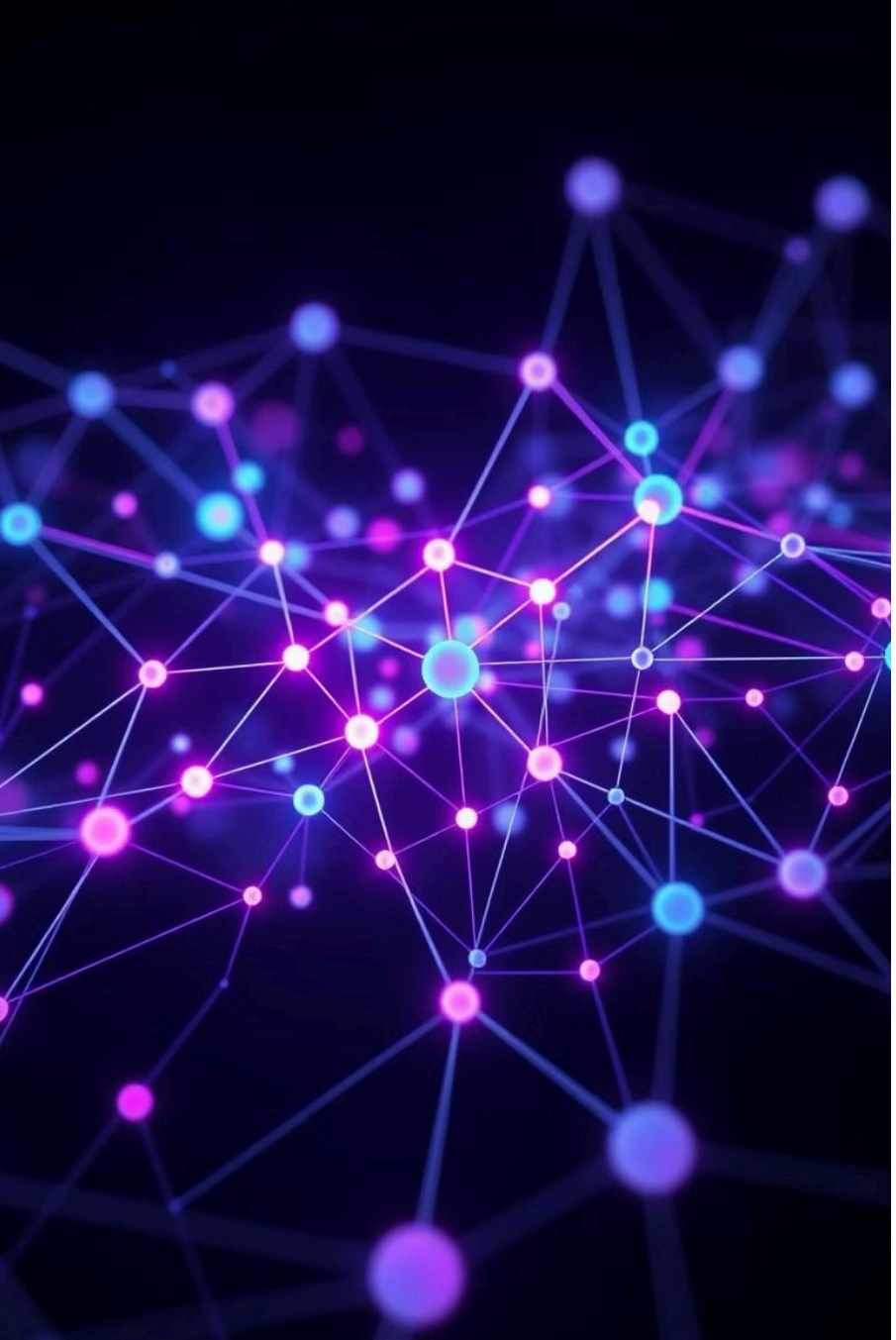


Zero-Knowledge Proof: Interactive vs Non-Interactive

Tìm hiểu về Interactive vs Non-Interactive trong Zero-Knowledge Proofs (ZKP). So sánh Fiat-Shamir Heuristic và Interactive truyền thống. ZKP là đột phá trong mật mã học, cho phép chứng minh mà không tiết lộ thông tin chi tiết.

Chứng Minh Tương Tác (Interactive Proofs)

Định nghĩa

Yêu cầu trao đổi thông tin qua nhiều vòng giữa người chứng minh và người kiểm tra.

1. Người chứng minh gửi thông điệp đầu tiên.
2. Người kiểm tra phản hồi bằng thách thức ngẫu nhiên.
3. Người chứng minh trả lời thách thức.

Ví dụ: Alibaba's Cave

Người chứng minh (Peggy) vào hang có hai lối đi. Người kiểm tra (Victor) yêu cầu Peggy xuất hiện ở lối đi ngẫu nhiên.

Chứng Minh Không Tương Tác (Non-Interactive Proofs)

1

Định nghĩa

Loại bỏ sự trao đổi trực tiếp. Người chứng minh tạo bằng chứng duy nhất để xác minh.

2

Cách hoạt động

Người chứng minh tạo bằng chứng dựa trên thông tin bí mật. Người kiểm tra xác minh mà không cần trao đổi thêm.

3

Ứng dụng

Phù hợp với blockchain và hệ thống phân tán.

Ví dụ: zk-SNARKs & zk-STARKs

zk-SNARKs

Sử dụng cặp ghép elliptic curve. Yêu cầu thiết lập tin cậy. Dùng trong Zcash, zkSync, Polygon zkEVM.

zk-STARKs

Không cần thiết lập tin cậy, dựa vào mã hóa hash. Bảo mật hơn zk-SNARKs. Dùng trong StarkNet.

Fiat-Shamir Heuristic

1

Bước 1

Người chứng minh tạo thông điệp đầu tiên.

2

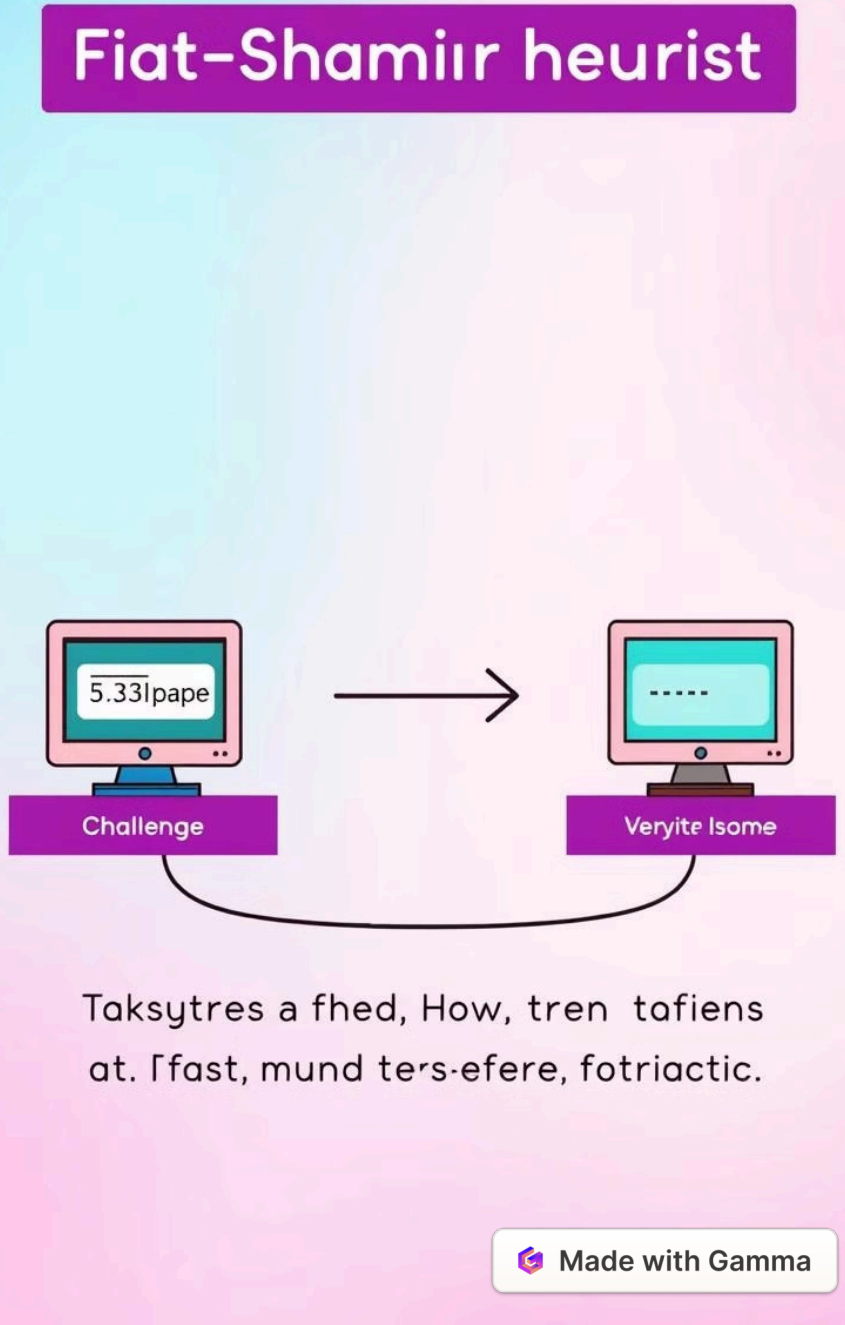
Bước 2

Tự tạo thách thức bằng cách băm thông điệp đầu tiên: c = H(m).

3

Bước 3

Tiếp tục quy trình chứng minh như bình thường.



1. Compmturative efficient

1. Saft a abcol

Fiat-Shamir vs Interactive

Tiêu chí	Fiat-Shamir Heuristic	Interactive
Số lần giao tiếp	Không cần	Cần nhiều vòng
Hiệu suất	Cao	Thấp
Giả định bảo mật	Dựa vào random oracle	Không cần

Ưu và Nhược Điểm

Fiat-Shamir Heuristic

- Ưu: Tăng tốc độ, khả năng mở rộng.
- Nhược: Dựa trên giả định mạnh về bảo mật.

Interactive

- Ưu: Không cần giả định mạnh.
- Nhược: Hiệu suất thấp, cần đồng bộ hóa.

Ứng Dụng Thực Tế

Blockchain

Xác minh giao dịch nhanh chóng và an toàn.

Bảo Mật Dữ Liệu

Chứng minh tính hợp lệ mà không tiết lộ dữ liệu.

Xác Thực Danh Tính

Xác minh danh tính mà không lộ thông tin cá nhân.

Kết Luận

Chứng minh tương tác và không tương tác là hai loại ZKP quan trọng. Fiat-Shamir Heuristic giúp chuyển đổi chứng minh tương tác thành không tương tác. Tạo nền tảng cho zk-SNARKs và zk-STARKs, ứng dụng trong blockchain.

Tiếp Theo

Tìm hiểu sâu hơn

Polynomial Commitments – Kỹ Thuật Lõi Của SNARKs & STARKs.

Nghiên cứu

Các giao thức ZKP mới và ứng dụng tiềm năng.

Thực hành

Xây dựng ứng dụng ZKP đơn giản.