Ứng Dụng ZKP: Bảo Mật DeFi & Quyền Riêng Tư Blockchain

Zero-Knowledge Proofs (ZKP) cách mạng hóa bảo mật DeFi & quyền riêng tư. Khám phá các ứng dụng và tranh cãi pháp lý!

Giới Thiệu về ZKP trong DeFi

1 Vấn đề

Giao dịch trên blockchain công khai có thể bị theo dõi.

2 Giải pháp

ZKP giúp xác minh thông tin mà không tiết lộ dữ liệu.

3 Ứng dụng

Giao dịch riêng tư, vay mượn ẩn danh, DeFi an toàn hơn.

Tornado Cash - Giao Dịch Riêng Tư

Hoạt động

Giao thức phi tập trung giúp giao dịch ẩn danh trên Ethereum.

Sử dụng zk-SNARKs để bảo vệ quyền riêng tư.

Lợi ích

Bảo vệ quyền riêng tư, tránh bị theo dõi giao dịch.

Không yêu cầu bên thứ ba kiểm soát.

Tranh Cãi Về Tornado Cash

Lệnh Cấm

OFAC cấm vì cáo buộc liên quan đến rửa tiền.

Lạm Dụng

Bị lợi dụng để che giấu nguồn gốc tài sản.

Lo Ngại

Gây lo ngại về tính hợp pháp của giao thức quyền riêng tư.

Aztec Protocol - Hợp Đồng Thông Minh Bí Mật

Giao dịch ẩn danh

Không công khai số tiền hoặc danh tính.

Tích hợp DeFi

Vay mượn, giao dịch, staking không bị theo dõi.

Chứng minh hợp lệ

Dùng ZKP để chứng minh hợp đồng thông minh hợp lệ.

Shielded Pools - Giao Dịch Ẩn Danh

1

Gửi tài sản

Người dùng gửi tài sản vào pool.

2

Nhận cam kết

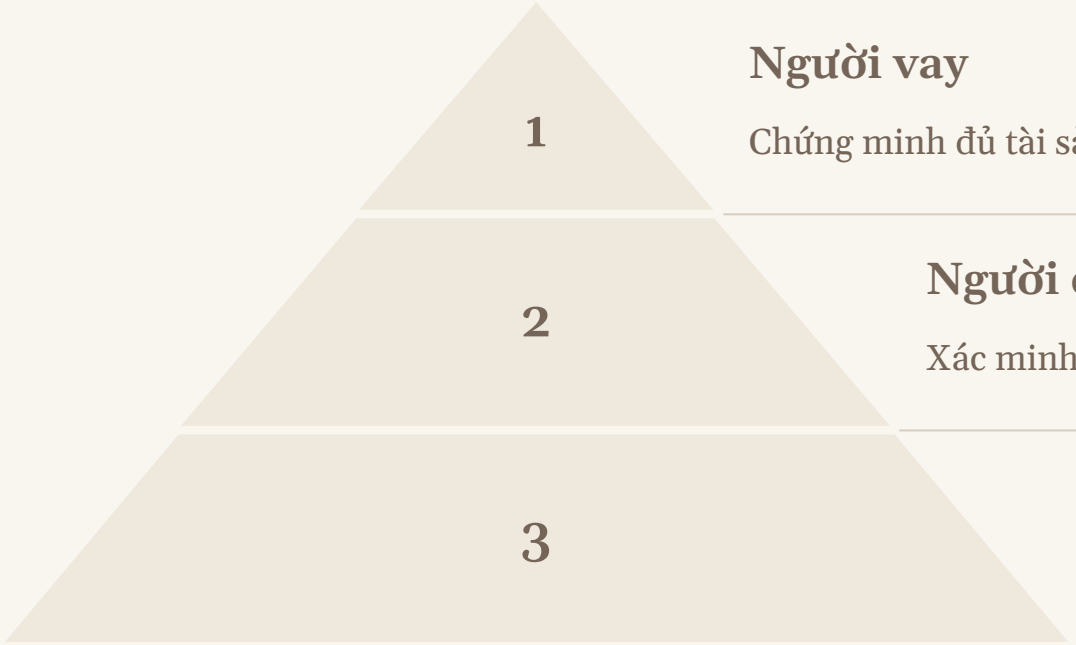
Nhận một cam kết ZKP.

3

Rút tài sản

Cung cấp bằng chứng zk-SNARK.

Private Lending - Vay Mượn Ẩn Danh



Người vay

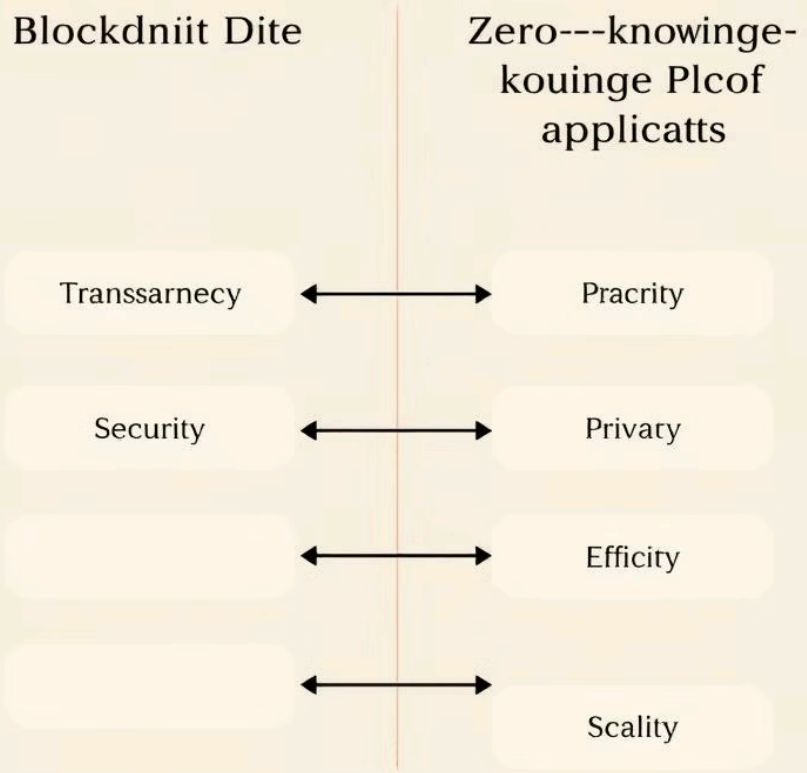
Chứng minh đủ tài sản thế chấp.

Người cho vay

Xác minh khoản vay hợp lệ.

Không tiết lộ

Không tiết lộ thông tin cá nhân.



So Sánh Các Ứng Dụng ZKP

Tiêu chí	Tornado Cash	Aztec Protocol	Shielded Pools	Private Lending
Mục đích	Giao dịch ẩn danh	Hợp đồng thông minh bí mật	Pool giao dịch ẩn danh	Vay mượn không công khai
Công nghệ ZKP	zk-SNARKs	zk-SNARKs	zk-SNARKs, zk-STARKs	zk-SNARKs, zk-STARKs

Thách Thức và Rủi Ro

1

Pháp lý

Khả năng bị cấm hoặc hạn chế.

2

Lạm dụng

Nguy cơ rửa tiền.

3

Triển khai

Đòi hỏi tài nguyên tính toán lớn.

Kết Luận

ZKP đang thay đổi bảo mật và quyền riêng tư trong DeFi.

Tornado Cash và Aztec Protocol đối mặt thách thức pháp lý.

Shielded pools giúp bảo vệ giao dịch, nhưng có nguy cơ bị lạm dụng.