

CS251 Mùa thu năm 2023

(cs251.stanford.edu)



Sử dụng zk-SNARK để bảo mật trên Blockchain

Dan Boneh

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?

Bài giảng trước





Cả Bitcoin và Ethereum đều không riêng tư

etherscan.io:

Địa chỉ 0x1654b0c3f62902d7A86237.

Balance: 1.114479450024297906 Ether

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

	Txn Hash	Method ⓘ	Block
	0x0269eff8b4196558c07...	Set Approval For...	13426561
	0xa3dacb0e7c579a99cd...	Cancel Order_	13397993
	0x73785abcc7ccf030d6a...	Set Approval For...	13387834
	0x1463293c495069d61c...	Atomic Match_	13387703

Bài giảng này: các công cụ chung cho quyền riêng tư trên blockchain

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

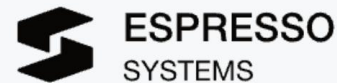
Ví dụ câu lệnh: “Tôi biết một số sao cho $\text{SHA256}() = 0$ ”

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

[nếu như là 1GB thì bằng chứng tầm thường (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 hơn sử dụng SNARK

Ứng dụng Blockchain I

Gia công tính toán: (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 (Đã được chứng minh)

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

. nhưng nhiều ứng dụng không phải blockchain được hưởng lợi

Tại sao tất cả những điều này lại có thể xảy ra ngay bây giờ?

Đột phá: thiết bị chứng minh SNARK mới nhanh hơn

- Thời gian tạo bằng chứng là tuyến tính (hoặc gần tuyến tính) về kích thước tính toán
- Nhiều ý tưởng đẹp.bài giảng tiếp theo

một danh mục tài liệu tham khảo lớn: a16zcrypto.com/zero-knowledge-canon

SNARK là gì?

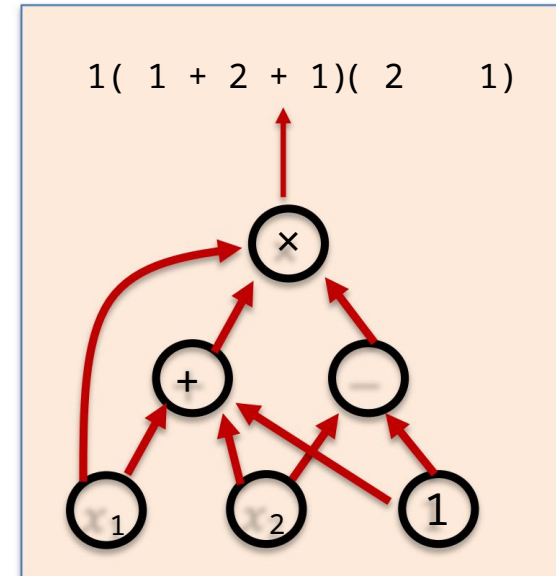
Đánh giá: mạch số học

Cố định một trường hữu hạn $= \{0, \dots, p-1\}$ với một số nguyên tố $p > 2$.

Mạch số học:

- đồ thị có hướng không có chu trình (DAG) trong đó
 - các nút bên trong được gắn nhãn $+$, $-$ hoặc \times
 - đầu vào được gắn nhãn $1, \dots, n$
- xác định một đa thức n biến với một công thức đánh giá

$|V| = \#$ cổng trong

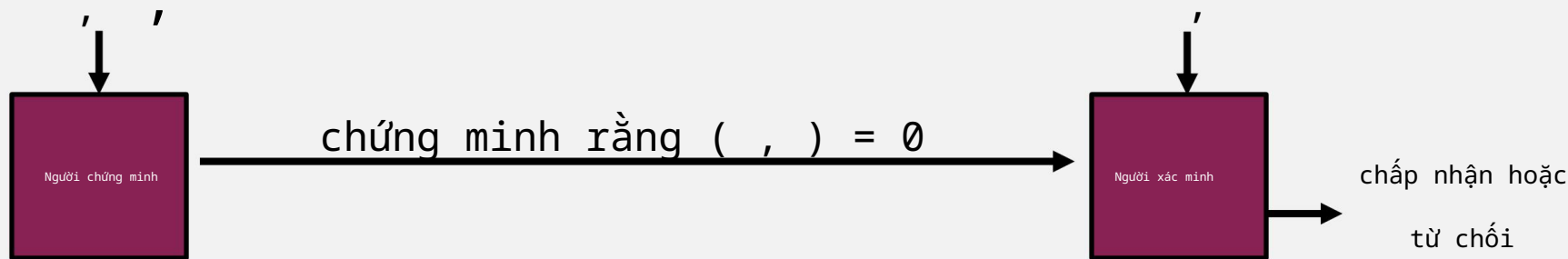


(tiền xử lý) NARK: Lập luận không tương tác của kiến thức

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 tương 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

tất cả các thuật toán và đối thủ đều có
quyền truy cập vào một oracle ngẫu nhiên

NARK: yêu cầu (không chính thức)

Người chứng minh $P(, ,)$

Người xác minh $V(, ,)$

bằng chứng

chấp nhận hoặc từ chối

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

Kiến thức âm thanh thích ứng : 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 mới" về
(nhân chứng tồn tại có thể mô phỏng bằng chứng)

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 ;

$$\text{dài}() = + (| |)$$

- $V(, ,)$ nhẹ chóng để xác minh ;

$$\text{thời gian}(V) = t(| , (| |)$$

“tóm tắt” ngắn gọn về mạch điện

V không có thời gian để đọc!!

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

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

Các loại tiền xử lý Thiết lập

Thu hồi thiết lập cho mạch: $S(;)$ tham số công khai $(,)$

bit ngẫu nhiên

Các loại thiết lập:

thiết lập đáng tin cậy cho mỗi mạch: $S(;)$ ngẫu nhiên phải được giữ bí mật với người chứng minh

người chứng minh học được có thể chứng minh những câu phát biểu sai

thiết lập đáng tin cậy nhưng phổ biến (có thể cập nhật): bí mật độc lập với

$= (\# !\# \$, \# !\% \& ')$
 $\underbrace{\# !\# \$ (;)}_{\text{một lần}}, \underbrace{\# !\% \& ' (,) (,)}_{\text{không có dữ liệu bí mật từ prover}}$

thiết lập minh bạch: $S()$ không sử dụng dữ liệu bí mật (không có thiết lập đáng tin cậy)

hỗn

Tiến bộ đáng kể trong những năm gần đây (danh sách một phần)

	kích thước của bằng chứng	thời gian xác minh	Cài đặt	hậu lượng tử?
Groth'16	≈ 200 Byte !(1)	$\approx 1,5\text{ms}$!(1)	tin cậy trên mỗi mạch	KHÔNG
Cá mú / Cá cờ	≈ 400 Byte !(1)	$\approx 3\text{ms}$!(1)	thiết lập tin cậy phổ quát	KHÔNG

Chống đạ	$\approx 1,5\text{KB}$!(nhập ký)	≈ 3 giây !()	ĐĂNG NHẬP	KHÔNG
NGAY ĐƠ	$\approx 100\text{KB}$!(nhập ký")	$\approx 10\text{ms}$!(nhập ký)	va chạm sức chống cự	Đúng

(cho mạch có 220 cổng)

Tiến bộ đáng kể trong những năm gần đây (danh sách một phần)

	kích thước của bằng chứng	thời gian xác minh	cài đặt	hậu lượng tử?
Groth'16	≈ 200 Byte !(1)	$\approx 1,5\text{ms}$!(1)	tin cậy trên mỗi mạch	KHÔNG
Cá mú / Cá cờ	≈ 400 Byte !(1)	$\approx 3\text{ms}$!(1)	thiết lập tin cậy phổ quát	KHÔNG
Chống đạn	$\approx 1,5\text{KB}$!(nhập ký)	≈ 3 giây !()	trong suốt	KHÔNG
NGAY ĐỢ	$\approx 100\text{KB}$!(nhập ký")	$\approx 10\text{ms}$!(nhập ký)	trong suốt	Đúng

(cho mạch có 220 cổng)

Tiến bộ đáng kể trong những năm gần đây (danh sách một phần)

	kích thước của bằng chứng	thời gian xác minh	cài đặt	hậu lượng tử?
Groth'16	≈ 200 Byte !(1)	≈ 1,5ms !(1)	tin cậy trên mỗi mạch	KHÔNG
Cá mú / Cá cờ	≈ 400 Byte !(1)	≈ 3ms !(1)	thiết lập đáng tin cậy	KHÔNG
Chống đận	≈ 1,5KB !(nhập ký)	≈ 3 giây !()	trong suốt	KHÔNG
NGAY ĐỢ	≈ 100KB !(nhập ký")	≈ 10ms !(nhập ký)	trong suốt	Đúng

(cho mạch có 220 cổng)

Làm thế nào để định nghĩa “kiến thức vững chắc” và “kiến thức bằng không”?

Định nghĩa: (1) kiến thức âm thanh

Mục tiêu: nếu V chấp nhận thì P “biết” st (,) = 0

“Biết” có nghĩa là gì?

định nghĩa không chính thức: P biết , nếu có thể được “trích xuất” từ P



Định nghĩa: (1) kiến thức âm thanh (giảm lược)

Về mặt hình thức: một SNARK phổ quát (S, P, V) là kiến thức vững chắc nếu

với mọi đối thủ thời gian poly $A = (A_0, A_1)$ tồn tại

một poly. bộ trích xuất thời gian (sử dụng A như một hộp đen) st

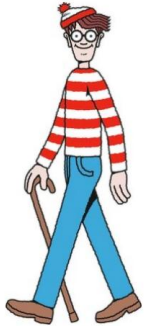
nếu $\text{Sinit}(\cdot), (C, \cdot, \text{trạng thái}) \quad A_0(\cdot), (\cdot, \cdot) \quad \text{Chỉ số}(\cdot, \cdot),$
 $A_1(\cdot, \cdot, \text{trạng thái}), (\cdot, \cdot, \cdot)$

nhân chứng được trích xuất

Sau đó

$\Pr[V(v_p, \cdot, \cdot) = \text{chấp nhận} \mid (C, \cdot) = 0] \geq 1 - \epsilon$ (đối với một số bỏ qua)

Định nghĩa: (2) Không có kiến thức



Waldo
ở đâu?



Định nghĩa: (2) Không có kiến thức (giản lược)

(S, P, V) là kiến thức bằng không nếu với mọi

bằng chứng “không tiết lộ điều gì” về , ngoài sự tồn tại của nó

“Không tiết lộ điều gì” có nghĩa là gì?

Định nghĩa không chính thức: “không tiết lộ điều gì” về việc liệu người xác minh có thể tự tạo ra nó không học được điều gì mới từ

(S, P, V) là kiến thức bằng không nếu có một thuật toán hiệu quả.

thứ (, , Sim) Sim(,) “giống như” thực tế , Và .

Điểm chính: Sim(, x) mô phỏng mà không cần biết

Định nghĩa: (2) Không có kiến thức (giảm lược)

Về mặt hình thức: (S, P, V) là (người xác minh trung thực) không có kiến thức về một mạch điện

nếu có một Sim mô phỏng hiệu quả như vậy

cho tất cả $'$: $(,) = \emptyset$ phân phối:

$(, , ,)$: Ở đâu $(,)$ $S()$, $P(, ,)$

không thể phân biệt được với phân phối:

$(, , ,)$: Ở đâu $(, ,)$ Giả sử $(,)$

Điểm chính: Sim $(, x)$ mô phỏng mà không cần biết

Làm thế nào để xây dựng zk-SNARK?

Nhắc lại: prover tạo ra một bằng chứng ngắn gọn , nhANH chóng để xác minh _____

Làm thế nào để xây dựng zk-SNARK?

Bài giảng tiếp theo

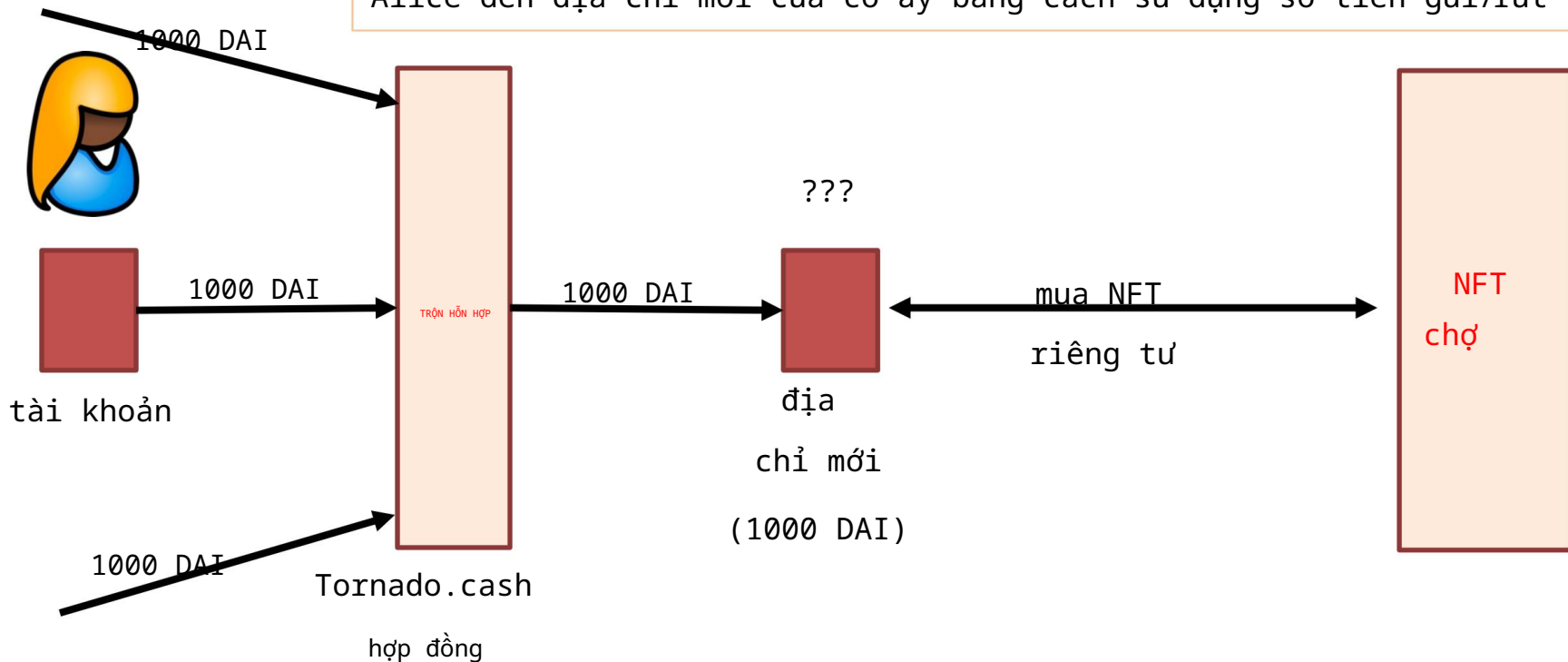
Ứng dụng của SNARK:

(1) Tornado cash: máy trộn dựa trên zk

Ra mắt trên chuỗi khối Ethereum vào tháng 5 năm 2020 (v2)

Tornado Cash: máy trộn ZK

Cần có một mệnh giá chung (1000 DAI) để ngăn chặn việc liên kết Alice đến địa chỉ mới của cô ấy bằng cách sử dụng số tiền gửi/rút



Hợp đồng tiền mặt lốc xoáy (đơn giản hóa)

Nhóm 100 DAI: mỗi

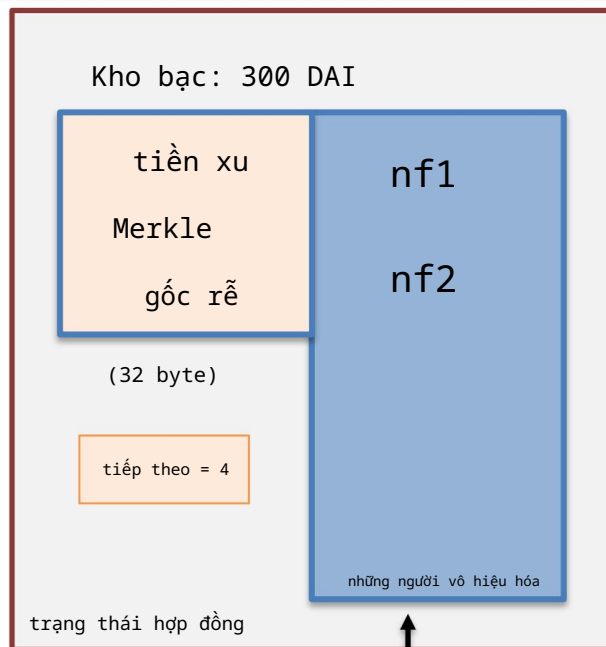
xu = 100 DAI

Hiện tại: •

ba đồng tiền trong nhóm • hợp

đồng có 300 DAI • hai bộ hủy

được lưu trữ

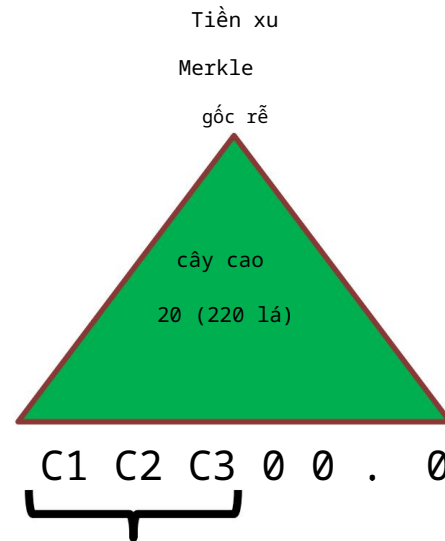


danh sách rõ

ràng: một mục nhập cho mỗi đồng xu đã chi

H1, H2: R {0,1}256

CRHF



danh sách tiền xu công khai

Tiền mặt Tornado: tiền gửi (đơn giản hóa)

Nhóm 100 DAI: mỗi

xu = 100 DAI

Alice gửi 100 DAI:



100 DAI

C4, Bảng chứng Merkle(4)

Xây dựng bảng chứng Merkle cho lá số 4:

MerkleProof(4) (lá=0)

chọn ngẫu nhiên k, r trong

R đặt $C4 = H1(k, r)$

Kho bạc: 300 DAI

tiền xu

Merkle

gốc rễ

(32 byte)

tiếp theo = 4

nf1

nf2

những người vô hiệu hóa

trạng thái hợp đồng

danh sách rõ

ràng: một mục nhập cho mỗi đồng xu đã chi

H1, H2: R {0,1}256

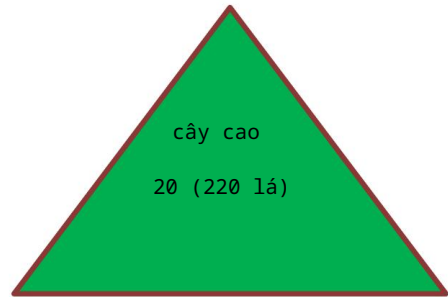
Tiền xu

Merkle

gốc rễ

cây cao

20 (220 lá)



danh sách tiền xu công khai

Tiền mặt Tornado: tiền gửi (đơn giản hóa)



100 DAI

C4 , Bảng chứng Merkle(4)

Hợp đồng Tornado có tác dụng:

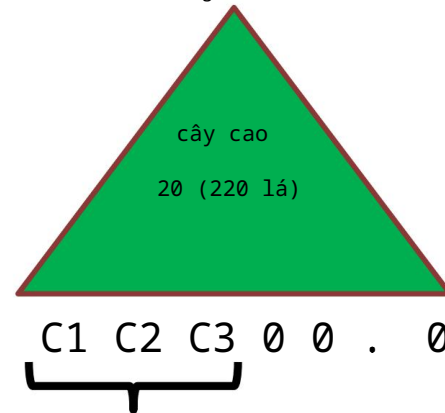
- (1) xác minh MerkleProof(4) với
liên quan đến gốc được lưu trữ hiện tại
- (2) sử dụng C4 và MerkleProof(4) để tính toán
gốc Merkle đã cập nhật
- (3) cập nhật trạng thái



Hợp đồng Tornado

H1, H2: R {0,1}256

Tiền xu
Merkle
gốc rễ



danh sách tiền xu công khai

Tiền mặt Tornado: tiền gửi (đơn giản hóa)

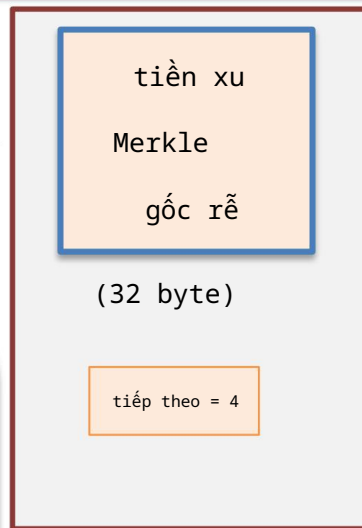


100 DAI

C4 , Bảng chứng Merkle(4)

Hợp đồng Tornado có tác dụng:

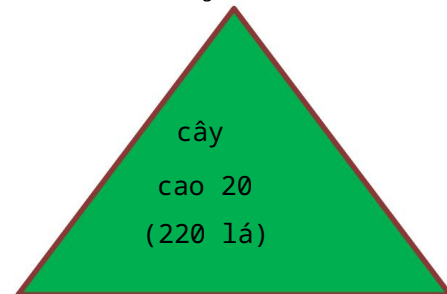
- (1) xác minh MerkleProof(4) với
liên quan đến gốc được lưu trữ hiện tại
- (2) sử dụng **C4** và MerkleProof(4) để tính toán
gốc Merkle đã cập nhật
- (3) cập nhật trạng thái



Hợp đồng Tornado

H1, H2: R {0,1}256

đã cập nhật
Merkle
gốc rễ



C1 C2 C3 **C4** 0 . 0

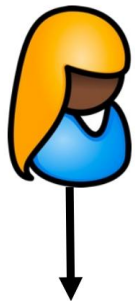
danh sách tiền xu công khai

Tiền mặt Tornado: tiền gửi (đơn giản hóa)

Nhóm 100 DAI: mỗi

xu = 100 DAI

Alice gửi 100 DAI:



100 DAI

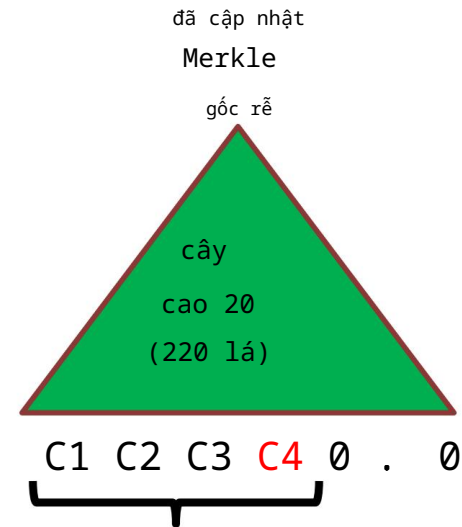
C4 , Bằng chứng Merkle(4)

chú thích: (k, r)

Alice giữ bí mật (một
tờ tiền cho mỗi đồng xu)



Mỗi khoản tiền gửi: Coin mới
được thêm vào cây theo trình tự



danh sách tiền xu công khai

người quan sát thấy ai sở
hữu lá nào

Tornado cash: rút tiền (đơn giản hóa)

Nhóm 100 DAI: mỗi

xu = 100 DAI

Rút coin số 3 vào

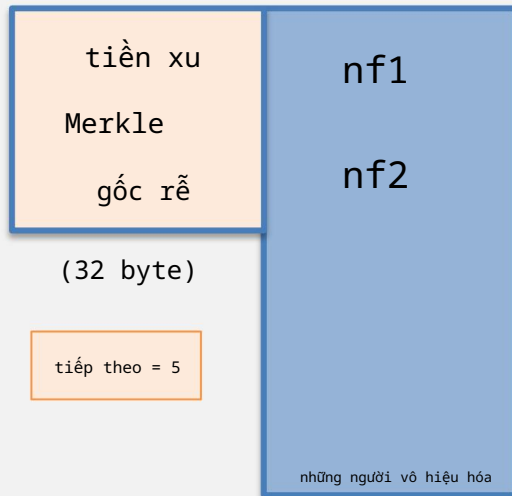
địa chỉ A:



có ghi chú = (k', r')

đặt $nf = H2(k')$

Kho bạc: 400 DAI



tiếp theo = 5

trạng thái hợp đồng

$H1, H2: R \quad \{0,1\}^{256}$

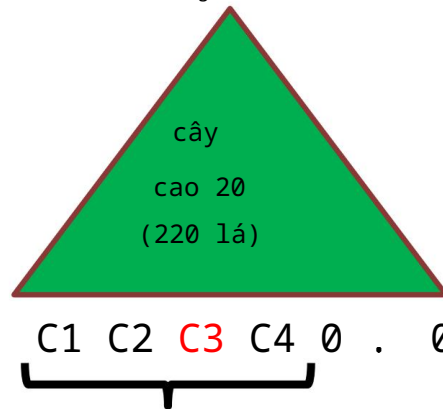
Merkle

gốc rễ

cây

cao 20

(220 lá)



danh sách tiền xu công khai

Bob chứng minh “Tôi có một ghi chú cho một số lá trong cây tiền xu, và số vô hiệu của nó là nf ” (mà không tiết lộ đồng tiền nào)

Tornado cash: rút tiền (đơn giản hóa)

Rút coin số 3 vào địa chỉ A:



có ghi chú = (k', r') đặt $nf = H2(k')$

Bob xây dựng bằng chứng zk-SNARK cho

tuyên bố công khai $x = (\text{root}, nf, A)$ nhân chứng

bí mật $w = (k', r', C3, \text{MerkleProof}(C3))$

trong đó $\text{Circuit}(x, w) = 0$ nếu và chỉ nếu:

(i) $C3 = (\text{lá số 3 của gốc})$, tức là $\text{MerkleProof}(C3)$ là hợp lệ,

(ii) $C3 = H1(k', r')$, và

(iii) $nf = H2(k')$.

$H1, H2: R \rightarrow \{0,1\}^{256}$

Merkle

gốc rễ

cây

cao 20

(220 lá)

C1 C2 C3 C4 0 . 0

(địa chỉ A không được sử dụng trong Circuit)

Tornado cash: rút tiền (đơn giản hóa)

H1, H2: R {0,1}256

Rút coin số 3 vào địa chỉ A:

Địa chỉ A là một phần của câu lệnh để đảm bảo rằng thợ đào không thể thay đổi A
 địa chỉ riêng của nó và đánh cấp tiền
 thành $has_note = (k', r') \text{ set } nf = H2(k')$

Merkle
gốc rễ

Giả sử SNARK không thể thay đổi được:

đối thủ không thể sử dụng bằng chứng cho x để xây dựng bằng chứng cho một số x "có liên quan"
 (ví dụ, trong x' địa chỉ A được thay thế bằng một số A')

cây của
chiều cao 20

(220 lá)

C1 C2 C3 C4 0 . 0

Bob xây dựng bằng chứng zk-SNARK cho

tuyên bố công khai $x = (\text{root}, nf, A)$

nhân chứng bí mật $w = (k', r', C3, \text{MerkleProof}(C3))$

Tornado cash: rút tiền (đơn giản hóa)

Nhóm 100 DAI: mỗi

xu = 100 DAI

Rút coin số 3 vào địa

chỉ A:



nf, bằng chứng, A

(trên Tor)

Không tiết lộ ID và đồng xu C3 của Bob

Kho bạc: **400** DAI

tiền xu

Merkle

gốc rễ

(32 byte)

tiếp theo = 5

nf1

nf2

những người vô hiệu hóa

trạng thái hợp đồng

H1, H2: R {0,1}256

Merkle

gốc rễ

cây

cao 20

(220 lá)

C1 C2 **C3** C4 0 . 0

danh sách tiền xu công khai

Hợp đồng kiểm tra (i) bằng chứng có giá trị đối với (root, **nf**, A) và (ii)

nf không nằm trong danh sách các phần tử vô hiệu

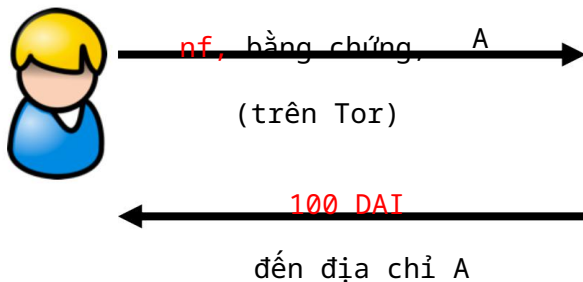
Tornado cash: rút tiền (đơn giản hóa)

Nhóm 100 DAI: mỗi

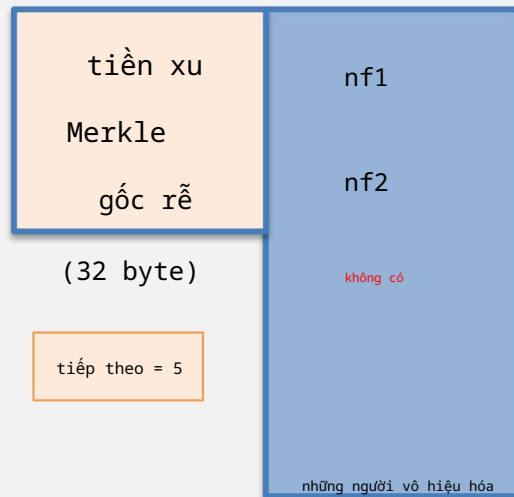
xu = 100 DAI

Rút coin số 3 vào địa

chỉ A:



Kho bạc: 300 DAI

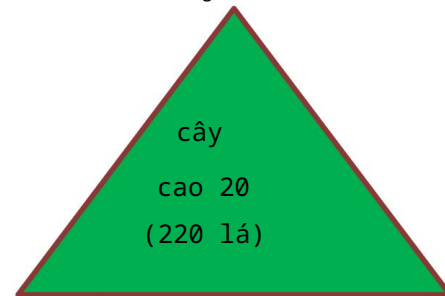


trạng thái hợp đồng

H1, H2: R {0,1}256

Merkle

gốc rễ



C1 C2 C3 C4 0 . 0

danh sách công khai các

đồng tiền . nhưng người quan sát

không biết đồng nào đã được chi tiêu

nf và không tiết lộ bất cứ thông tin gì về đồng tiền đã được chi tiêu.

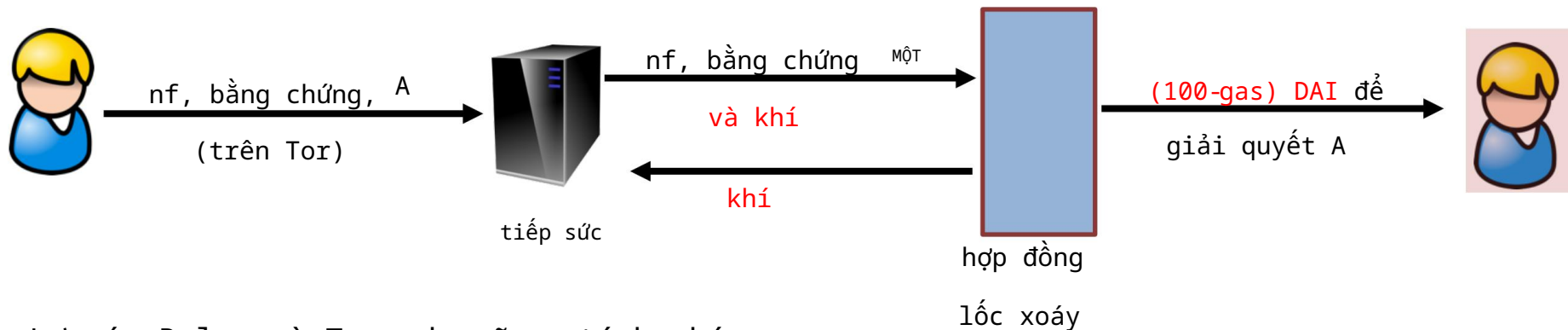
Tuy nhiên, đồng xu số 3 không thể được chi tiêu lần nữa vì $nf = H2(k')$ hiện đã bị vô hiệu.

Ai là người trả phí gas rút tiền?

Vấn đề: Bob trả tiền xăng cho giao dịch rút tiền Tx như thế nào?

- Nếu trả từ địa chỉ của Bob, thì địa chỉ mới sẽ được liên kết với Bob

Giải pháp của Tornado: Bob sử dụng rơle



Lưu ý: Relay và Tornado cũng tính phí

Tornado Cash: Giao diện người dùng

Deposit

Withdraw

Token

DAI

Amount

100 DAI1K DAI10K DAI100K DAI

Sau khi gửi tiền: nhận được ghi chú

Deposit

Withdraw

Note

Please enter your note

Recipient Address

Địa chỉ

Donate

Sau đó, sử dụng ghi chú để rút tiền

(chờ trước khi rút lui)

Rắc rối lốc xoáy . lệnh trừng phạt của Hoa Kỳ

Vụ tấn công cầu Ronin (năm 2022): •

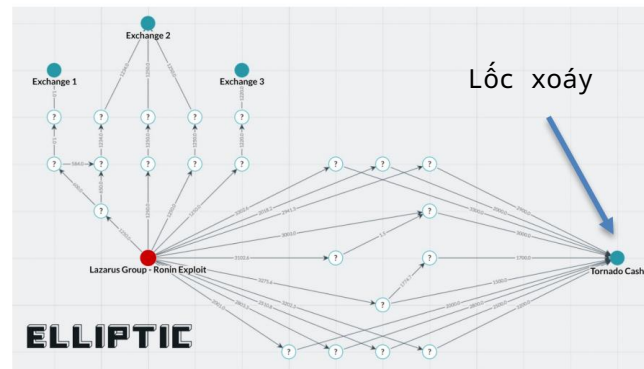
Cuối tháng 3: ~600 triệu đô la Mỹ bị đánh cắp. 80 triệu đô la Mỹ được gửi

đến Tornado • Tháng 4: Nhóm Lazarus bị nghi ngờ

tấn công • Tháng 8: "Bộ Tài chính Hoa Kỳ trừng phạt Máy trộn tiền ảo

Tornado Cash" • Nhiều thiệt hại tài sản thế chấp. và hai vụ kiện

Bài học: tính ẩn danh hoàn toàn trong hệ thống
thanh toán là vấn đề



Trùng phạt

“Các quy định trùng phạt của Hoa Kỳ sẽ không cấm công dân Hoa Kỳ sao chép mã nguồn mở và cung cấp trực tuyến để người khác xem, cũng như thảo luận, giảng dạy hoặc đưa mã nguồn mở vào các ấn phẩm viết, chẳng hạn như sách giáo khoa, trừ khi có thêm thông tin thực tế”

[Câu hỏi thường gặp về Bộ Tài chính Hoa Kỳ](#), Tháng 9 năm 2022

Thiết kế một chiếc Tornado tuân thủ quy định?

(1) lọc tiền gửi: đảm bảo tiền gửi vào không bị xử phạt

Hợp đồng Chainalysis SanctionsList :

```
hàm isSanctioned(địa chỉ địa chỉ) chế độ xem công khai trả về (bool)
    { trả về approvedAddresses[địa chỉ] == true ;
    }
```

Từ chối các khoản tiền đến từ địa chỉ đã bị xử phạt.

Khó khăn: (1) tập trung, (2) cập nhật chậm

Thiết kế một chiếc Tornado tuân thủ quy định?

(2) Lọc rút tiền: khi rút tiền, yêu cầu bằng chứng ZK chứng minh nguồn tiền hiện không nằm trong danh sách bị xử phạt.

Làm sao?

- sửa đổi cách Tornado tính toán lá Merkle trong quá trình gửi tiền để bao gồm `msg.sender`.

trong ví dụ của chúng tôi, Alice đặt: $C4 = [H1(k, r), \text{msg.sender}]$

- Trong quá trình rút tiền, Bob chứng minh với ZK rằng người gửi tin nhắn trong danh sách của anh ta hiện không có tên trong danh sách trừng phạt.

Thiết kế một chiếc Tornado tuân thủ quy định?

(3) Xem khóa: khi rút tiền, yêu cầu người hủy bỏ phải bao gồm mã hóa tin nhắn gửi tiền của người gửi theo khóa công khai của chính phủ.

Làm thế nào? Merkle leaf **C4** được tính như ở slide trước.

- Trong khi rút lui, Bob đặt bộ vô hiệu hóa **nf** = [$H_2(k')$, ,]
 trong đó (i) = $\text{Enc}(pk, \text{msg.sender})$ và (ii) là
 bằng chứng ZK được tính toán chính xác

Khi cần thiết, chính phủ có thể theo dõi nguồn tiền thông qua Tornado

- có rất nhiều vấn đề với thiết kế này .

Các dự án tư nhân khác của Tx

Zcash / IronFISH: thanh toán riêng tư •

Blockchain L1 mở rộng Bitcoin, sử dụng Nullifiers tương tự. • Hỗ trợ mọi giao dịch Tx có giá trị và chuyển khoản trong hệ thống.

Aztec / Aleo:

- Hỗ trợ giao dịch riêng tư tương tác với hợp đồng thông minh công khai.
- Aleo: chuỗi khối L1. Aztec: chạy trên Ethereum.

KẾT THÚC BÀI GIẢNG

Bài giảng tiếp theo: cách xây dựng SNARK

Các chủ đề khác

Giao tiếp riêng tư với blockchain: Nym

- Cách thức bồi thường riêng cho các proxy để chuyển tiếp lưu lượng truy cập

Bài giảng tiếp theo: cách xây dựng SNARK