# **Halo & Nova – Chứng Minh Đệ Quy Không Cần Trusted Setup**

## **Meta Description**

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

## **Giới Thiệu**

Khi các hệ thống **blockchain** mở rộng quy mô, nhu cầu về **ZKP hiệu quả, linh hoạt và không cần Trusted Setup** ngày càng lớn. **Halo & Nova** xuất hiện như một **bước tiến quan trọng**, giúp **tạo bằng chứng đệ quy**, giảm chi phí tính toán mà vẫn đảm bảo bảo mật cao.

Được phát triển bởi các nhà nghiên cứu từ **ECC (Electric Coin Company) và Cryptography Research Labs**, Halo và Nova đã chứng minh tiềm năng lớn trong các ứng dụng như **zk-EVM, zk-Rollups, và AI Proof Verification**.

### **Nội dung chính trong bài viết:**

🔹 **Recursive SNARKs – Cách ZKP mở rộng vô hạn** 🔹 **Halo & Halo2 – Ứng dụng trong zk-EVM** 🔹 **Nova Proofs – Giải pháp tối ưu kích thước bằng chứng ZKP**

Hãy cùng khám phá chi tiết! 🚀

## **Key Takeaways**

✅ **Recursive SNARKs giúp mở rộng quy mô blockchain**, giảm tải cho chuỗi chính bằng cách tạo **một bằng chứng duy nhất cho nhiều giao dịch**.  
 ✅ **Halo & Halo2 là các giao thức SNARKs đệ quy không cần Trusted Setup**, giúp tối ưu hóa hiệu suất cho **zk-EVM** và **zk-Rollups**.  
 ✅ **Nova Proofs tập trung vào giảm kích thước bằng chứng**, làm cho ZKP hiệu quả hơn trong blockchain và các ứng dụng **AI Proof Verification**.  
 ✅ **Cả Halo và Nova đều không cần Trusted Setup**, giúp giảm rủi ro bảo mật và tăng tính minh bạch trong hệ thống.

## **Recursive SNARKs – Cách ZKP Mở Rộng Vô Hạn**

[**Recursive SNARKs**](https://medium.com/@richardchen_81235/intro-to-recursive-snarks-50d201796109) là một khái niệm trong ZKP cho phép:

✔️ **Xác minh một chuỗi tính toán phức tạp** bằng cách đệ quy các bằng chứng trước đó vào bằng chứng mới.  
 ✔️ **Tạo một bằng chứng duy nhất** để xác minh nhiều giao dịch blockchain.  
 ✔️ **Giảm chi phí tính toán** cho các ứng dụng như **zk-EVM, zk-Rollups và AI Model Verification**.

### **Cách Hoạt Động**

1️⃣ **Người chứng minh tạo bằng chứng** cho một bước tính toán đầu tiên.  
 2️⃣ **Dùng bằng chứng đó làm đầu vào** cho bước tiếp theo, tiếp tục tạo các bằng chứng mới.  
 3️⃣ **Lặp lại quá trình** cho đến khi có một bằng chứng duy nhất đại diện cho toàn bộ chuỗi tính toán.  
 4️⃣ **Người kiểm tra chỉ cần xác minh bằng chứng cuối cùng**, thay vì phải xác minh từng bước riêng lẻ.

### **Lợi Ích Của Recursive SNARKs**

✔️ **Mở rộng quy mô blockchain** – Cho phép tổng hợp hàng ngàn giao dịch trong một proof duy nhất.  
 ✔️ **Tiết kiệm tài nguyên tính toán** – Người kiểm tra chỉ cần xác minh một proof, thay vì từng proof riêng lẻ.  
 ✔️ **Giảm phí gas trên Ethereum** – Ứng dụng trong **zk-Rollups**, giúp giảm chi phí giao dịch đáng kể.

💡 **Một chi tiết bất ngờ:** Recursive SNARKs **không chỉ ứng dụng trong blockchain**, mà còn trong **AI Model Verification**, nơi cần xác minh hàng triệu phép tính mà không tiết lộ dữ liệu gốc.

## **Halo & Halo2 – Ứng Dụng Trong zk-EVM**

### **Giới Thiệu Halo & Halo2**

[Halo](https://eprint.iacr.org/2020/1536.pdf) là một trong những giao thức SNARKs đầu tiên hỗ trợ **đệ quy không cần Trusted Setup**, ra mắt vào năm 2018 bởi **ECC (Electric Coin Company)**. [**Halo2**](https://docs.orbisprotocol.com/orbis/technology/halo-2) là phiên bản cải tiến, được tối ưu hóa để hỗ trợ **Ethereum Layer 2** và **zk-EVM**.

### **Tại Sao Halo Quan Trọng Trong zk-EVM?**

Ethereum đang tiến tới **zk-EVM**, nơi các giao dịch có thể được xác minh bằng **ZKP** để giảm tải cho chuỗi chính. **Halo & Halo2 đóng vai trò quan trọng trong quá trình này**, nhờ các lợi ích sau:

✔️ **Hỗ trợ đệ quy không cần Trusted Setup**, giúp giảm rủi ro bảo mật.  
 ✔️ **Tổng hợp nhiều giao dịch thành một proof duy nhất**, giúp giảm phí gas trên Ethereum.  
 ✔️ **Tăng tốc độ xác minh**, cho phép xử lý hàng ngàn giao dịch mỗi giây.

### **Ứng Dụng Halo & Halo2 Trong zk-EVM**

🔹 **zkSync & Scroll** – Các giao thức zk-Rollups có thể tích hợp Halo để cải thiện hiệu suất.  
 🔹 **Zcash & Private Transactions** – Halo giúp bảo vệ quyền riêng tư giao dịch bằng cách tổng hợp các proof.  
 🔹 **Ethereum Scaling** – Halo có thể giúp Ethereum mở rộng quy mô với chi phí thấp hơn.

## **Nova Proofs – Giải Pháp Tối Ưu Kích Thước Bằng Chứng ZKP**

### **Giới Thiệu Nova Proofs**

[Nova Proofs](https://eprint.iacr.org/2021/370.pdf) là một hệ thống **ZKP tối ưu**, được phát triển để **giảm kích thước proof và cải thiện hiệu suất xác minh**.

🔹 **Được giới thiệu vào năm 2020**, Nova tập trung vào **low-depth circuits** – các mạch tính toán đơn giản nhưng cần hiệu suất cao.  
 🔹 **Tích hợp Polynomial Commitment Schemes** để giảm tải tính toán và kích thước proof.  
 🔹 **Ứng dụng trong zk-Rollups & AI Proof Verification**, giúp giảm chi phí lưu trữ và tăng tốc độ xác minh.

💡 **Một chi tiết bất ngờ:** Nova không chỉ giúp **giảm kích thước proof trong blockchain**, mà còn trong **AI Model Verification**, giúp xác minh các mô hình AI mà không cần tiết lộ dữ liệu huấn luyện.

## **So Sánh Halo, Halo2 & Nova**

| **Tiêu chí** | **Halo & Halo2** | **Nova Proofs** |
| --- | --- | --- |
| **Mục tiêu** | Đệ quy SNARKs không cần Trusted Setup | Tối ưu kích thước proof & tốc độ xác minh |
| **Kích thước proof** | Trung bình (~vài trăm bytes) | Nhỏ (~vài trăm bytes) |
| **Ứng dụng** | zk-EVM, tổng hợp nhiều giao dịch | zk-Rollups, AI Proof Verification |
| **Yêu cầu Trusted Setup** | Không cần | Không cần |
| **Tốc độ xác minh** | Nhanh | Rất nhanh |

## **Kết Luận**

✅ **Halo, Halo2 và Nova Proofs là những tiến bộ quan trọng trong Zero-Knowledge Proofs**, giúp tăng cường hiệu suất và mở rộng quy mô blockchain.  
 ✅ **Halo & Halo2 tập trung vào Recursive SNARKs không cần Trusted Setup**, phù hợp cho **zk-EVM** và **Ethereum Scaling**.  
 ✅ **Nova Proofs tối ưu hóa kích thước proof**, giúp giảm chi phí xác minh trong **zk-Rollups và AI Verification**.  
 ✅ **Cả Halo & Nova đều giúp giảm phí gas trên Ethereum**, mở ra tiềm năng ứng dụng rộng rãi hơn trong Web3.

🔹 **Bạn nghĩ gì về Halo & Nova? Liệu chúng có thể thay thế zk-SNARKs và zk-STARKs trong tương lai?** Hãy để lại bình luận bên dưới! 👇

💡 **Bài tiếp theo:** ZK-Rollups – Cách ZKP Giúp Ethereum Mở Rộng Quy Mô & Giảm Phí Gas 🚀