merkle và mã hóa Reed-Solomon, không cần cặp ghép, phù hợp với zk-STARKs. Kích thước cam kết lớn hơn, xác minh chậm hơn, nhưng không cần thiết lập tin cậy và bảo mật trước máy tính lượng tử.

KZG Commitment – Tối Ưu Cho SNARKs

Hiệu suất

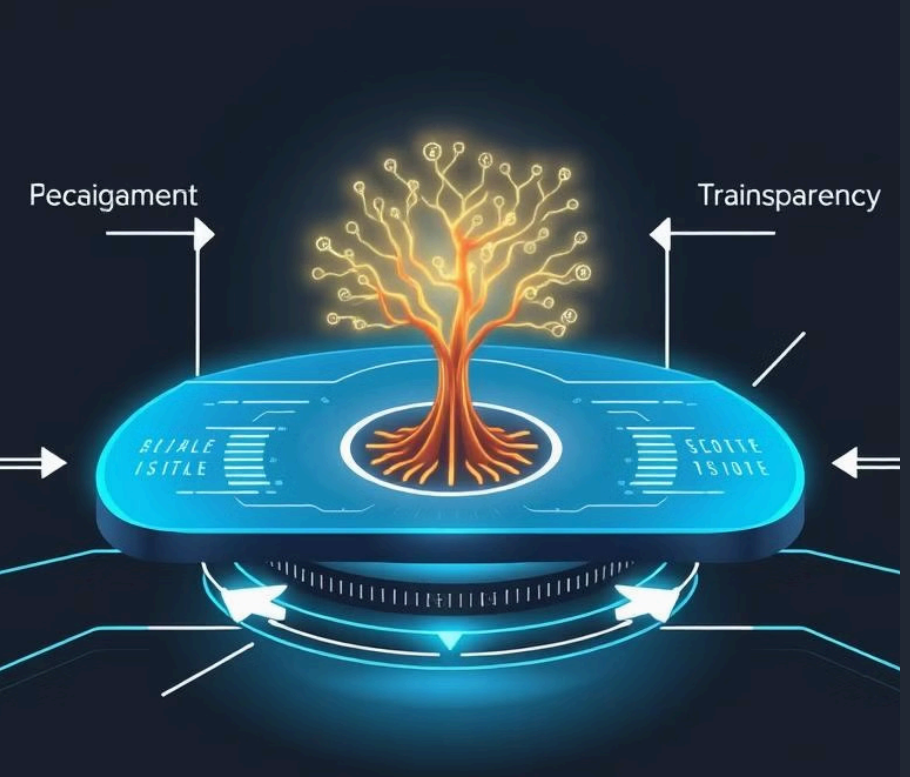
Kích thước cam kết và bằng chứng nhỏ, xác minh nhanh.

Bảo mật

Dựa trên Discrete Logarithm Problem (DLP), có tính bảo mật cao.

Điểm yếu

Yêu cầu Trusted Setup, có thể là điểm yếu nếu bị xâm phạm.



FRI Commitment – Tối Ưu Cho STARKs

Bảo mật

Không cần thiết lập tin cậy, an toàn hơn trong môi trường phi tập trung.

Post-quantum

Không bị đe dọa bởi máy tính lượng tử.

Hiệu suất

Kích thước cam kết lớn hơn, xác minh chậm hơn.

Ứng Dụng KZG Commitment Trong EIP-4844

1

Blob

Dữ liệu giao dịch được lưu dưới dạng "blob" (khối dữ liệu lớn).

2

Cam kết

Mỗi blob được cam kết bằng KZG Commitment.

3

Xác minh

Các node xác minh dữ liệu mà không cần lưu trữ toàn bộ blob, chỉ cần kiểm tra KZG Commitment.

Lợi Ích Của KZG Trong EIP-4844

Giảm phí gas

Vì các node không cần tải toàn bộ dữ liệu.

Mở rộng quy mô

Giúp Ethereum hỗ trợ nhiều giao dịch hơn.

Xác minh nhanh chóng

Giúp các node nhẹ hoạt động hiệu quả hơn.

Ứng Dụng Rộng Hơn Của KZG Commitment

Layer 2

Giúp Layer 2 như Optimistic Rollups và ZK-Rollups hoạt động hiệu quả hơn.

Mở rộng

Cải thiện khả năng mở rộng của các giải pháp blockchain.

Chi phí

Giảm chi phí giao dịch cho người dùng.

Tóm Lược Về Polynomial Commitment Schemes

1

KZG

Tối ưu cho SNARKs, hiệu suất cao, yêu cầu Trusted Setup.

2

FRI

Phù hợp cho STARKs, minh bạch hơn, bảo mật trước máy tính lượng tử.

3

EIP-4844

Sử dụng KZG Commitment để mở rộng quy mô và giảm phí gas.

Kết Luận

Polynomial Commitment Schemes là nền tảng quan trọng của SNARKs và STARKs, giúp xác minh tính toán mà không cần tiết lộ thông tin. KZG Commitment tối ưu cho SNARKs, với hiệu suất cao nhưng yêu cầu Trusted Setup. FRI Commitment phù hợp cho STARKs, minh bạch hơn và bảo mật trước máy tính lượng tử. Ethereum EIP-4844 (Proto-Danksharding) sử dụng KZG Commitment để mở rộng quy mô và giảm phí gas.