Halo & Nova: Chứng Minh Đệ Quy Không Cần Trusted Setup

Halo & Nova là Zero-Knowledge Proofs (ZKP) đột phá. Chúng hỗ trợ chứng minh đệ quy mà không cần Trusted Setup. Tìm hiểu về Recursive SNARKs, Halo2 & Nova Proofs trong zk-EVM!

Giới Thiệu

1 Nhu cầu ZKP

Nhu cầu về ZKP hiệu quả, linh hoạt ngày càng lớn.

2 Halo & Nova

Bước tiến quan trọng, tạo bằng chứng đệ quy, giảm chi phí.

3 Phát triển

Được phát triển bởi ECC và Cryptography Research Labs.

Key Takeaways

Recursive SNARKs

Mở rộng quy mô blockchain, tạo bằng chứng duy nhất.

Halo & Halo2

SNARKs đệ quy không cần Trusted Setup, tối ưu zk-EVM.

Nova Proofs

Giảm kích thước bằng chứng ZKP, hiệu quả hơn.

Recursive SNARKs

Xác minh

Chuỗi tính toán phức tạp bằng cách đệ quy.

Tạo

Một bằng chứng duy nhất cho nhiều giao dịch.

Giảm

Chi phí tính toán cho zk-EVM, zk-Rollups.

Cách Hoạt Động

1

Tạo bằng chứng

Cho bước tính toán đầu tiên.

2

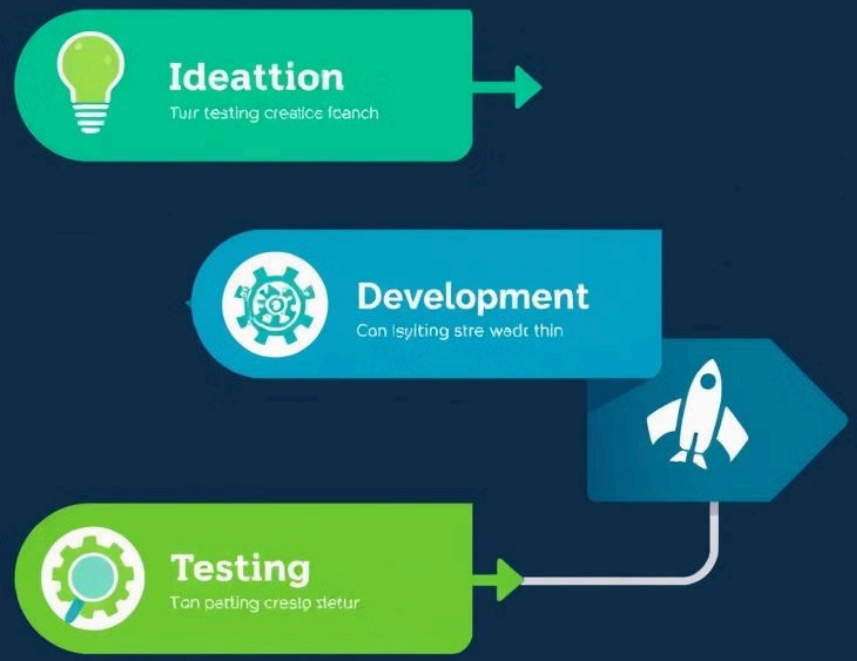
Dùng bằng chứng

Làm đầu vào cho bước tiếp theo.

3

Lặp lại

Quá trình cho đến khi có bằng chứng duy nhất.



Lợi Ích

Mở rộng

Quy mô blockchain.

Tiết kiệm

Tài nguyên tính toán.

Giảm

Phí gas trên Ethereum.

Halo & Halo2

Giới Thiệu

Halo: SNARKs đầu tiên hỗ trợ đệ quy không cần Trusted Setup.

Halo2: Phiên bản cải tiến, tối ưu hóa cho Ethereum Layer 2.

Tại Sao Quan Trọng?

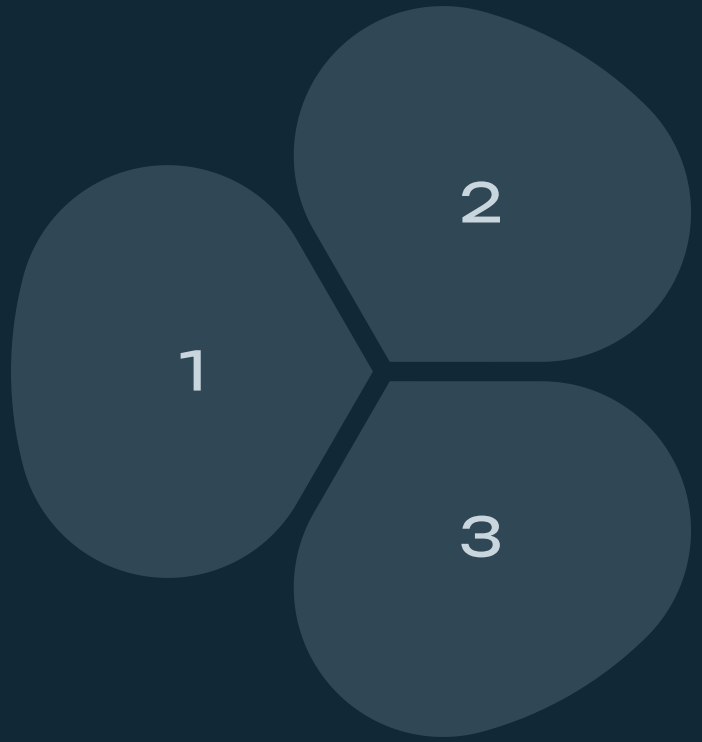
Hỗ trợ đệ quy không cần Trusted Setup, giảm rủi ro.

Tổng hợp nhiều giao dịch, giảm phí gas.

Nova Proofs

Giới Thiệu

Hệ thống ZKP tối ưu, giảm kích thước proof.



Tập trung

Low-depth circuits, hiệu suất cao.

Tích hợp

Polynomial Commitment Schemes.

So Sánh

Tiêu chí	Halo & Halo2	Nova Proofs
Mục tiêu	Đệ quy SNARKs	Tối ưu kích thước
Kích thước	Trung bình	Nhỏ

Kết Luận

Tiến bộ

Quan trọng trong ZKP, tăng hiệu suất.

Tập trung

Halo & Halo2 cho Recursive SNARKs.

Tối ưu

Nova Proofs giảm chi phí xác minh.