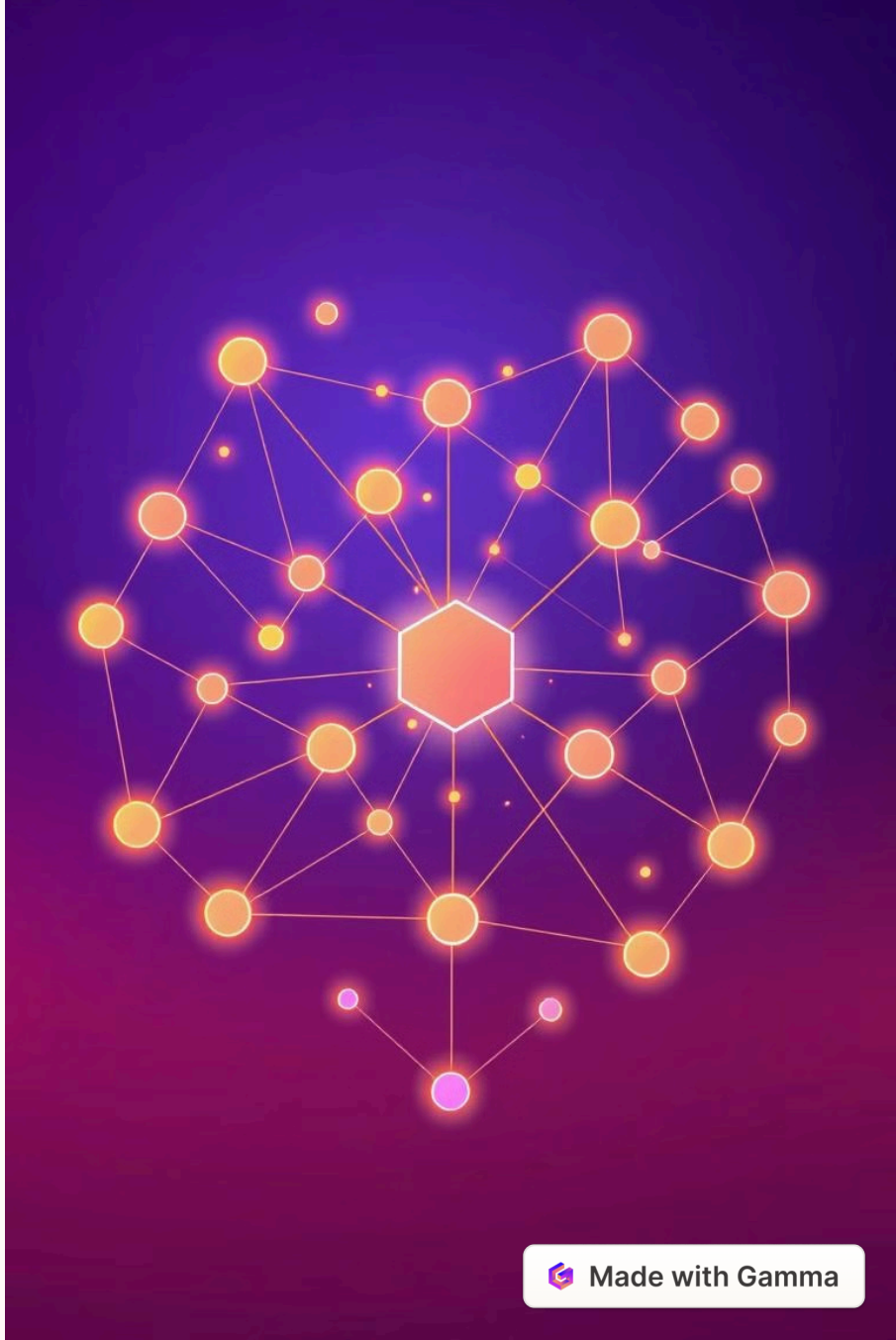
Zero-Knowledge Proof (ZKP) – Công Nghệ Bảo Mật Tương Lai

Zero-Knowledge Proof (ZKP) là kỹ thuật mật mã. Nó cho phép chứng minh một tuyên bố là đúng. Điều này được thực hiện mà không tiết lộ thông tin chi tiết. ZKP tăng cường quyền riêng tư và bảo mật.



ZKP Là Gì?

1 **Không kiến thức**

Người xác minh không biết thêm thông tin.

2 **Hoàn chỉnh**

Nếu tuyên bố đúng, người xác minh sẽ bị thuyết phục.

3 **Đúng đắn**

Người chứng minh không trung thực thì không thể thuyết phục.

Ứng Dụng Của ZKP Trong Blockchain

Bảo mật giao dịch

Ẩn danh người gửi, người nhận và số tiền.

Nhận dạng phi tập trung

Xác thực danh tính mà không tiết lộ thông tin cá nhân.

Bảo mật giao dịch trong DeFi

Ẩn danh

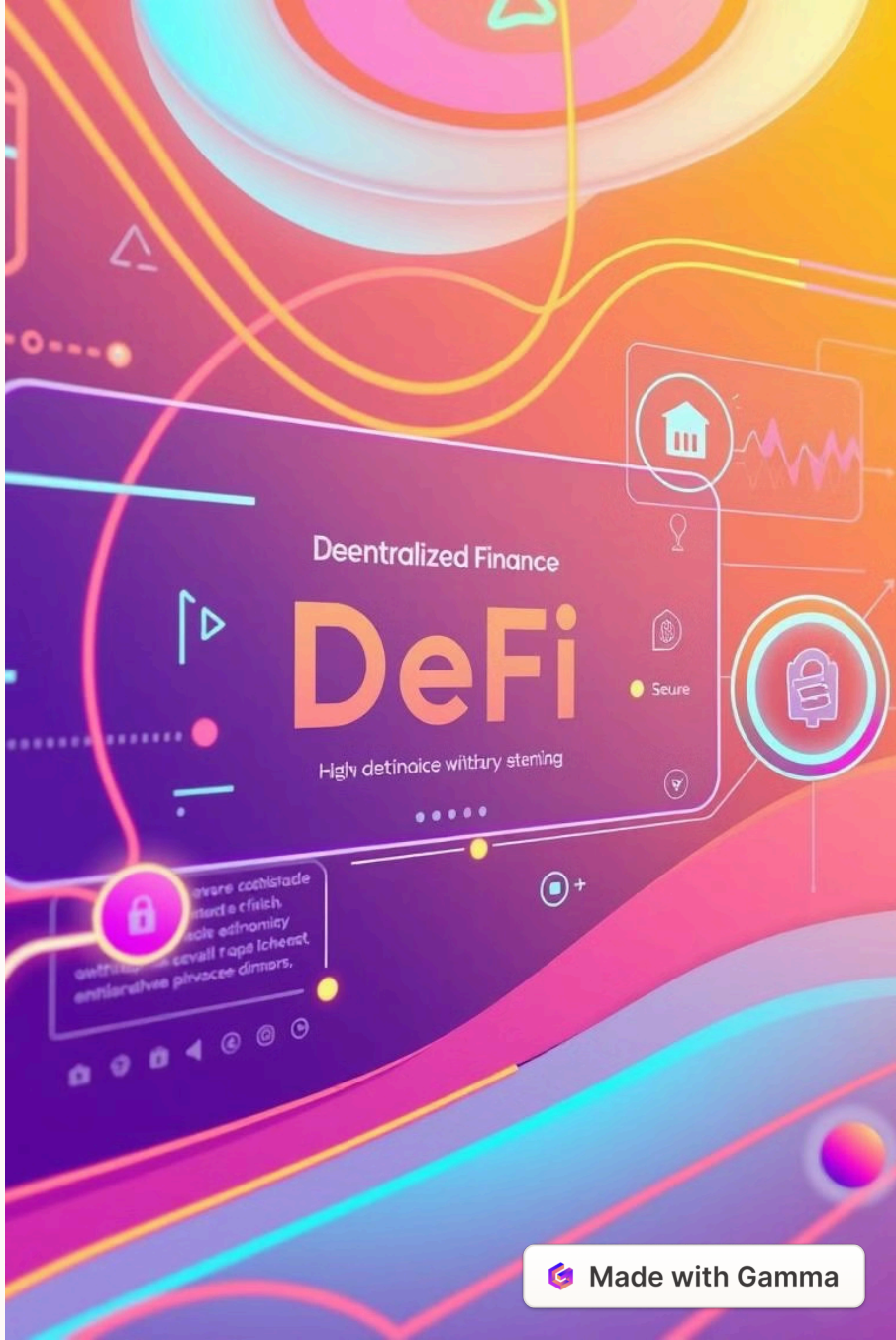
Ẩn danh người gửi, người nhận và số tiền giao dịch.

Tính hợp lệ

Đảm bảo tính hợp lệ của giao dịch mà không tiết lộ chi tiết.

Ví dụ

Zcash (ZEC) và Aztec Protocol sử dụng ZKP.



Nhận dạng phi tập trung (DID)

Xác thực danh tính

Không tiết lộ thông tin cá nhân.

Ví dụ

Worldcoin và Polygon ID sử dụng ZKP.

So Sánh ZK-SNARKs vs. ZK-STARKs

Tiêu chí	ZK-SNARKs	ZK-STARKs
Năm ra mắt	2012	2018
Cần thiết lập đáng tin cậy?	Có	Không
Thời gian xác minh	Nhanh hơn	Dài hơn

ZK-SNARKs

1

Nhanh và hiệu quả

Về kích thước bằng chứng.

2

Cần thiết lập

Đáng tin cậy.

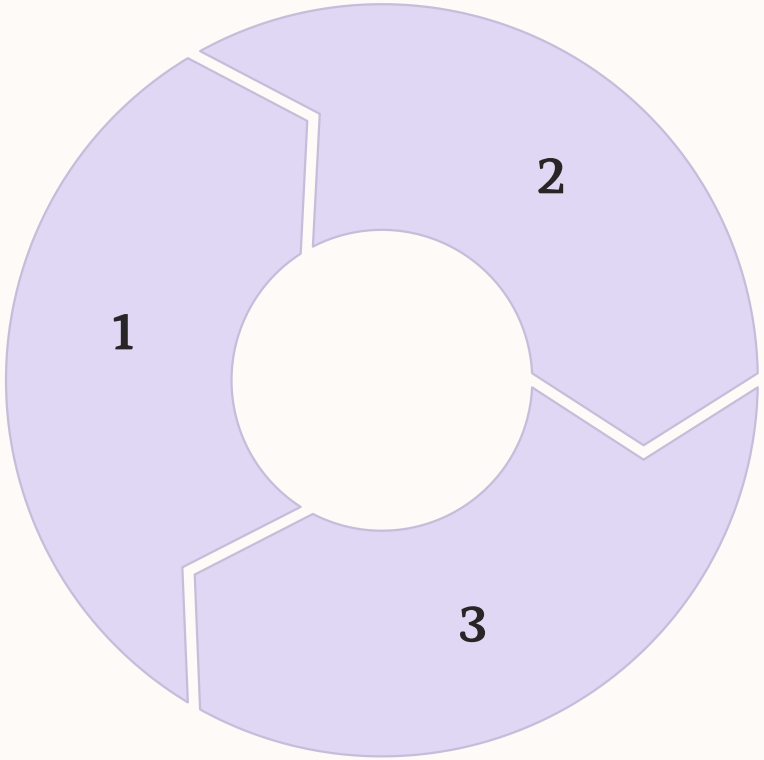
3

Ứng dụng

Zcash, Tornado Cash.

ZK-STARKs

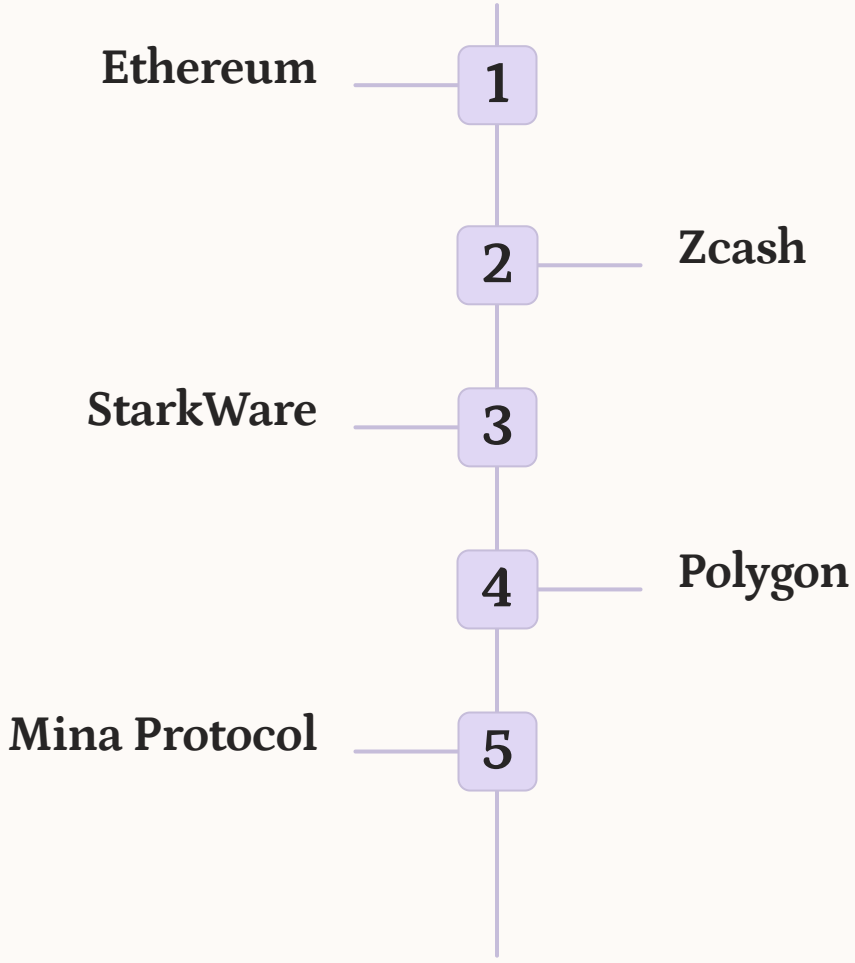
Bảo mật cao hơn



Không cần thiết lập

Chống tấn công lượng tử

Ứng dụng ZKP



Kết Luận

Zero-Knowledge Proof (ZKP) đang trở thành công nghệ bảo mật quan trọng. Nó giúp giao dịch ẩn danh và nhận dạng phi tập trung. ZKP nâng cao bảo mật và khả năng mở rộng cho blockchain. Với những tiến bộ trong ZK-SNARKs và ZK-STARKs, ZKP sẽ ngày càng phổ biến.