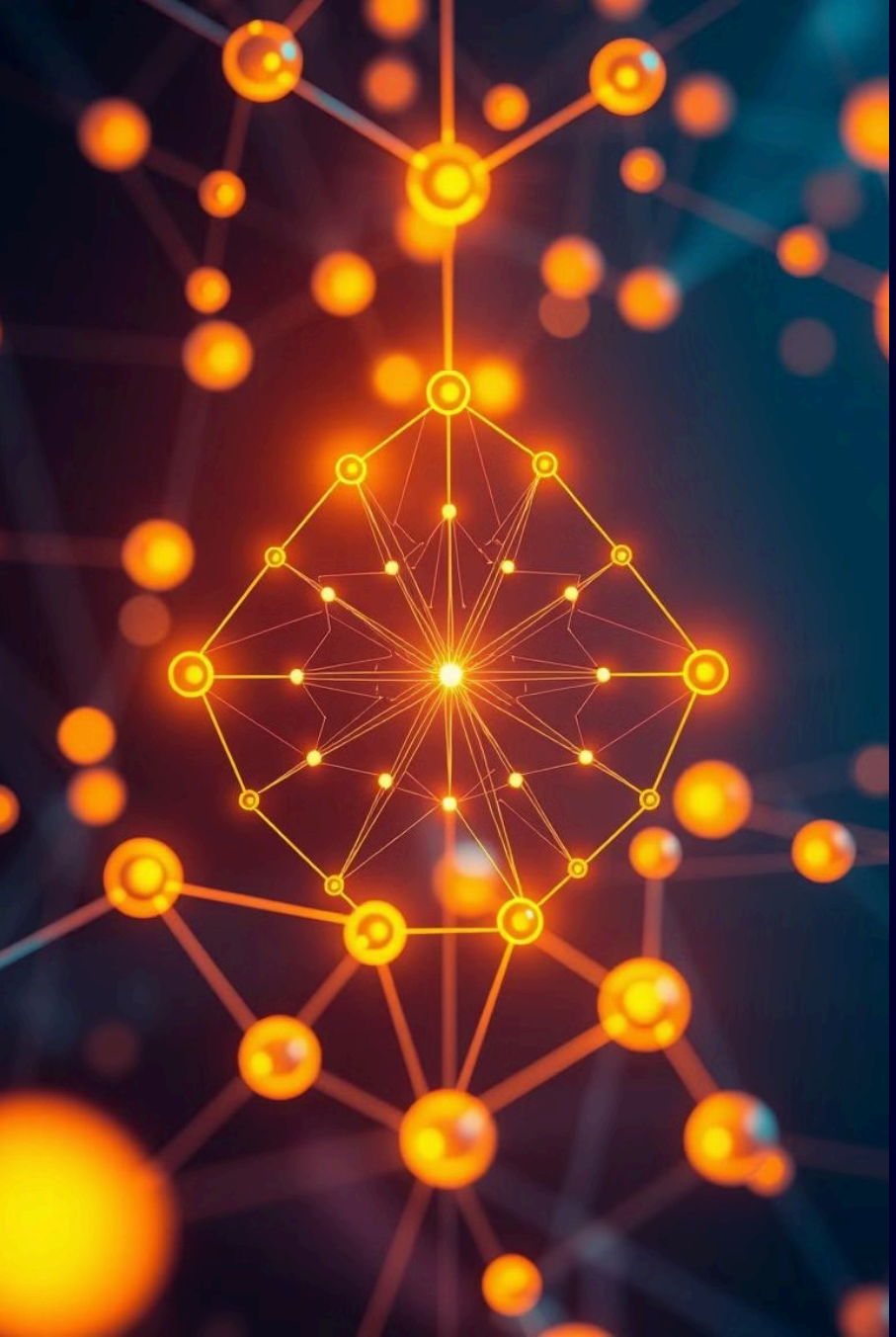


zk-SNARKs: Giao Thức Zero-Knowledge & Trusted Setup

Trong hệ thống **Zero-Knowledge Proofs (ZKP)**, **zk-SNARKs** (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) là một trong những giao thức quan trọng nhất, giúp chứng minh một tuyên bố mà không tiết lộ bất kỳ thông tin nào.

zk-SNARKs được ứng dụng rộng rãi trong **blockchain, bảo mật giao dịch, và xác minh tính toàn vẹn của dữ liệu** mà không cần chia sẻ nội dung. Một số hệ thống nổi bật sử dụng zk-SNARKs bao gồm **Zcash, Filecoin, và Ethereum Layer 2**.

Giới Thiệu Về zk-SNARKs

zk-SNARKs là một giao thức **Zero-Knowledge Proofs (ZKP)** không tương tác, nghĩa là người chứng minh (Prover) có thể tạo một bằng chứng duy nhất để người kiểm tra (Verifier) xác minh mà không cần trao đổi thông tin thêm.

- **Zero-Knowledge**: Người kiểm tra không học được gì ngoài sự thật của tuyên bố.
- **Succinct**: Bằng chứng có kích thước nhỏ và thời gian kiểm tra nhanh.
- **Non-Interactive**: Chỉ cần một thông điệp duy nhất, không yêu cầu tương tác.

zk-SNARKs nhanh hơn so với các giao thức ZKP khác như zk-STARKs, nhưng yêu cầu **Trusted Setup**, một điểm yếu bảo mật quan trọng.

Zcash

Bảo mật giao dịch mà không tiết lộ số tiền hoặc địa chỉ.

Ethereum Layer 2

Giúp mở rộng quy mô bằng zk-Rollups.

Filecoin

Xác minh lưu trữ dữ liệu mà không cần tiết lộ nội dung.

Cơ Chế zk-SNARKs: R1CS (Rank-1 Constraint System)

Một trong những bước quan trọng trong zk-SNARKs là **chuyển đổi bài toán tính toán thành hệ phương trình đại số**. liên kết không xác định **(Rank-1 Constraint System)** là cách tiếp cận phổ biến nhất để làm điều này.

R1CS giúp chuyển đổi các bài toán phức tạp thành hệ phương trình dễ dàng xử lý bằng zk-SNARKs.

1 **Chuyển đổi chương trình thành mạch số học**

Biểu diễn các phép tính cộng, nhân bằng các cổng logic.

2 **Chuyển đổi thành hệ ràng buộc R1CS**

Sử dụng cổng nhân và cổng cộng để biểu diễn các ràng buộc.

3 **Chuyển đổi R1CS thành Quadratic Arithmetic Program (QAP)**

QAP là dạng mà SNARKs có thể sử dụng để tạo bằng chứng.

So Sánh Groth16, PLONK, Marlin

Groth16, PLONK và Marlin là ba thuật toán zk-SNARKs phổ biến, mỗi thuật toán có những ưu nhược điểm riêng.

Groth16 có hiệu suất cao, nhưng cần **Trusted Setup**, ít linh hoạt. **PLONK** linh hoạt, không cần setup lại khi thay đổi bài toán, nhưng bằng chứng lớn hơn. **Marlin** giống Groth16 nhưng có setup phi tập trung, giảm rủi ro bảo mật.

Thuật toán	Kích thước bằng chứng	Thời gian kiểm tra	Yêu cầu Trusted Setup	Linh hoạt
Groth16	Nhỏ (~96 bytes)	Nhanh	✅ Có	❌ Thấp
PLONK	Trung bình (~384-480 bytes)	Trung bình	⚠️ Có hoặc không	✅ Cao
Marlin	Nhỏ (~96 bytes)	Nhanh	✅ Phi tập trung	✅ Trung bình

Trusted Setup & Những Rủi Ro Bảo Mật

Trusted Setup là giai đoạn tạo tham số khởi tạo cho zk-SNARKs. Nếu các tham số này bị xâm phạm, có thể dẫn đến bằng chứng giả.

Nếu khóa bí mật bị lộ, kẻ tấn công có thể tạo bằng chứng giả mà vẫn được hệ thống chấp nhận. Cần tin tưởng vào quy trình setup, nếu một bên độc hại tham gia, có thể phá vỡ bảo mật.

Lý do cần Trusted Setup

- Đảm bảo tính toán trên cặp ghép elliptic curve.
- Tăng hiệu suất bằng cách sử dụng Common Reference String (CRS).

Lỗ hổng bảo mật

- Nếu khóa bí mật bị lộ, kẻ tấn công có thể tạo bằng chứng giả.
- Cần tin tưởng vào quy trình setup.

Giảm Rủi Ro Bằng Multi-Party Computation (MPC)

Multi-Party Computation (MPC) là một phương pháp để giảm rủi ro trong Trusted Setup bằng cách cho phép nhiều người tham gia tạo khóa ngẫu nhiên. Không ai biết toàn bộ khóa bí mật, nhưng vẫn có rủi ro nếu một số người thông đồng.

zk-STARKs không cần Trusted Setup, nhưng bằng chứng lớn hơn.

1

Nhiều người tham gia

Tạo khóa ngẫu nhiên.

2

Không ai biết toàn bộ khóa

Bí mật được chia sẻ.

3

Vẫn có rủi ro

Nếu một số người thông đồng.

Kết Luận

zk-SNARKs là một công nghệ mạnh mẽ giúp xác minh thông tin mà không tiết lộ dữ liệu. **R1CS** giúp chuyển đổi tính toán thành hệ ràng buộc đại số để SNARKs có thể xử lý.

Groth16, PLONK, Marlin có ưu nhược điểm khác nhau, với Groth16 phổ biến nhưng yêu cầu Trusted Setup. **Trusted Setup** là điểm yếu bảo mật quan trọng, có thể bị xâm phạm nếu không thực hiện đúng.

Bảo mật

Tính toán

Xác minh

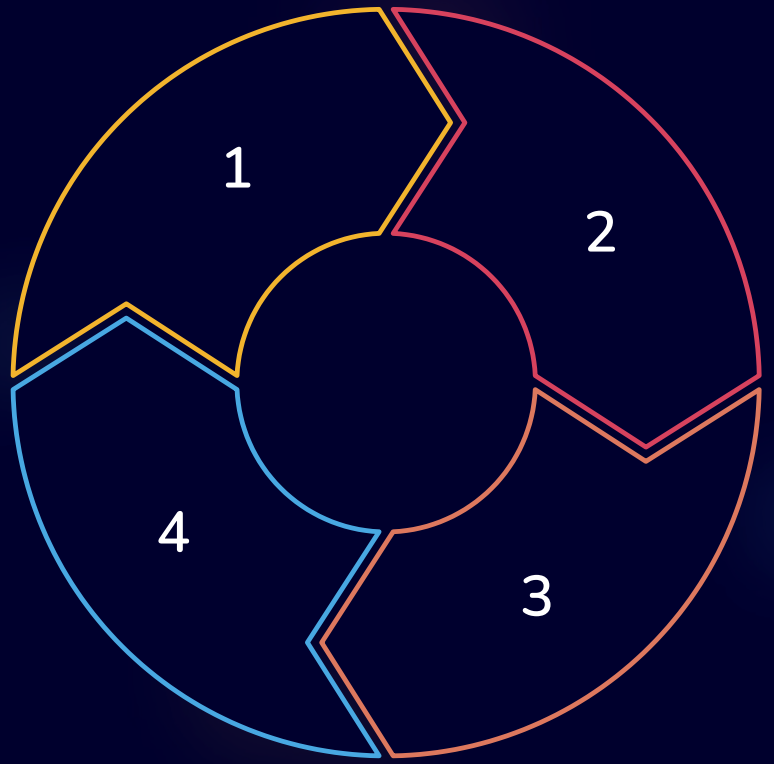
Ứng dụng của zk-SNARKs trong Zcash

Zcash sử dụng zk-SNARKs để bảo vệ quyền riêng tư của người dùng bằng cách cho phép họ thực hiện các giao dịch mà không tiết lộ thông tin về người gửi, người nhận hoặc số tiền giao dịch.

zk-SNARKs cho phép Zcash đạt được tính bảo mật cao mà không ảnh hưởng đến tính toàn vẹn của blockchain.

Giao dịch

Người dùng tạo giao dịch.



Chứng minh

zk-SNARKs tạo bằng chứng.

Bảo mật

Thông tin giao dịch được bảo vệ.

Xác minh

Mạng xác minh bằng chứng.

zk-SNARKs trong Ethereum Layer 2

Ethereum Layer 2 sử dụng zk-SNARKs để mở rộng quy mô mạng bằng cách xử lý các giao dịch ngoài chuỗi và chỉ gửi bằng chứng về tính hợp lệ của các giao dịch đó lên chuỗi chính.

zk-Rollups là một giải pháp Layer 2 phổ biến sử dụng zk-SNARKs để đạt được hiệu suất cao và bảo mật.

1

Giao dịch ngoài chuỗi

Xử lý giao dịch.

2

Tạo bằng chứng

zk-SNARKs tạo bằng chứng.

3

Xác minh trên chuỗi

Gửi bằng chứng lên chuỗi chính.

Giải pháp thay thế: zk-STARKs

zk-STARKs là một giải pháp thay thế cho zk-SNARKs không yêu cầu Trusted Setup, nhưng bằng chứng lớn hơn và thời gian xác minh lâu hơn.

zk-STARKs đang trở nên phổ biến hơn do tính bảo mật cao và khả năng chống lại các cuộc tấn công liên quan đến Trusted Setup.

10x	5x	0
Bằng chứng lớn hơn.	Thời gian xác minh lâu hơn.	Không cần Trusted Setup.