

CS251 Mùa thu năm 2023

([cs251.stanford.edu](https://cs251.stanford.edu))



# Quyền riêng tư trên Blockchain

Dan Boneh

[dự án #4 đã được đăng]

# Nhu cầu về quyền riêng tư trong hệ thống tài chính

Quyền riêng tư của chuỗi cung ứng:

- Nhà sản xuất không muốn tiết lộ số tiền họ trả cho nhà cung cấp để mua các bộ phận.



Quyền riêng tư thanh toán:

- Một công ty trả lương cho nhân viên bằng tiền điện tử muốn giữ danh sách của nhân viên và tiền lương riêng tư.
- Người dùng cuối cần sự riêng tư khi cho thuê, tặng, mua hàng

Quyền riêng tư về logic kinh doanh: Mã của hợp đồng thông minh có thể riêng tư không?

# Nhu cầu về quyền riêng tư trong hệ thống tài chính

Đường bo+om:

Blockchain không thể đạt được tiềm năng đầy đủ của chúng nếu không có một số hình thức giao dịch riêng tư

# Các loại quyền riêng tư

Bí danh: (quyền riêng tư yếu) • Mỗi

người dùng đều có một bí danh nhất quán trong thời gian dài (ví dụ: reddit)

- Ưu điểm: reputaFon •

Nhược điểm: liên kết đến danh tính thực tế có thể bị rò rỉ qua Fme

Hoàn toàn ẩn danh: Giao dịch của người dùng không thể liên kết

- Không ai có thể biết được liệu hai giao dịch có đến từ cùng một địa chỉ hay không

# Một câu hỏi khó: quyền riêng tư khỏi ai?

Không có sự riêng tư :

Mọi người đều có thể xem  
tất cả các giao dịch



Quyền riêng tư của công chúng:

Chỉ có người điều hành đáng tin  
cậy mới có thể xem các giao dịch

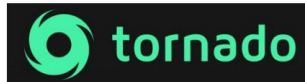


Quyền riêng tư bán đầy đủ:

chỉ có cơ quan thực thi pháp luật "địa  
phương" mới có thể xem các giao dịch

sự riêng tư hoàn toàn:

không ai có thể nhìn thấy giao dịch



# Các khía cạnh tiêu cực của sự riêng tư hoàn toàn

Làm thế nào để ngăn chặn hoạt động tội phạm?

## Thách thức:

- Làm thế nào để hỗ trợ các ứng dụng tích cực của

thanh toán tư nhân như ng ngăn chặn các khoản thanh toán tiêu cực?

- Chúng ta có thể đảm bảo tuân thủ pháp luật trong khi vẫn bảo vệ đư ợc quyền riêng tư không?

- Đúng!

Công nghệ chính: bằng chứng không kiến thức



# Bitcoin và Ethereum có riêng tư không?

Hệ thống cơ sở chắc chắn không phải là.

# Quyền riêng tư trong Ethereum?

- Mọi số dư tài khoản đều công khai • Đối

với Dapp: mã và trạng thái nội bộ đều công khai





- Tất cả các giao dịch tài khoản đư ợc liên kết với tài khoản

[etherscan.io](https://etherscan.io):

Địa chỉ 0x1654b0c3f62902d7A86237.

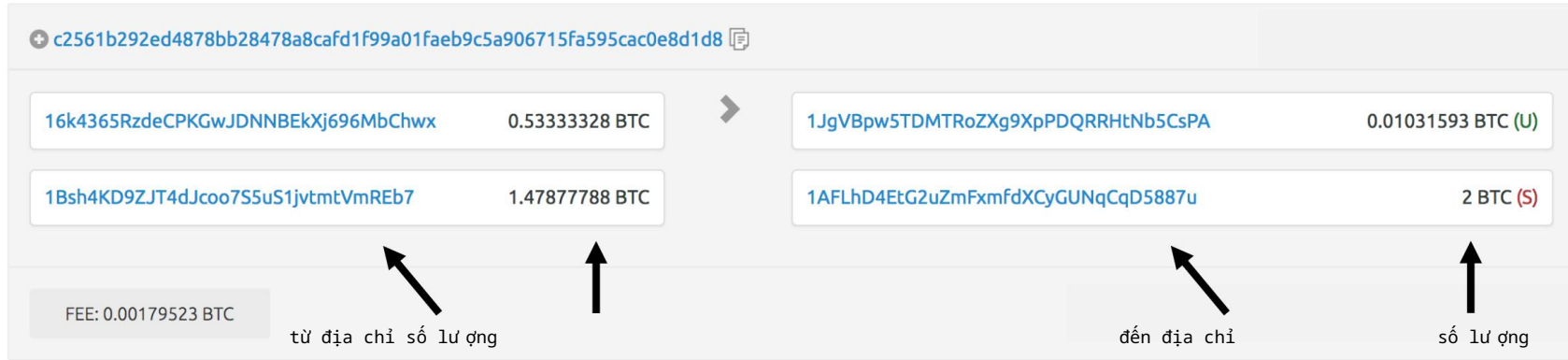
Balance: 1.114479450024297906 Ether

Ether Value: \$4,286.34 (@ \$3,846.05/ETH)

	Txn Hash	Method ⓘ	Block
	<a href="#">0x0269eff8b4196558c07...</a>	Set Approval For...	<a href="#">13426561</a>
	<a href="#">0xa3dacb0e7c579a99cd...</a>	Cancel Order_	<a href="#">13397993</a>
	<a href="#">0x73785abcc7ccf030d6a...</a>	Set Approval For...	<a href="#">13387834</a>
	<a href="#">0x1463293c495069d61c...</a>	Atomic Match_	<a href="#">13387703</a>



# Quyền riêng tư trong Bitcoin?



Alice có thể có nhiều địa chỉ (việc tạo địa chỉ là miễn phí)

Đầu vào: A1:4, A2:5

ra: B:6, A3:3

Thay đổi địa chỉ

Địa chỉ của Alice

Địa chỉ của Bob

Dữ liệu giao dịch có thể được sử dụng để liên kết một địa chỉ với một danh tính vật lý

(phân tích chuỗi)

# Liên kết địa chỉ với danh tính

đầu vào: A1: 4, A2: 5

đầu ra: B: 6, A3: 3

Alice mua một cuốn sách từ một thư ơ ng gia: •

Alice biết đư ợc một trong những địa chỉ của thư ơ ng gia

(B) • Thư ơ ng gia liên kết ba địa chỉ với Alice (A1, A2, A3)

---

Alice sử dụng một sàn giao dịch (ETH     USD) •

BSA: một sàn giao dịch của Hoa Kỳ phải thực hiện KYC (biết khách hàng của bạn)

. thu thập và xác minh ID của Alice

• Trao đổi liên kết Alice đến địa chỉ của cô ấy (A1, A2, A3)

# Chiến lược ẩn danh: Thành ngữ sử dụng

Một chiến lược chung để khử ẩn danh địa chỉ Bitcoin

Phươ ng pháp 1:

Hai địa chỉ đư ợc nhậ p vào TX      cả hai

địa chỉ đều đư ợc kiểm soát bởi cùng một thực thể

The screenshot displays a Bitcoin transaction interface. At the top, the transaction ID is `c2561b292ed4878bb28478a8cafd1f99a01faeb9c5a906715fa595cac0e8d1d8` with a 'mined Apr 10, 2017 12:38:00 AM' timestamp. The transaction is divided into two main sections: inputs (left) and outputs (right), separated by a right-pointing arrow. The input section contains two entries: `16k4365RzdeCPKGwJDNNBEkXj696MbChwx` (0.53333328 BTC) and `1Bsh4KD9ZJT4dJcoo7S5uS1jvtmtVmREb7` (1.47877788 BTC). The output section contains two entries: `1JgVBpw5TDMTRoZXg9XpPDQRRHtNb5CsPA` (0.01031593 BTC (U)) and `1AFLhD4EtG2uZmFxmfdXCyGUNqCqD5887u` (2 BTC (S)). At the bottom left, the fee is listed as 'FEE: 0.00179523 BTC'. At the bottom right, there is a blue button labeled '1 CONFIRMATIONS' and a green button labeled '2.01031593 BTC'.

Address	Amount (BTC)
<code>16k4365RzdeCPKGwJDNNBEkXj696MbChwx</code>	0.53333328
<code>1Bsh4KD9ZJT4dJcoo7S5uS1jvtmtVmREb7</code>	1.47877788
<code>1JgVBpw5TDMTRoZXg9XpPDQRRHtNb5CsPA</code>	0.01031593 (U)
<code>1AFLhD4EtG2uZmFxmfdXCyGUNqCqD5887u</code>	2 (S)

FEE: 0.00179523 BTC

1 CONFIRMATIONS      2.01031593 BTC

Địa chỉ thay đổi đư ợc kiểm soát bởi cùng một ngư ời dùng như địa chỉ đầu vào Địa chỉ thay đổi là gì? • Heuristic: một địa chỉ mới nhận đư ợc ít h ơn mọi đầu vào

+ c2561b292ed4878bb28478a8cafd1f99a01faeb9c5a906715fa595cac0e8d1d8

mined Apr 10, 2017 12:38:00 AM

16k4365RzdeCPKGwJDNNBEkXj696MbChwx

0.53333328 BTC

>

1JgVBpw5TDMTRoZXg9XpPDQRRHtNb5CsPA

0.01031593 BTC (U)

1Bsh4KD9ZJT4dJcoo7S5uS1jvtmtVmREb7

1.47877788 BTC

1AFLhD4EtG2uZmFxmfdXCyGUNqCqD5887u

2 BTC (S)

FEE: 0.00179523 BTC

1 CONFIRMATIONS

2.01031593 BTC

# Một thí nghiệm Bitcoin [Meiklejohn, et al.]

bước 1: Heuristic 1 và 2      cụm 3,3M

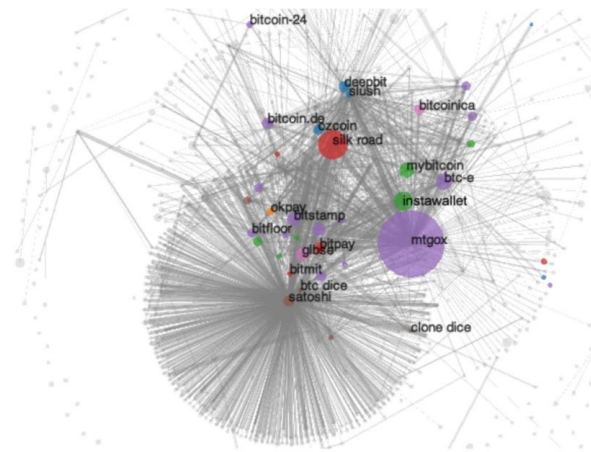
bước 2: 1070 địa chỉ được xác định bằng cách tương tác với các thư ngân gia

- Coinbase, Kraken, .

Bước 3: bây giờ 15% tổng số địa chỉ đã được xác định

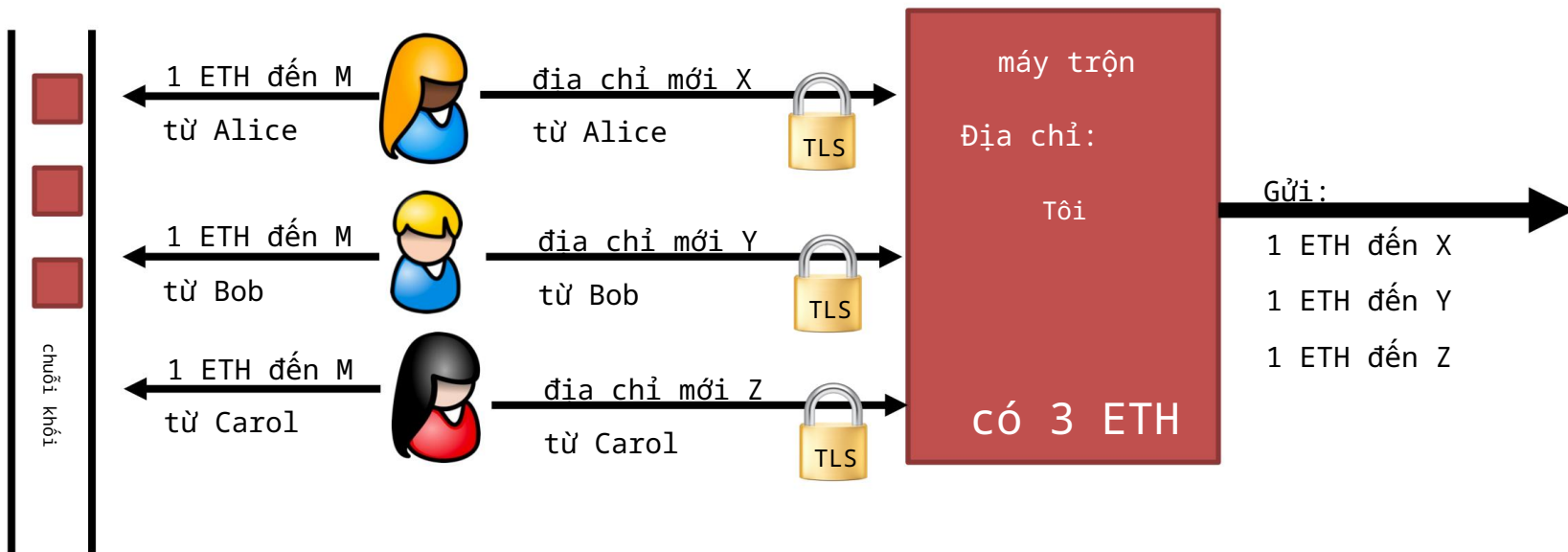
- Tìm hiểu tổng tài sản cho tất cả các cụm

Những nỗ lực thư ngân mại: Chainalysis, EllipFc, .



Tiền riêng tư trên Blockchain công khai

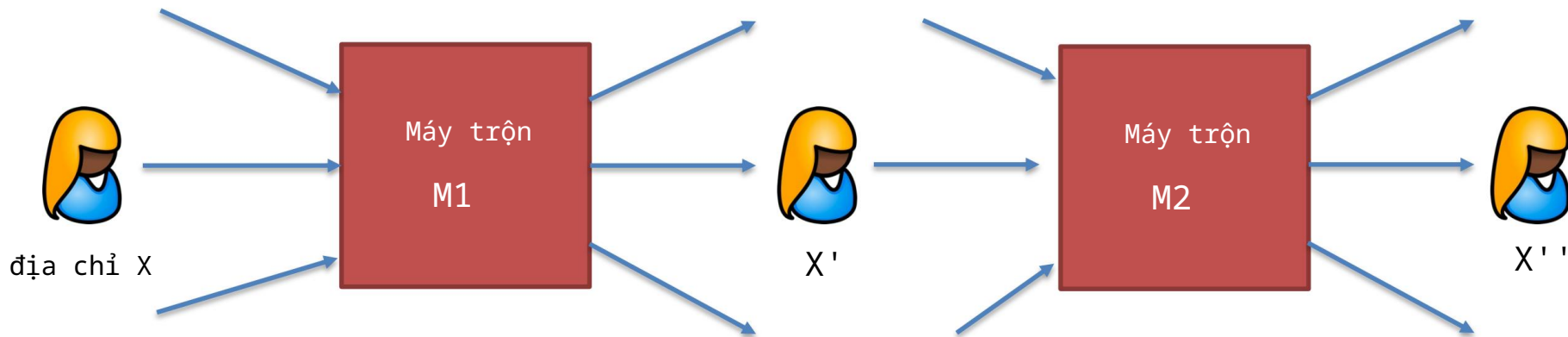
# Cố gắng 1: trộn đơ n giản



Người quan sát biết Y thuộc về một trong {Alice, Bob, Carol} nhưng không biết Y thuộc về ai  
bộ ẩn danh có kích thước 3.

Vấn đề: (i) máy trộn M biết xáo trộn, (ii) máy trộn có thể trốn thoát với 3 ETH !!

# Tăng cường bộ ẩn danh



M1: trộn các đầu vào từ người dùng      X' có kích thước tập ẩn danh =

M2: kết quả đầu ra từ bộ trộn      X''' có kích thước thiết lập ẩn danh =  $\times$

Quyền riêng tư : miễn là một trong hai người đi M1 hoặc M2 trung thực



# Trộn an toàn mà không cần máy trộn?

Vấn đề: Mixer có thể bỏ trốn với tiền hoặc tiết lộ sự xáo trộn.

Chúng ta có thể trộn an toàn mà không cần máy trộn đáng tin cậy không? Câu trả lời: Có!

- trên Bitcoin: CoinJoin (được sử dụng bởi, ví dụ, ví Wasabi)
- trên Ethereum: Tornado cash, Privacy Pools, .

. một máy trộn đơn sử dụng bản in thử ZK - bài giảng tiếp theo

# CoinJoin: Trộn Bitcoin mà không cần Mixer

Bối cảnh: Alice, Bob và Carol muốn gặp nhau.

Alice sở hữu UTXO A1:5, Bob sở hữu UTXO B1:3, Carol sở hữu C1:2



A1: 5, A3 (thay đổi địa chỉ)

A2 (địa chỉ kết hợp sau qua Tor)



B1: 3, B3 (thay đổi địa chỉ)

B2 (địa chỉ sau khi kết hợp qua Tor)



(giống như Alice và Bob)



A1: 5, A3

B1: 3, B3

C1: 2, C3

Diễn đàn

địa  
chỉ hỗn hợp

công cộng B2, A2, C2

# CoinJoin: Trộn Bitcoin mà không cần Mixer

CoinJoin TX: cả ba đều chuẩn bị và ký các Tx sau:

đầu vào (không riêng tư): A1: 5, B1: 3, C1: 2

đầu ra (riêng tư): B2: 2, A2: 2, C2: 2

đầu ra (không riêng tư): A3: 3, B3: 1

địa chỉ hỗn hợp

Tất cả các UTXO hỗn hợp đều có cùng giá trị = min đầu vào (2 trong trường hợp này)

Cả ba bài đăng chữ ký trên Pastebin      một trong số chúng đăng Tx trên chuỗi.

# Như ợc điểm của Coinjoin

Trong thực tế: mỗi CoinJoin Tx kết hợp khoảng 40 đầu vào • Tx

lớn: 40 đầu vào, 80 đầu ra

Tất cả người tham gia phải ký CoinJoin Tx để nó có hiệu lực      đảm  
bảo tất cả họ đều chấp thuận CoinJoin Tx

. nhưng bất kỳ ai trong số họ cũng có thể phá vỡ quá trình

Không chỉ đơn giản là trộn

Giao dịch riêng tư trên blockchain công khai

# Chúng ta có thể thực hiện giao dịch riêng tư trên blockchain công khai không?

Lý luận ngây thơ :

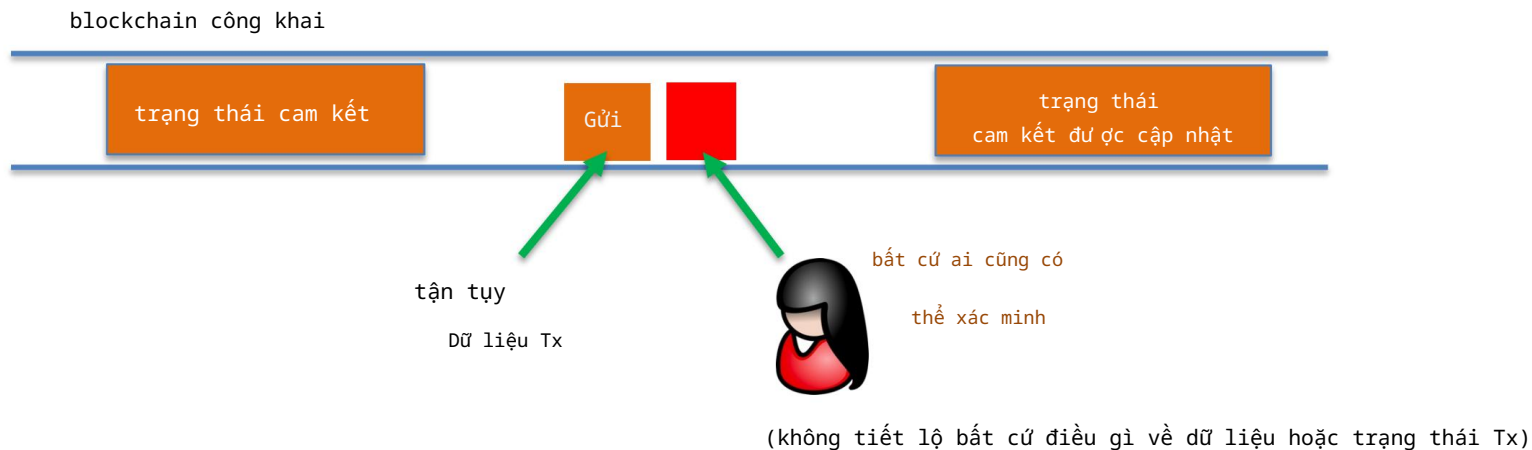
khả năng xác minh phổ quát     dữ liệu giao dịch phải được công khai

nếu không thì làm sao chúng ta có thể xác minh Tx??

phép thuật mật mã     Tx riêng tư trên blockchain có thể xác minh công khai

Công cụ tiền điện tử: cam kết và bằng chứng không kiến thức

# Một mô hình cho Tx tư nhân



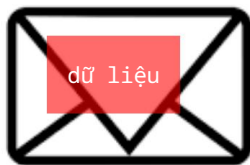
Dữ liệu đã cam kết: cam kết ngắn (ẩn) trên chuỗi

Bằng chứng : bằng chứng ngắn gọn không có kiến thức rằng

- (1) dữ liệu Tx đã cam kết phù hợp với trạng thái hiện tại đã cam kết và
- (2) trạng thái cập nhật đã cam kết là chính xác

# Đánh giá: cam kết mật mã

Cam kết mật mã: mô phỏng một phong bì



Nhiều ứng dụng: ví dụ, DAPP cho phiên đấu giá kín

- Mỗi người tham gia cam kết với giá thầu của mình,
- Khi tất cả các giá thầu đã được đưa ra, mọi người đều mở cam kết của mình



# Cam kết mật mã

Cú pháp: một lược đồ cam kết là hai thuật toán

- cam kết(msg, r)      com

sự ngẫu nhiên bí mật

chuỗi cam kết

- xác minh(msg, com, r)      chấp nhận hoặc từ chối

bất kỳ ai cũng có thể xác minh rằng cam kết đã được mở đúng cách

# Cam kết: bảo mật proper6es

- ràng buộc: Bob không thể tạo ra hai lần mở hợp lệ cho com

Chính xác hơn: không có đối thủ hiệu quả nào có thể tạo ra

$com, (m1, r1), (m2, r2)$

sao cho  $verify(m1, com, r1) = verify(m2, com, r2) = accept$  và  $m1 \neq m2$ .

---

- ản: com không tiết lộ bất cứ điều gì về dữ liệu đã cam kết

$commit(m, r)$  cho ra  $com$ , và  $r$  được lấy mẫu đồng đều trong một tập hợp  $S$ ,

thì  $com$  độc lập về mặt thống kê với  $m$

# Ví dụ: cam kết dựa trên băm

Sửa hàm băm  $on : \times$  (ví dụ: SHA256)

chống va chạm ở đâu, và  $|$   $|$   $|$   $|$

- cam kết(  $,$  ) :  $com = ( , )$
- verify(  $, com,$  ) : chấp nhận nếu  $com = ( , )$

ràng buộc: theo sau từ khả năng chống va chạm  
của ản: theo sau từ một giả định nhẹ > trên trên

# zk-SNARK là gì?

Bằng chứng không kiến thức ngắn gọn:  
một công cụ quan trọng cho quyền riêng tư trên blockchain

# zk-SNARK là gì? (trực giác)

SNARK: một bằng chứng ngắn gọn cho thấy một tuyên bố nào đó là đúng

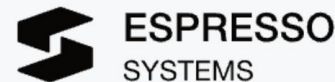
Ví dụ câu lệnh: “Tôi biết một số sao cho  $\text{SHA256}( ) = 0$ ”

- SNARK: bằng chứng “ngắn” và “nhanh” để xác minh

[nếu như      là 1GB thì bằng chứng tầm thư ờng (thông điệp) không phải là cả hai]

- zk-SNARK: bằng chứng “không tiết lộ điều gì” về

# Lợi ích thương mại trong SNARKs



Nhiều ứng dụng xây dựng hơ n sử dụng SNARK

# Ứng dụng Blockchain I

Gia công phần mềm tính toán/trên: (không cần kiến thức cơ bản)

Chuỗi L1 nhanh chóng xác minh công việc của dịch vụ ngoài chuỗi

Để giảm thiểu khí: cần một bằng chứng ngắn, nhanh chóng để xác minh

Ví dụ: •

Khả năng mở rộng: dịch vụ ngoài chuỗi Rollups dựa

trên bằng chứng (zkRollup) xử lý một loạt Tx;

Chuỗi L1 xác minh bằng chứng ngắn gọn rằng Tx đã được xử lý chính xác

• Kết nối các blockchain: bằng chứng về sự đồng thuận (zkBridge)

Chuỗi A đưa ra bằng chứng ngắn gọn về trạng thái của nó. Chuỗi B xác minh.

# Ứng dụng Blockchain II

Một số ứng dụng không yêu cầu kiến thức (quyền riêng tư):

- Giao dịch riêng tư trên blockchain công khai: •

bằng chứng zk cho thấy giao dịch riêng tư là hợp lệ (Tornado cash, Zcash, IronFish, Aleo)

- Tuân thủ: • Bằng

chứng cho thấy một giao dịch tư nhân tuân thủ luật ngân hàng (Espresso) • Bằng chứng cho

thấy một sàn giao dịch có khả năng thanh toán trong điều kiện không có kiến thức (Raposa)

Thêm thông tin về các ứng dụng blockchain này trong một phút



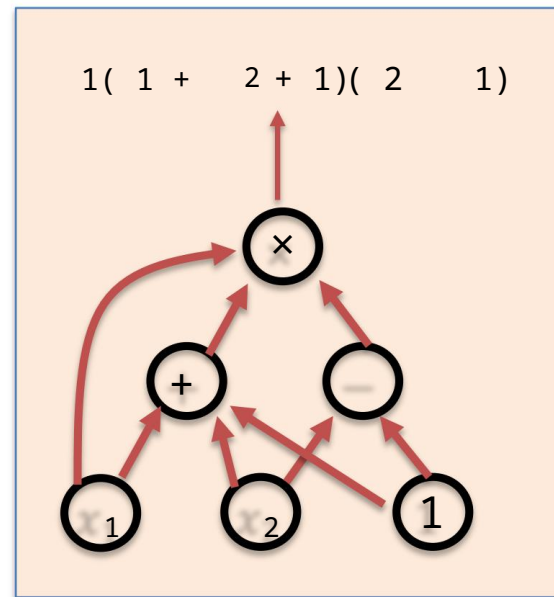
# Nhiều ứng dụng không phải blockchain

Blockchain thúc đẩy sự phát triển của SNARK

. như ng\_nhiều ứng dụng không phải blockchain đư ợc h ư ớ ng l ợi

# Mạch số học

- Sửa một trường hữu hạn  $= \{0, \dots, p-1\}$  với một số nguyên tố  $p > 2$ .
- Mạch số học/c:
  - đồ thị có hướng không có chu trình (DAG) trong đó các nút bên trong được gắn nhãn  $+$ ,  $-$  hoặc  $\times$  đầu vào được dán nhãn  $1, x_1, x_2, \dots, x_n$
  - định nghĩa một đa thức  $n$  biến với một đánh giá về công thức
  - $|V| = \#$  cổng trong



# Mạch số học thú vị

Ví dụ:

- $\text{Chash}(h, m)$ : đầu ra 0 nếu  $\text{SHA256}(m) = h$  , và 0 nếu không

Kiểm tra(h, m) = (h - SHA256(m)) ,  $|\text{Chash}| \approx 20K$  công

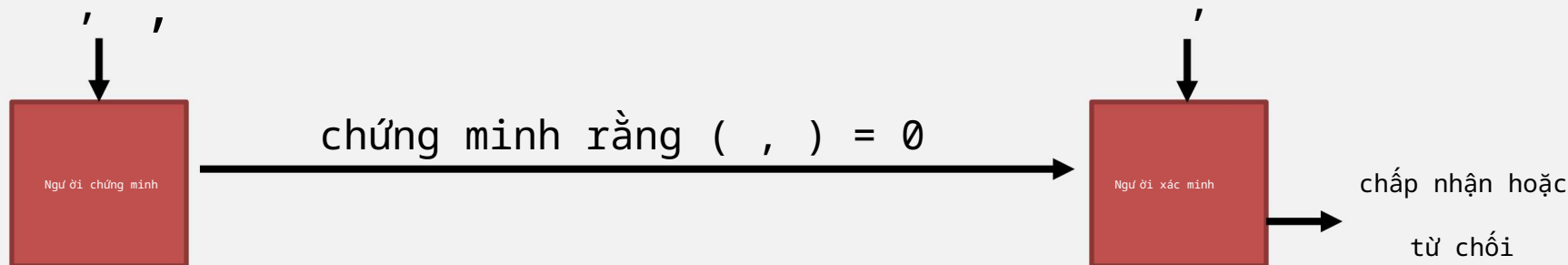
- $\text{Csig}(pk, m, \sigma)$ : đưa ra 0 nếu  $\sigma$  là chữ ký ECDSA hợp lệ trên m đối với pk

# (tiền xử lý) NARK: Lập luận không tơ ơ ng tác của kiến thức

Mạch số học công cộng:

tuyên bố công khai trong ! ( , ) nhân chứng bí mật trong "

Tiền xử lý (thiết lập):  $S( )$  tham số công khai ( , )



# (tiền xử lý) NARK: Lập luận không tư ơ ng tác của kiến thức

NARK tiền xử lý là bộ ba  $(S, P, V)$ :

- $S( )$  tham số công khai  $( , )$  cho người chứng minh và người xác minh
- $P( , , )$  bằng chứng
- $V( , , )$  chấp nhận hoặc từ chối

# NARK: yêu cầu (không chính thức)

Người chứng minh  $P( , , )$

Người xác minh  $V( , , )$

bằng chứng

chấp nhận hoặc từ chối

Hoàn thành:  $( , : ( , ) = 0 \quad \Pr[ V( , , P( , , ) ) = \text{chấp nhận} ] = 1$

âm thanh kiến thức:  $V$  chấp nhận  $P$  "biết" st (một trình  $( , ) = 0$

trích xuất có thể trích xuất một giá trị hợp lệ từ  $P$ )

Tùy chọn: Không có kiến thức:  $( , , , , )$  "không tiết lộ điều gì" về

# SNARK: Một lập luận ngắn gọn về kiến thức

Một NARK tiền xử lý ngắn gọn là bộ ba  $(S, P, V)$ :

- $S( )$  tham số công khai  $( , )$  cho người chứng minh và người xác minh

- $P( , , )$  bản chứng minh ngắn ;  $len() = .( | | )$

- $V( , , )$  nhẹ chóng để xác minh ;  $Fme(V) = .( | , | | | )$

“tóm tắt” ngắn gọn về mạch điện

V không có thời gian để đọc!!

[ đối với một số SNARK,  $len = \text{thời gian} = (1)$  ]

# SNARK: Một lập luận ngắn gọn về kiến thức

SNARK: một NARC (hoàn chỉnh và có kiến thức) ngắn gọn \_\_\_\_\_

zk-SNARK: một SNARK cũng không có kiến thức



# SNARK tầm thường không phải là SNARK

- (a) Người chứng minh gửi cho người xác minh,
- (b) Người xác minh kiểm tra xem  $(\cdot, \cdot) = 0$  hay không và chấp nhận nếu đúng.

Vấn đề với điều này:

- (1) có thể dài: chúng tôi muốn một bằng chứng “ngắn”
- (2)  $\text{compuFng}(\cdot, \cdot)$  có thể khó: chúng ta muốn một trình xác minh “nhanh”
- (3) có thể là bí mật: người chứng minh có thể không muốn tiết lộ để xác minh

# Vườn thú SNARK. bài giảng tiếp theo



NGAY ĐỢ

Chống đạn

Groth16

Song Tử

Plonky2

Halo2

Tiếng kêu

TỐI TẮM

Phân tích

Tân tinh

Cá cờ

Siêu Plonk

chòm sao Orion

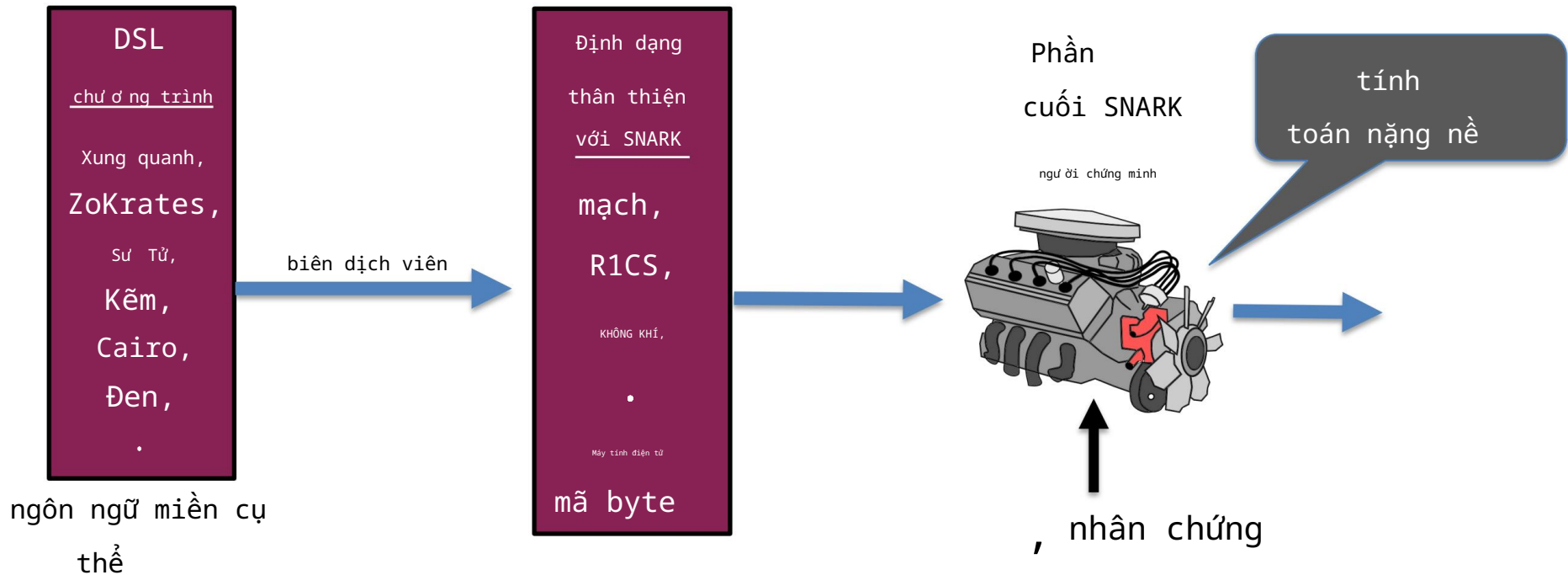
Chuột đá

Âm thanh

Ngư ời Sparta

Mở: một SNARK để thống trị tất cả

# SNARK trong thực tế



# KẾT THÚC BÀI GIẢNG

Bài giảng tiếp

theo: thêm về zk-SNARK và ứng dụng của chúng