Zero-Knowledge Proof: Interactive vs Non-Interactive

Meta Description

Tìm hiểu Interactive & Non-Interactive Proofs trong Zero-Knowledge Proofs (ZKP). So sánh Fiat-Shamir Heuristic & chứng minh tương tác truyền thống!

Giới Thiệu

Zero-Knowledge Proofs (ZKP) là một đột phá trong mật mã học, cho phép chứng minh một tuyên bố mà không tiết lộ thông tin chi tiết. Ra đời từ bài báo khoa học năm 1985 của **Shafi Goldwasser, Silvio Micali, và Charles Rackoff**, ZKP đã trở thành công nghệ cốt lõi trong bảo mật blockchain và Web3.

Một trong những phân loại quan trọng của ZKP là **chứng minh tương tác (Interactive Proofs)** và **chứng minh không tương tác (Non-Interactive Proofs)**. Vậy sự khác biệt giữa hai mô hình này là gì? Fiat-Shamir Heuristic đóng vai trò gì trong việc chuyển đổi từ tương tác sang không tương tác? Hãy cùng tìm hiểu chi tiết.

Key Takeaways

✅ **Chứng minh tương tác (Interactive Proofs)** yêu cầu nhiều vòng trao đổi giữa người chứng minh (Prover) và người kiểm tra (Verifier).
✅ **Chứng minh không tương tác (Non-Interactive Proofs)** giúp loại bỏ sự trao đổi, cho phép xác minh mà không cần tương tác thực tế.
✅ **Fiat-Shamir Heuristic** giúp biến chứng minh tương tác thành không tương tác bằng cách sử dụng hàm băm thay cho thách thức ngẫu nhiên từ người kiểm tra.
✅ **zk-SNARKs và zk-STARKs** là các giao thức không tương tác phổ biến trong blockchain, cải thiện tốc độ và khả năng mở rộng.
✅ **Fiat-Shamir Heuristic tuy hiệu quả nhưng phụ thuộc vào giả định random oracle**, trong khi chứng minh tương tác truyền thống đảm bảo tính bảo mật chặt chẽ hơn.

Chứng Minh Tương Tác (Interactive Proofs) Là Gì?

Chứng minh tương tác (Interactive Proofs) là một loại Zero-Knowledge Proof trong đó **người chứng minh (Prover) và người kiểm tra (Verifier) phải trao đổi thông tin qua nhiều vòng lặp** để xác thực một tuyên bố.

- **Cách hoạt động:**

1. **Người chứng minh gửi một thông điệp đầu tiên** chứa một phần của bằng chứng.
2. **Người kiểm tra phản hồi bằng một thách thức ngẫu nhiên** (random challenge).
3. **Người chứng minh trả lời thách thức**, chứng minh rằng họ biết thông tin bí mật.

4. **Người kiểm tra xác minh bằng chứng** và kết luận tính đúng đắn.

Ví dụ: Bài toán Alibaba's Cave

Bài toán **Alibaba's Cave** là một ví dụ kinh điển mô phỏng chứng minh tương tác:

1️⃣ **Người chứng minh (Peggy)** vào một hang động có hai lối đi A và B, với một cánh cửa bí mật ở giữa.
2️⃣ **Người kiểm tra (Victor)** đứng bên ngoài và yêu cầu Peggy xuất hiện ở một lối đi ngẫu nhiên.
3️⃣ Nếu Peggy biết mật khẩu mở cửa, cô có thể đi qua và xuất hiện đúng lối Victor yêu cầu.
4️⃣ Nếu thử nghiệm lặp lại nhiều lần và Peggy luôn thành công, Victor tin rằng cô biết mật khẩu mà không cần thấy nó.

👉 **Ứng dụng:** Chứng minh tương tác thường được sử dụng trong các hệ thống bảo mật yêu cầu xác minh trực tiếp, chẳng hạn như **xác thực danh tính** và **bảo mật trong giao dịch ngân hàng**.

Chứng Minh Không Tương Tác (Non-Interactive Proofs) Là Gì?

Chứng minh không tương tác (Non-Interactive Proofs) tác giúp loại bỏ sự trao đổi trực tiếp giữa người chứng minh và người kiểm tra, thay vào đó **người chứng minh tạo một bằng chứng duy nhất mà bất kỳ ai cũng có thể xác minh** mà không cần thêm thông tin.

- **Cách hoạt động:**

1. **Người chứng minh tạo ra bằng chứng** dựa trên thông tin bí mật của họ.
2. **Người kiểm tra nhận bằng chứng và xác minh tính đúng đắn** mà không cần trao đổi thêm.

Ví dụ: zk-SNARKs & zk-STARKs

- **zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge)**

  - Sử dụng các cặp ghép elliptic curve để tạo bằng chứng nhỏ gọn.
  - Yêu cầu thiết lập tin cậy (Trusted Setup).
  - Được sử dụng trong **Zcash, zkSync, Polygon zkEVM**.

- **zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge)**

  - Không cần thiết lập tin cậy, dựa vào mã hóa hash.
  - Bảo mật hơn zk-SNARKs trước máy tính lượng tử.
  - Được sử dụng trong **StarkNet**.

👉 **Ứng dụng:** Chứng minh không tương tác phù hợp với **blockchain và hệ thống phân tán** vì nó giúp xác minh nhanh mà không cần tương tác thực tế.

Fiat-Shamir Heuristic: Chuyển Đổi Từ Chứng Minh Tương Tác Sang Không Tương Tác

Fiat-Shamir Heuristic là một kỹ thuật mật mã giúp biến một giao thức **chứng minh tương tác thành không tương tác** bằng cách sử dụng **hàm băm mật mã** thay cho thách thức ngẫu nhiên từ người kiểm tra.

🔹 **Quy trình:**

1. **Người chứng minh tạo ra thông điệp đầu tiên**, như trong chứng minh tương tác.
2. **Thay vì nhận thách thức từ người kiểm tra, họ tự tạo thách thức bằng cách băm thông điệp đầu tiên**: c = H(m) (với H là hàm băm, m là thông điệp đầu tiên).
3. **Tiếp tục quy trình chứng minh như bình thường**, sử dụng c thay vì chờ phản hồi từ người kiểm tra.

👉 **Ứng dụng:** Fiat-Shamir Heuristic giúp tạo **chứng minh không tương tác** mà không cần giao tiếp, phù hợp cho blockchain.

So Sánh Fiat-Shamir Heuristic và Chứng Minh Tương Tác

Tiêu chí	Fiat-Shamir Heuristic (Non-Interactive)	Chứng minh tương tác truyền thống
Số lần giao tiếp	Không cần giao tiếp thực tế	Cần nhiều vòng trao đổi thông tin
Hiệu suất	Cao, phù hợp cho blockchain	Thấp, cần đồng bộ hóa
Giả định bảo mật	Dựa vào random oracle, cần hàm băm an toàn	Không cần giả định mạnh
Kích thước bằng chứng	Lớn hơn, chứa toàn bộ thông tin	Nhỏ hơn, thông tin chia nhỏ theo vòng
Yêu cầu thiết lập	Có thể cần (như zk-SNARKs)	Không cần thiết lập tin cậy

👉 **Tóm lại:** Fiat-Shamir Heuristic giúp tăng tốc độ và khả năng mở rộng, nhưng dựa trên giả định mạnh hơn về bảo mật so với chứng minh tương tác truyền thống.

Kết Luận

Chứng minh tương tác và không tương tác là hai loại Zero-Knowledge Proof quan trọng, mỗi loại có ưu và nhược điểm riêng. **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.

💡 **Bài tiếp theo:** Polynomial Commitments – Kỹ Thuật Lõi Của SNARKs & STARKs 🚀