# **zk-STARKs: Zero-Knowledge Proof Không Cần Trusted Setup**

## **Meta Description**

zk-STARKs giúp xác minh tính toán mà không cần Trusted Setup. Tìm hiểu STARK Proofs, FRI Commitment Scheme & vì sao zk-STARKs an toàn trước máy tính lượng tử!

## **Giới Thiệu**

Trong hệ thống **Zero-Knowledge Proofs (ZKP)**, **zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge)** là một trong những giao thức tiên tiến nhất. Nó giúp xác minh tính toán mà không cần **Trusted Setup**, giúp tăng tính minh bạch và loại bỏ rủi ro bảo mật.

zk-STARKs được ứng dụng rộng rãi trong **blockchain, bảo mật giao dịch, và mở rộng quy mô**, đặc biệt trong các nền tảng như **StarkNet, zk-Rollups, và Ethereum Layer 2**.

Trong bài viết này, chúng ta sẽ tìm hiểu:

🔹 **zk-STARKs là gì và cách hoạt động** 🔹 **Vai trò của STARK Proofs và FRI Commitment Scheme** 🔹 **Tại sao zk-STARKs an toàn hơn zk-SNARKs trước máy tính lượng tử** 🔹 **So sánh zk-STARKs và zk-SNARKs**

Hãy cùng khám phá! 🚀

## **Key Takeaways**

✅ **zk-STARKs** là một giao thức Zero-Knowledge Proofs không cần Trusted Setup, tăng tính minh bạch.  
 ✅ **STARK Proofs & FRI Commitment Scheme** giúp chứng minh tính toán trên blockchain một cách an toàn và hiệu quả.  
 ✅ **zk-STARKs an toàn hơn zk-SNARKs trước máy tính lượng tử** vì không phụ thuộc vào logarithm rời rạc hay cặp ghép elliptic curve.  
 ✅ **Nhược điểm của zk-STARKs** là kích thước bằng chứng lớn hơn và tốc độ xác minh chậm hơn so với zk-SNARKs.

## **Cách Hoạt Động Của zk-STARKs**

### **zk-STARKs là gì?**

zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge) là một loại Zero-Knowledge Proofs **không cần Trusted Setup**, giúp chứng minh một tuyên bố mà không tiết lộ thông tin liên quan.

Giao thức này được phát triển bởi **Eli Ben-Sasson** và các cộng sự vào năm 2018. Nó được sử dụng trong **blockchain, bảo mật giao dịch, và mở rộng quy mô**, đặc biệt trong **Ethereum Layer 2 và ZK-Rollups**.

💡 **Điểm đặc biệt:** zk-STARKs **không phụ thuộc vào giả định bảo mật yếu** như logarithm rời rạc, giúp nó an toàn trước máy tính lượng tử.

### **Quy Trình Hoạt Động Của zk-STARKs**

🔹 **Bước 1: Biểu Diễn Tính Toán**

* Tính toán được biểu diễn dưới dạng **một chuỗi trạng thái** hoặc **bước thực thi chương trình**.
* Mỗi bước được biểu diễn dưới dạng **chuỗi nhị phân hoặc số học**.

🔹 **Bước 2: Cam Kết Với Đa Thức**

* Chuỗi trạng thái được chuyển đổi thành một **đa thức**, thường qua **nội suy Lagrange**.
* Cam kết với đa thức này bằng cách sử dụng **cây Merkle** hoặc giao thức **FRI (Fast Reed-Solomon Interactive Oracle Proof)**.

🔹 **Bước 3: Tạo Bằng Chứng**

* Người chứng minh (Prover) tạo bằng chứng rằng chuỗi trạng thái **thỏa mãn các ràng buộc tính toán**.
* Bằng chứng này bao gồm các đánh giá tại các **điểm ngẫu nhiên** và các cam kết phụ.

🔹 **Bước 4: Xác Minh Bằng Chứng**

* Người kiểm tra (Verifier) kiểm tra tính hợp lệ mà **không cần biết chi tiết tính toán**.
* Điều này được thực hiện qua **các phép toán trên trường hữu hạn và cây Merkle**.

💡 **Bằng chứng zk-STARKs không tương tác**, được đạt được bằng cách sử dụng **Fiat-Shamir Heuristic**.

## **STARK Proofs & FRI Commitment Scheme**

### **STARK Proofs Là Gì?**

STARK Proofs là nền tảng của zk-STARKs, giúp chứng minh tính toán mà **không cần Trusted Setup**. Chúng sử dụng **FRI Commitment Scheme**, một kỹ thuật dựa trên **mã Reed-Solomon**, để cam kết với dữ liệu một cách an toàn.

### **FRI Commitment Scheme Hoạt Động Như Thế Nào?**

🔹 **Bước 1: Cam Kết Với Đa Thức**

* Chuỗi trạng thái được chuyển đổi thành một **đa thức**.
* Cam kết với đa thức này thông qua **cây Merkle** hoặc **FRI Commitment**.

🔹 **Bước 2: Giảm Độ Bậc Đa Thức**

* FRI kiểm tra xem đa thức có bậc thấp không bằng cách **giảm dần độ bậc** qua các bước đánh giá.
* Điều này giúp đảm bảo tính toàn vẹn và xác minh nhanh hơn.

🔹 **Bước 3: Xác Minh Bằng Chứng**

* Người kiểm tra kiểm tra tính hợp lệ của cam kết **mà không cần biết nội dung đa thức**.

💡 **FRI không cần Trusted Setup, giúp tăng tính minh bạch và bảo mật của zk-STARKs.**

## **Tại Sao zk-STARKs An Toàn Hơn zk-SNARKs Trước Máy Tính Lượng Tử?**

zk-STARKs an toàn hơn zk-SNARKs vì **không dựa trên logarithm rời rạc hay cặp ghép elliptic curve**, hai giả định bảo mật dễ bị phá vỡ bởi **máy tính lượng tử**.

### **So Sánh Bảo Mật**

| **Giao thức** | **Dựa vào giả định bảo mật** | **An toàn trước máy tính lượng tử?** |
| --- | --- | --- |
| **zk-SNARKs** | Logarithm rời rạc (Elliptic Curve) | ❌ Không an toàn (bị tấn công bởi thuật toán Shor) |
| **zk-STARKs** | Mã Reed-Solomon, không phụ thuộc vào số nguyên tố lớn | ✅ An toàn trước máy tính lượng tử |

💡 **Điểm quan trọng:** zk-STARKs **không bị ảnh hưởng** bởi thuật toán Shor, giúp nó **post-quantum secure**.

## **So Sánh zk-STARKs Và zk-SNARKs**

| **Tiêu chí** | **zk-STARKs** | **zk-SNARKs** |
| --- | --- | --- |
| **Yêu cầu Trusted Setup** | ❌ Không cần | ✅ Cần |
| **Kích thước bằng chứng** | 📏 Lớn (~từ vài KB) | 🏷 Nhỏ (~vài trăm byte) |
| **Tốc độ xác minh** | 🕒 Chậm hơn (nhiều phép toán) | ⚡ Nhanh hơn |
| **An toàn lượng tử** | ✅ Có | ❌ Không |
| **Dựa vào giả định bảo mật** | Mã Reed-Solomon | Logarithm rời rạc |

✅ **zk-STARKs** phù hợp cho các hệ thống **minh bạch, bảo mật cao, không cần Trusted Setup**.  
 ✅ **zk-SNARKs** phù hợp cho các hệ thống **cần hiệu suất cao và bằng chứng nhỏ gọn**.

## **Kết Luận**

✅ **zk-STARKs là một bước tiến lớn trong ZKP**, giúp loại bỏ Trusted Setup và tăng tính minh bạch.  
 ✅ **STARK Proofs và FRI Commitment Scheme** giúp xác minh tính toán trên blockchain một cách an toàn.  
 ✅ **zk-STARKs an toàn hơn zk-SNARKs trước máy tính lượng tử**, nhưng có kích thước bằng chứng lớn hơn.  
 ✅ **Nhược điểm của zk-STARKs** là tốc độ xác minh chậm hơn, nhưng đổi lại là bảo mật cao hơn.

💡 **Bài tiếp theo:** Bulletproofs – Zero-Knowledge Proof Không Cần Trusted Setup 🚀