Bulletproofs: Zero-Knowledge Proof Không Cần Trusted Setup

Bulletproofs là Zero-Knowledge Proofs (ZKP) không cần Trusted Setup. Nó giúp tăng quyền riêng tư. Tìm hiểu cơ chế, ứng dụng trong Monero & so sánh với zk-SNARKs, zk-STARKs!

Bulletproofs Là Gì?

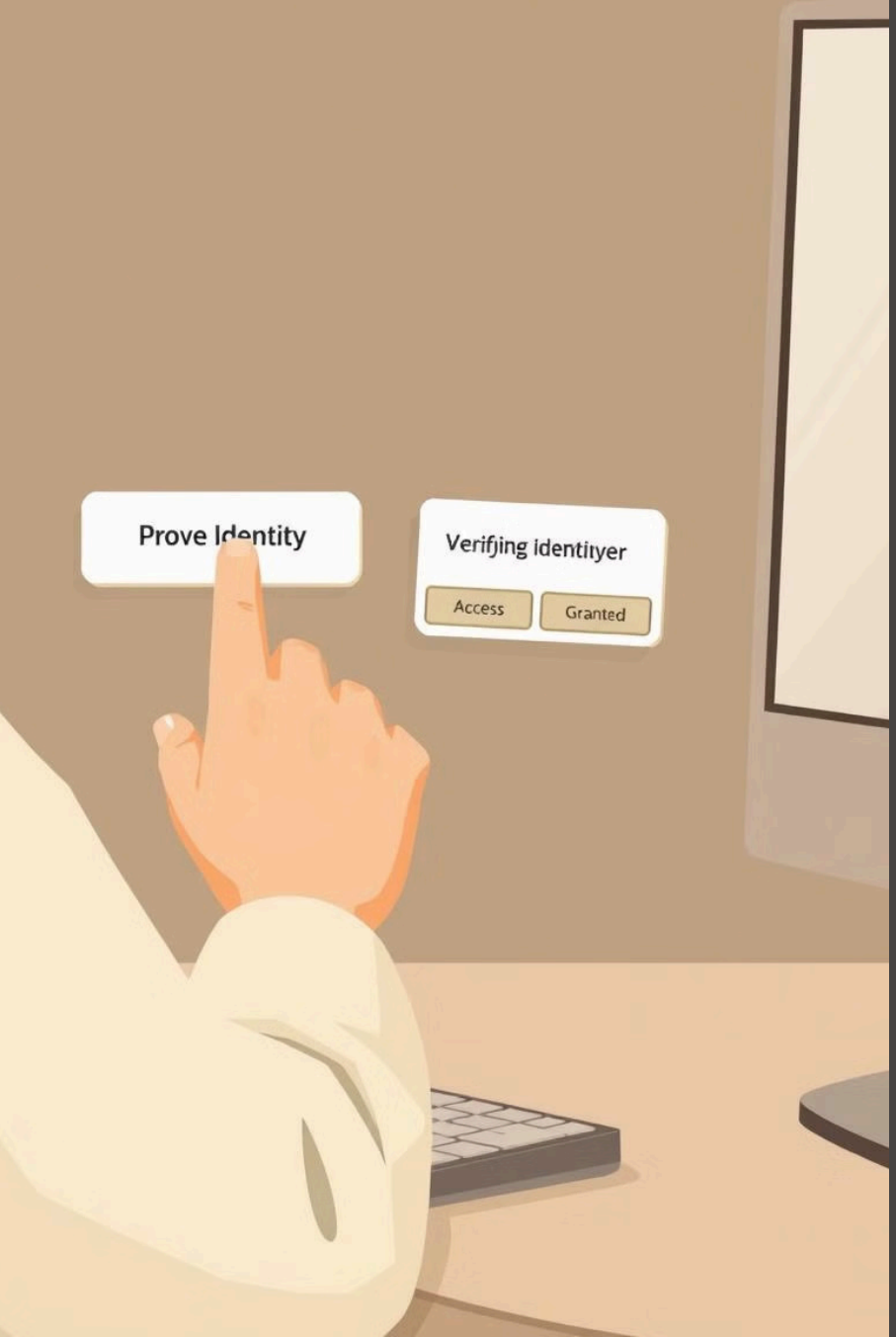
Bulletproofs là một loại chứng minh không tiết lộ kiến thức (ZKP) không tương tác. Nó được thiết kế để chứng minh các điều kiện số học.

1 Range proofs

Chứng minh một số nằm trong một phạm vi mà không tiết lộ giá trị thực.

2 Confidential Transactions

Xác minh tính hợp lệ của giao dịch mà không tiết lộ số tiền.



Cách Hoạt Động Của Bulletproofs

Người chứng minh sử dụng cam kết Pedersen để mã hóa giá trị cần chứng minh. Người chứng minh tạo bằng chứng rằng giá trị nằm trong khoảng hợp lệ mà không tiết lộ số thực tế.

Cam Kết

Mã hóa giá trị.

Bằng Chứng

Tạo range proofs.

Xác Minh

Kiểm tra tính hợp lệ.

Ứng Dụng Trong Monero

liên kết không xác định sử dụng RingCT để che giấu số tiền giao dịch. Bulletproofs giúp cải thiện hiệu suất RingCT.

Giảm kích thước

Giảm kích thước range proofs xuống còn ~1-2 KB.

Cải thiện hiệu suất

Cải thiện hiệu suất giao dịch và giảm phí gas.

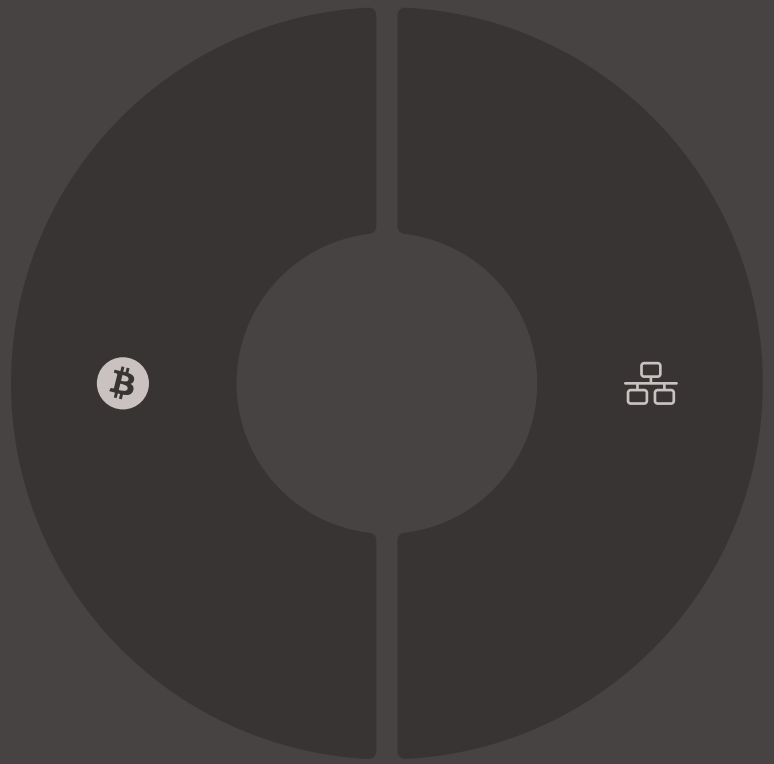
Tăng cường bảo mật

Loại bỏ Trusted Setup, không để lại lỗ hổng bảo mật.

Ứng Dụng Trong CT

Ngoài Monero, Bulletproofs có thể được sử dụng trong Confidential Transactions trên Bitcoin sidechains hoặc các blockchain bảo mật như Liquid Network.

Bitcoin Sidechains



Liquid Network

So Sánh Với zk-SNARKs & zk-STARKs

Bulletproofs có kích thước bằng chứng trung bình và thời gian xác minh nhanh. Nó không phù hợp cho các mạch tính toán lớn.

zk-SNARKs

Nhỏ (~100-200 bytes), cần Trusted Setup.

zk-STARKs

Lớn (~từ vài KB), không cần Trusted Setup.

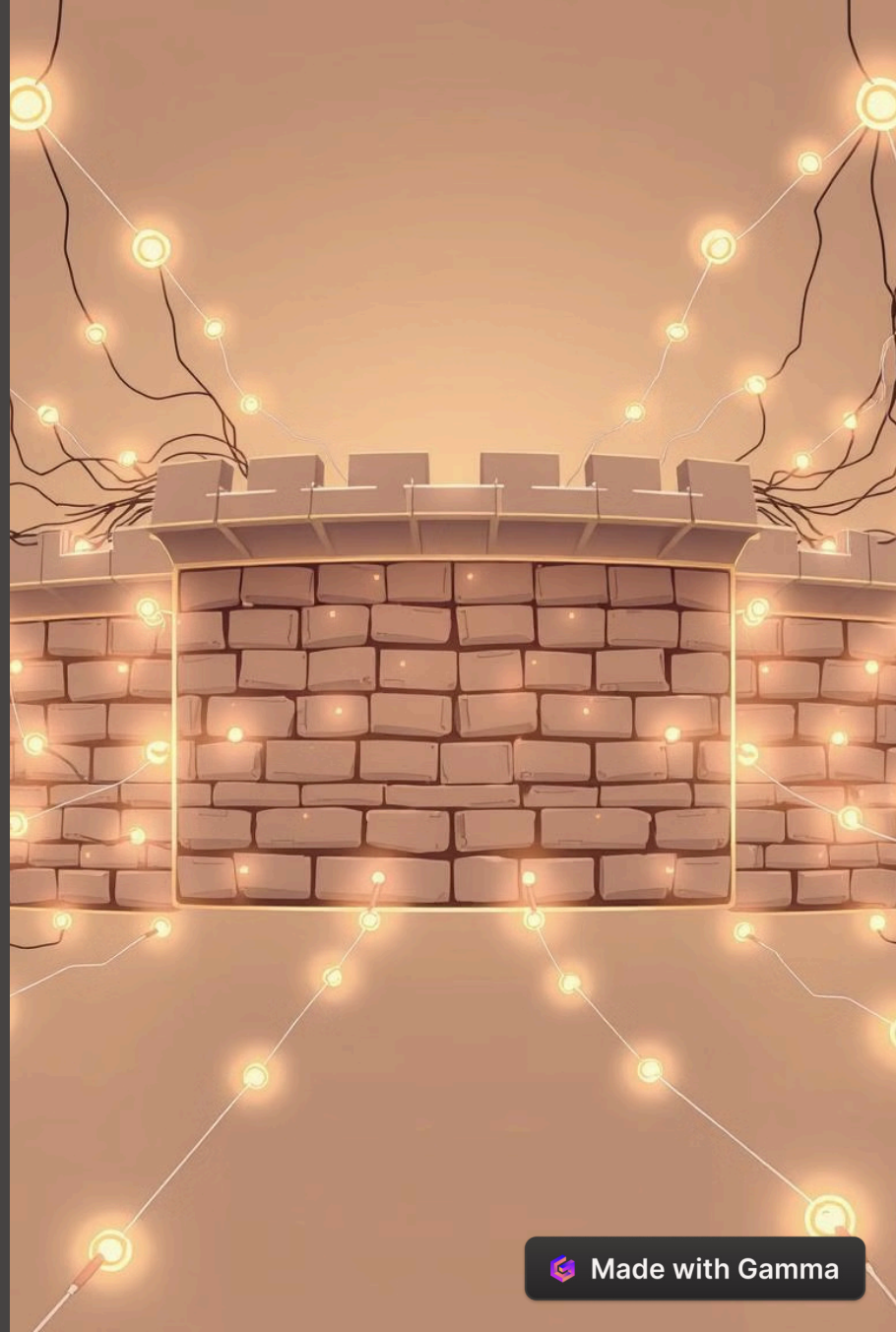
Điểm Mạnh Của Bulletproofs

Không cần Trusted Setup, giảm rủi ro bảo mật. Hiệu quả cao cho range proofs. An toàn trước máy tính lượng tử.

Không Trusted Setup

Hiệu Quả

An Toàn Lượng Tử



Nhược Điểm Của Bulletproofs

Không phù hợp cho các mạch tính toán lớn. Kích thước bằng chứng lớn hơn zk-SNARKs.

1 Mạch Tính Toán Lớn

2 Kích Thước Bằng Chứng

Kết Luận

Bulletproofs là một bước tiến lớn trong Zero-Knowledge Proofs. Nó giúp tăng cường quyền riêng tư mà không cần Trusted Setup.

1

Quyền Riêng Tư

Tăng cường quyền riêng tư.

2

Không Trusted Setup

Không cần Trusted Setup.

Kết Luận (Tiếp)

Bulletproofs đang chứng tỏ là một giải pháp mạnh mẽ cho quyền riêng tư giao dịch. Với sự phát triển của blockchain và DeFi, Bulletproofs có thể được áp dụng rộng rãi hơn trong tương lai.