



# Zero-Knowledge Proof (ZKP) Là Gì? Nguyên Lý & Ứng Dụng

Zero-Knowledge Proof (ZKP) giúp chứng minh một tuyên bố đúng mà không tiết lộ thông tin. Công nghệ này có nguyên lý toán học phức tạp, cách hoạt động độc đáo và ứng dụng rộng rãi trong blockchain, DeFi, Web3, bảo mật và AI. ZKP đang trở thành một nền tảng quan trọng trong bảo mật dữ liệu.

# Zero-Knowledge Proof (ZKP) là gì?

## Định nghĩa

Zero-Knowledge Proof (ZKP) là một giao thức mật mã cho phép một bên (**Prover** - người chứng minh) thuyết phục một bên khác (**Verifier** - người kiểm tra) rằng một tuyên bố là đúng, mà không tiết lộ bất kỳ thông tin nào ngoài sự thật của tuyên bố đó.

## Lịch sử

Công nghệ này được giới thiệu lần đầu vào năm 1985 trong bài báo khoa học [The Knowledge Complexity of Interactive Proof Systems](#) của Shafi Goldwasser, Silvio Micali và Charles Rackoff.



# Ví dụ đơn giản về ZKP

Hãy tưởng tượng bạn muốn chứng minh với bạn mình rằng bạn biết mật khẩu mở một két sắt, nhưng không muốn tiết lộ mật khẩu. Nếu bạn có thể làm điều này mà người bạn vẫn tin tưởng bạn, thì đó chính là **Zero-Knowledge Proof**.

## Bảo mật giao dịch blockchain

(\_zk-SNARKs, zk-STARKs trên Ethereum, zkSync, StarkNet\_)

## Xác thực danh tính

Xác thực danh tính mà không tiết lộ thông tin cá nhân (\_Polygon ID, Worldcoin\_)

## Thanh toán ẩn danh

Thanh toán ẩn danh trên blockchain (\_Tornado Cash, Aztec Protocol\_)

# ZKP hoạt động như thế nào?

## Interactive Zero-Knowledge Proofs (ZKP tương tác)

Trong mô hình này, **người chứng minh và người kiểm tra phải trao đổi nhiều lần** để xác minh tính đúng đắn của một tuyên bố. Đây là mô hình được minh họa rõ nhất qua **bài toán Alibaba's Cave**.

## Non-Interactive Zero-Knowledge Proofs (ZKP không tương tác)

Người chứng minh tạo ra **một bằng chứng duy nhất**, và người kiểm tra có thể xác minh mà không cần trao đổi thêm. Công nghệ **zk-SNARKs, zk-STARKs** sử dụng phương pháp này để tối ưu hóa bảo mật và tốc độ xác minh.

# Ba tính chất chính của ZKP

1

Hoàn chỉnh  
(Completeness)

Nếu tuyên bố là đúng và cả hai bên đều trung thực, thì **người kiểm tra luôn chấp nhận bằng chứng**.

2

Chính xác  
(Soundness)

Nếu tuyên bố là **sai**, thì không có kẻ gian lận nào có thể thuyết phục người kiểm tra rằng nó đúng, trừ khi có xác suất cực kỳ nhỏ.

3

Không tiết lộ kiến thức (Zero-Knowledge)

Người kiểm tra không học được bất kỳ thông tin nào khác ngoài sự thật rằng tuyên bố là đúng.



# Ứng dụng đầu tiên: Bài toán Alibaba's Cave

Bài toán **\*\*Alibaba's Cave\*\*** là một ví dụ kinh điển để minh họa cách Zero-Knowledge Proofs hoạt động.

1

## Cấu trúc bài toán

Có một **hang động** hình **vòng tròn**, với **hai lối vào** (A và B). Ở giữa hang là **một cánh cửa bí mật**, chỉ có thể mở bằng một mật khẩu.

2

## Peggy và Victor

Peggy (**người chứng minh**) muốn chứng minh rằng cô biết mật khẩu để mở cửa, nhưng không muốn tiết lộ mật khẩu đó với Victor (**người kiểm tra**).



# Quy trình chứng minh trong Alibaba's Cave



## Bước 1

Peggy chọn ngẫu nhiên đi vào lối A hoặc B.

## Bước 2

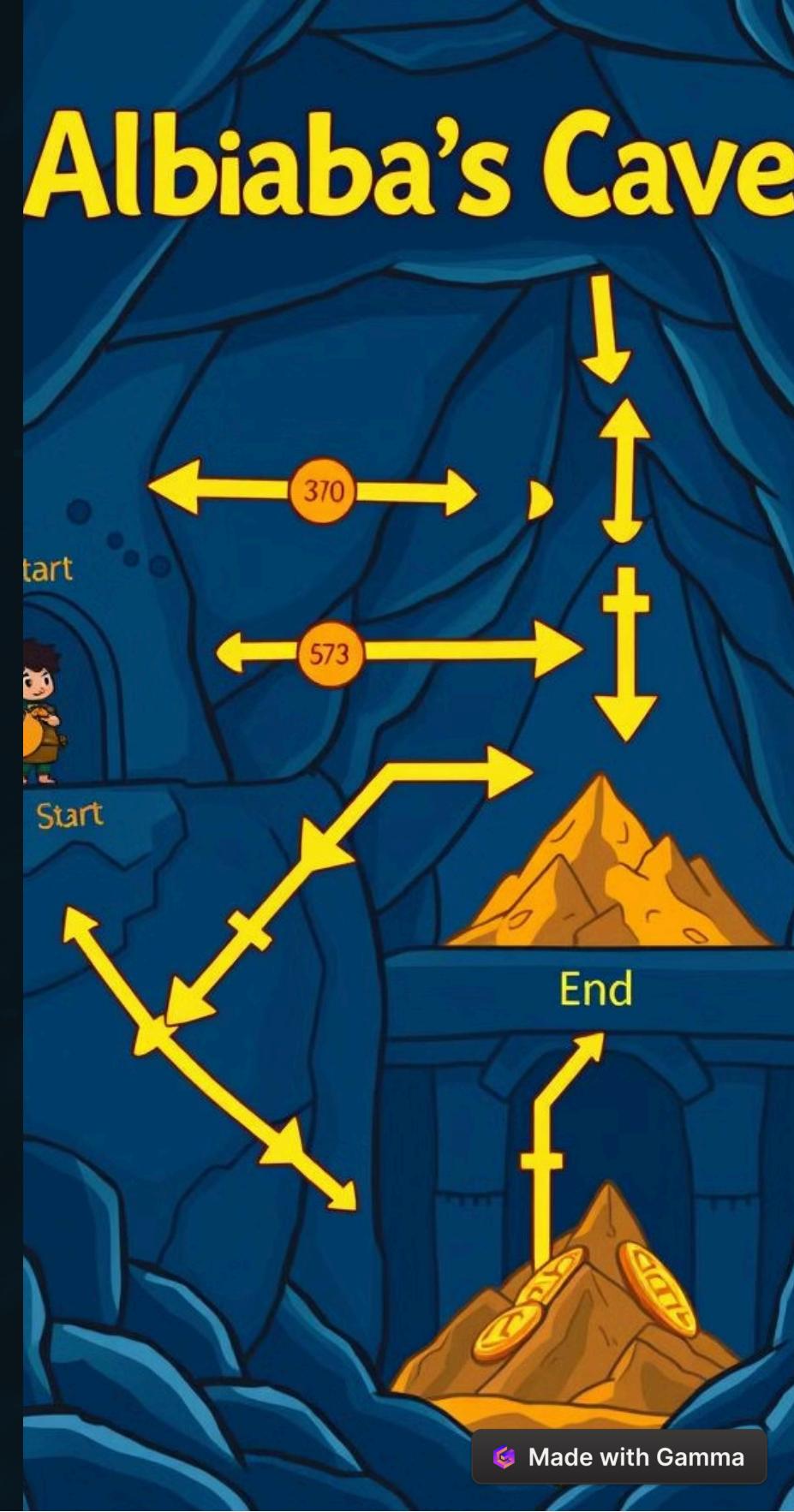
Victor đứng bên ngoài và gọi tên lối mà ông muốn Peggy đi ra (A hoặc B).

## Bước 3

Nếu Peggy **thực sự biết mật khẩu**, cô có thể mở cửa và đi ra đúng lối mà Victor yêu cầu.

## Bước 4

Nếu Peggy **không biết mật khẩu**, cô có **50% cơ hội đoán đúng**. Nếu lặp lại quy trình **nhiều lần**, xác suất cô gian lận thành công sẽ giảm xuống gần bằng 0.





# Phân tích tính chất ZKP trong Alibaba's Cave

Tính chất	Giải thích qua Alibaba's Cave
Hoàn chỉnh	Nếu Peggy biết mật khẩu, cô luôn <b>có thể mở cửa</b> và đi ra đúng lối Victor yêu cầu.
Chính xác	Nếu Peggy không biết mật khẩu, cô chỉ có <b>50% cơ hội đoán đúng</b> mỗi lần. Nếu lặp lại nhiều lần, xác suất gian lận thành công sẽ rất nhỏ.
Không kiến thức	Victor chỉ biết Peggy biết mật khẩu, nhưng không biết mật khẩu thực tế.

# Kết luận

Zero-Knowledge Proofs (ZKP) là một trong những công nghệ bảo mật quan trọng nhất, giúp **chứng minh một tuyên bố là đúng mà không tiết lộ thông tin thực tế**.



Hai loại chính

Interactive & Non-  
Interactive



Ba tính chất

Hoàn chỉnh, Chính  
xác, Không tiết lộ  
kiến thức



Minh họa

Bài toán Alibaba's  
Cave



Ứng dụng

Blockchain, bảo  
mật danh tính,  
thanh toán ẩn  
danh và AI

# Tiếp theo

Bạn muốn đi sâu hơn vào toán học đằng sau ZKP? Hãy đọc ngay [bài viết về Nhóm Số Học & Logarithm Rời Rạc](#) để hiểu nền tảng toán học của công nghệ này!

