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

zk-STARKs giúp xác minh tính toán mà không cần Trusted Setup. Nó 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.

Made with Gamma

zk-STARKs Là Gì?

zk-STARKs là Zero-Knowledge Proofs không cần Trusted Setup. Nó giúp chứng minh một tuyên bố mà không tiết lộ thông tin liên quan. Giao thức này được phát triển bởi Eli Ben-Sasson vào năm 2018.

Không Cần Trusted Setup

Tăng tính minh bạch và bảo mật.

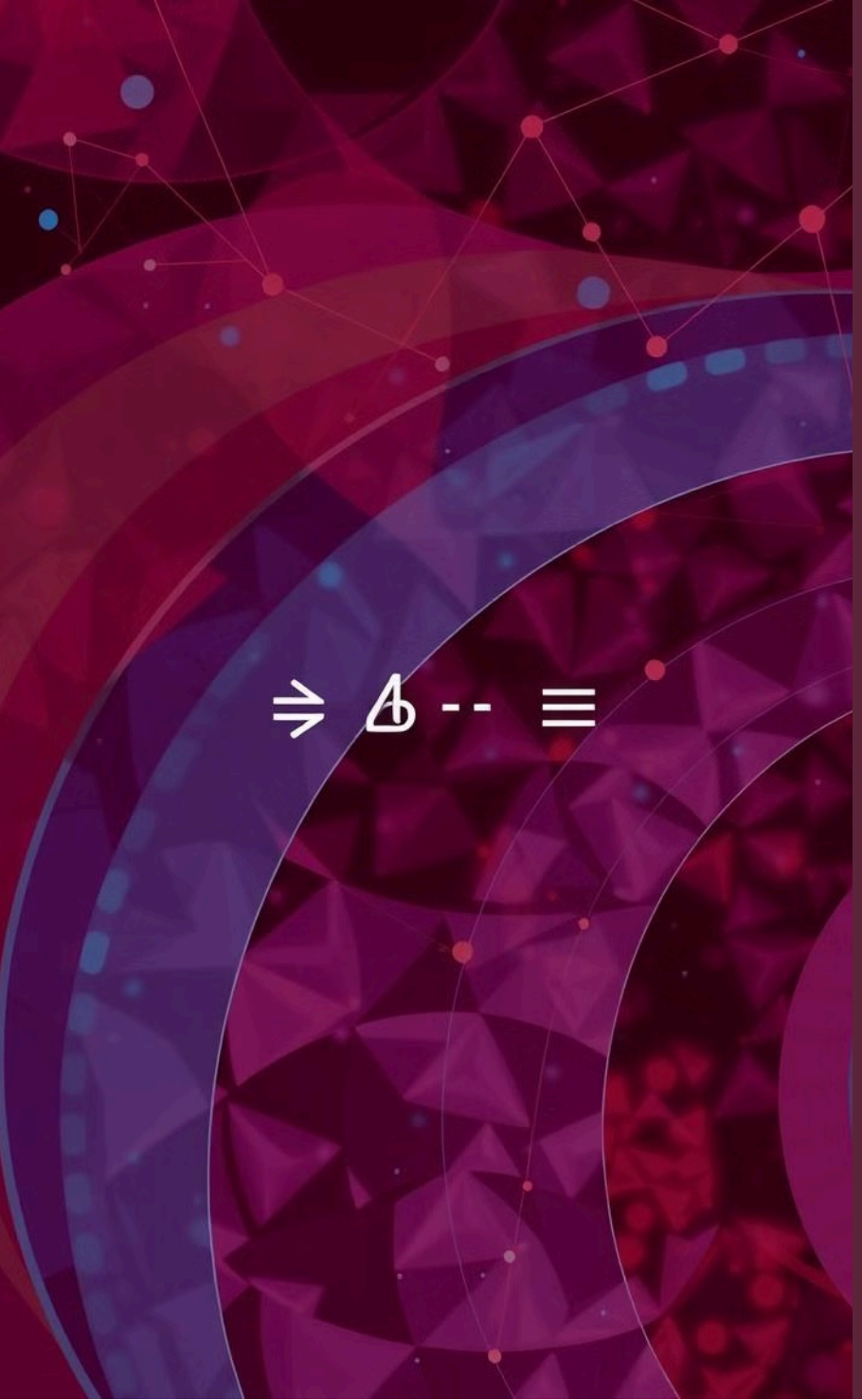
Ứng Dụng Rộng Rãi

Blockchain, bảo mật giao dịch, mở rộng quy mô.

An Toàn Lượng Tử

Không phụ thuộc vào giả định bảo mật yếu.

Made with Gamma



Quy Trình Hoạt Động Của zk-STARKs

Tính toán được biểu diễn dưới dạng một chuỗi trạng thái. Chuỗi trạng thái được chuyển đổi thành một đa thức. Người chứng minh tạo bằng chứng rằng chuỗi trạng thái thỏa mãn các ràng buộc tính toán.

1

Biểu Diễn Tính Toán

Chuỗi trạng thái hoặc bước thực thi chương trình.

2

Cam Kết Với Đa Thức

Chuyển đổi chuỗi trạng thái thành một đa thức.

3

Tạo Bằng Chứng

Chứng minh chuỗi trạng thái thỏa mãn các ràng buộc.

4

Xác Minh Bằng Chứng

Kiểm tra tính hợp lệ mà không cần biết chi tiết.

Made with Gamma

STARK Proofs Là Gì?

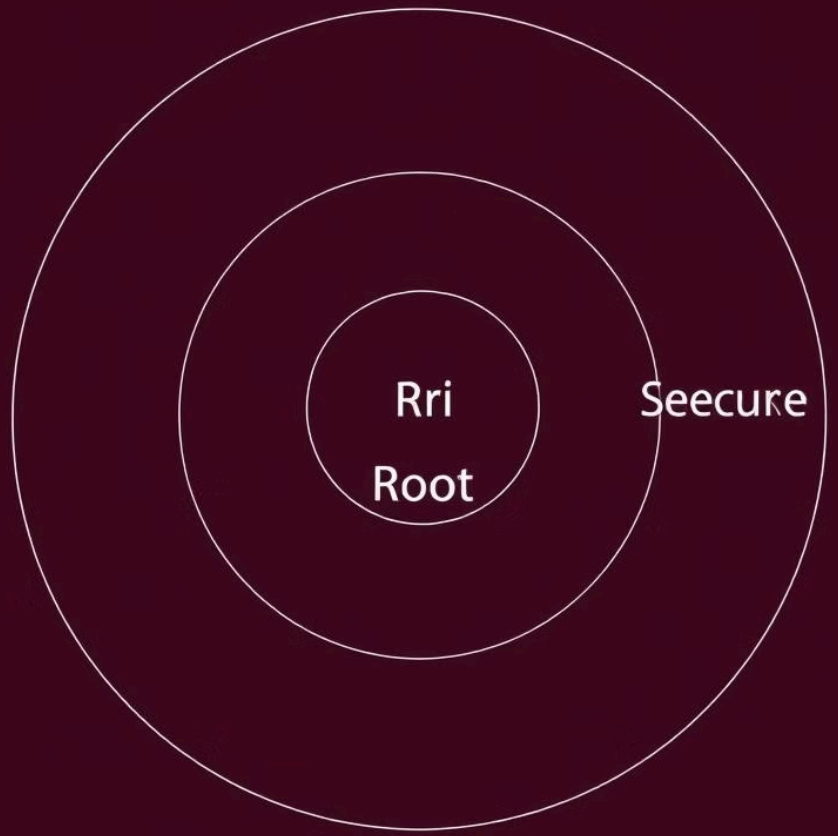
STARK Proofs là nền tảng của zk-STARKs. Nó giúp chứng minh tính toán mà không cần Trusted Setup. Chúng sử dụng FRI Commitment Scheme để cam kết với dữ liệu một cách an toàn.

Không Cần Trusted Setup

Chứng Minh Tính Toán

FRI Commitment Scheme

Made with Gamma



FRI Commitment Scheme Hoạt Động Như Thế Nào?

Chuỗi trạng thái được chuyển đổi thành một đa thức. FRI kiểm tra xem đa thức có bậc thấp không bằng cách giảm dần độ bậc. Người kiểm tra kiểm tra tính hợp lệ của cam kết mà không cần biết nội dung đa thức.

1 **Cam Kết Với Đa Thức**

2 **Giảm Độ Bậc Đa Thức**

3 **Xác Minh Bằng Chứng**

Made with Gamma

An Toàn Hơn 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 này dễ bị phá vỡ bởi máy tính lượng tử.

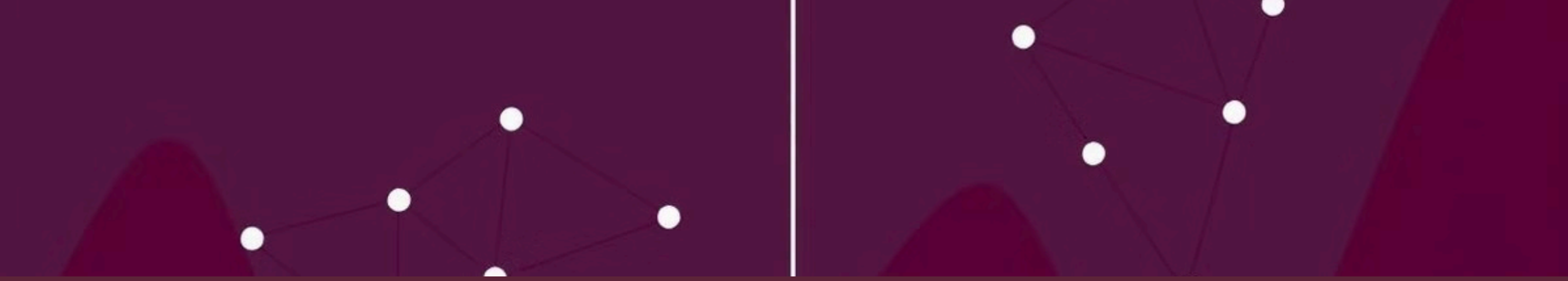
zk-SNARKs

Dựa vào logarithm rời rạc (Elliptic Curve). Không an toàn trước máy tính lượng tử.

zk-STARKs

Dựa vào mã Reed-Solomon. An toàn trước máy tính lượng tử.

Made with Gamma



So Sánh zk-STARKs Và zk-SNARKs

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.

Tiêu chí	zk-STARKs	zk-SNARKs
Yêu cầu Trusted Setup	Không cần	Cần
Kích thước bằng chứng	Lớn	Nhỏ
Tốc độ xác minh	Chậm hơn	Nhanh hơn
An toàn lượng tử	Có	Không

Made with Gamma

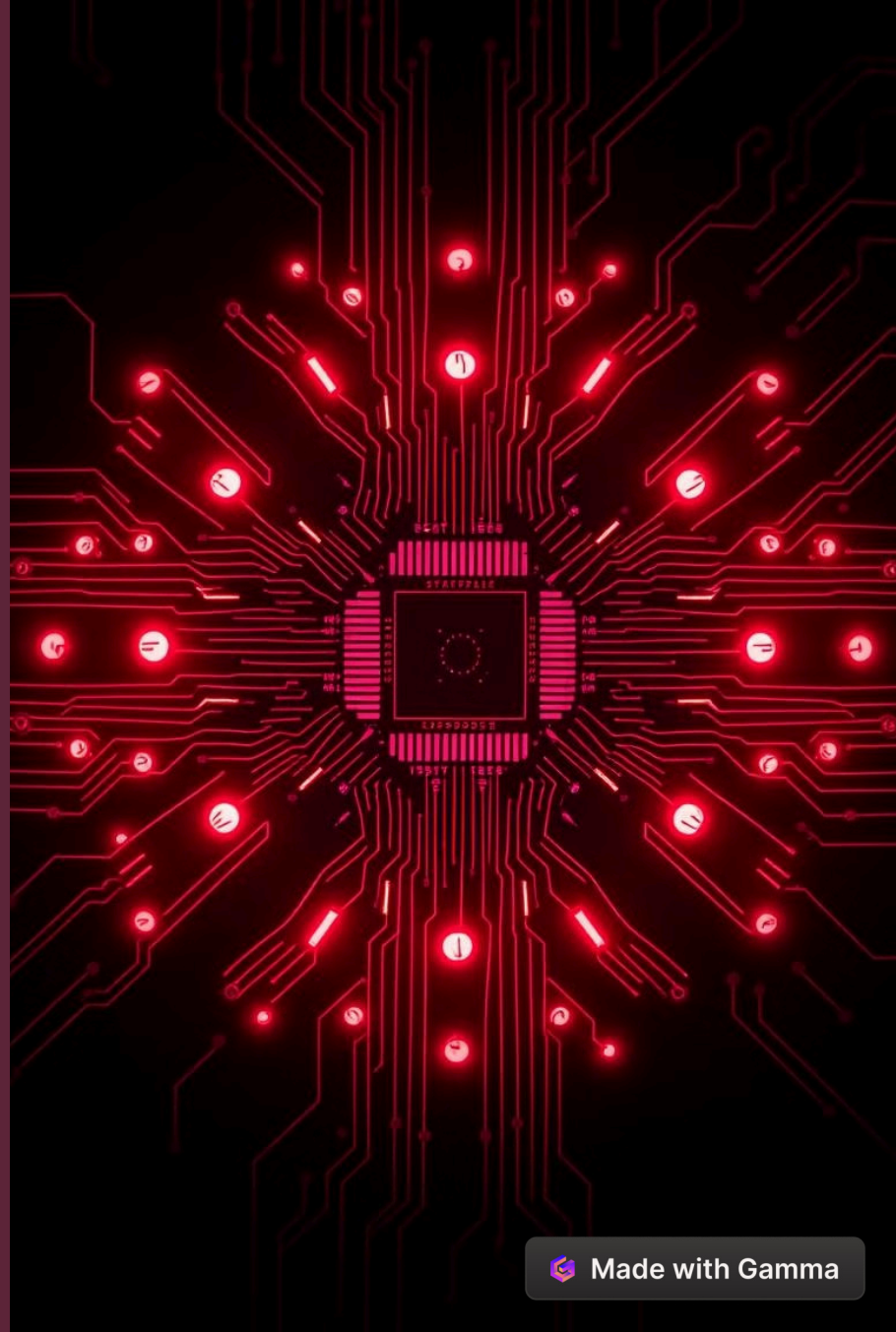
Ưu Điểm Của zk-STARKs

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.

Không Cần Trusted Setup

Bảo Mật Cao

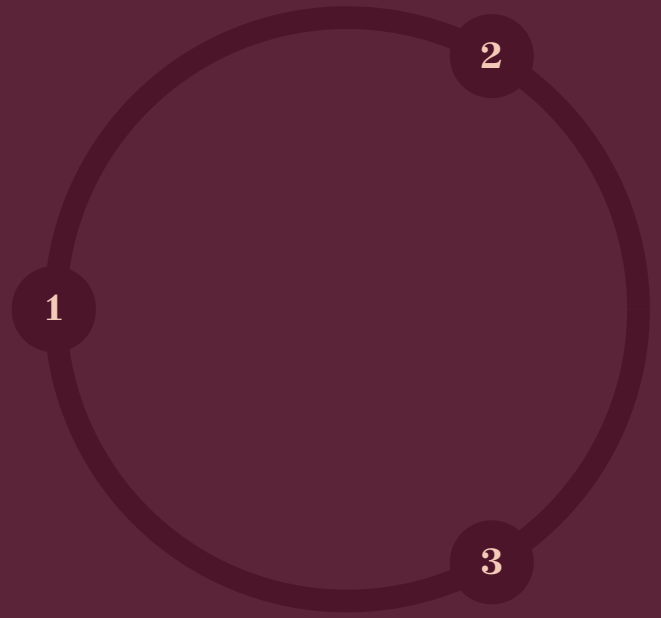
Minh Bạch



Made with Gamma

Nhược Điểm Của zk-STARKs

zk-STARKs có kích thước bằng chứng lớn hơn và tốc độ xác minh chậm hơn so với zk-SNARKs. Tuy nhiên, đổi lại là bảo mật cao hơn và không cần Trusted Setup.



Kích Thước Lớn

Bằng chứng lớn hơn zk-SNARKs.

Tốc Độ Chậm

Xác minh chậm hơn zk-SNARKs.

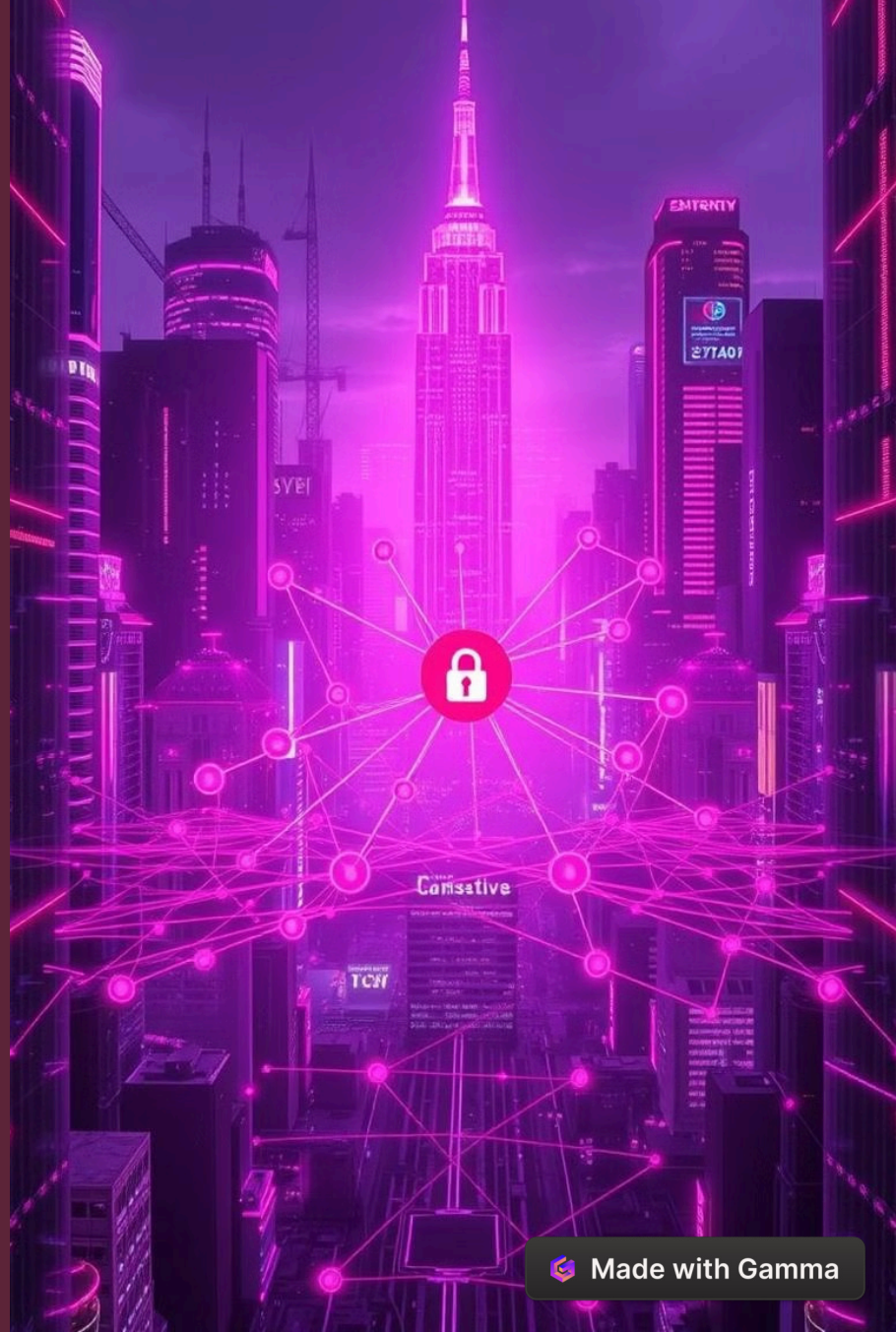
Bảo Mật Cao

An toàn trước máy tính lượng tử.

Made with Gamma

Kết Luận

zk-STARKs là một giao thức Zero-Knowledge Proofs không cần Trusted Setup. Nó an toàn hơn zk-SNARKs trước máy tính lượng tử. Bài tiếp theo: Bulletproofs – Zero-Knowledge Proof Không Cần Trusted Setup.



Made with Gamma