Rapidash:

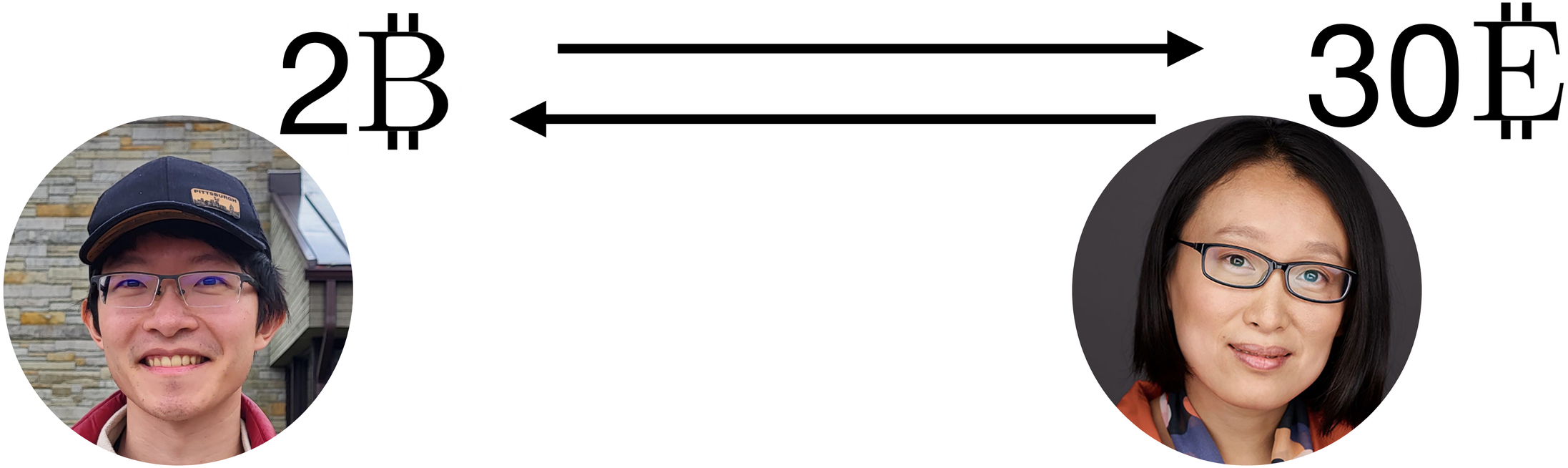
Atomic Swaps Secure under User-Miner Collusion

Hao Chung (Carnegie Mellon University)

Joint work with Elisaweta Masserova, Elaine Shi, and Sri AravindaKrishnan Thyagarajan

Atomic swap

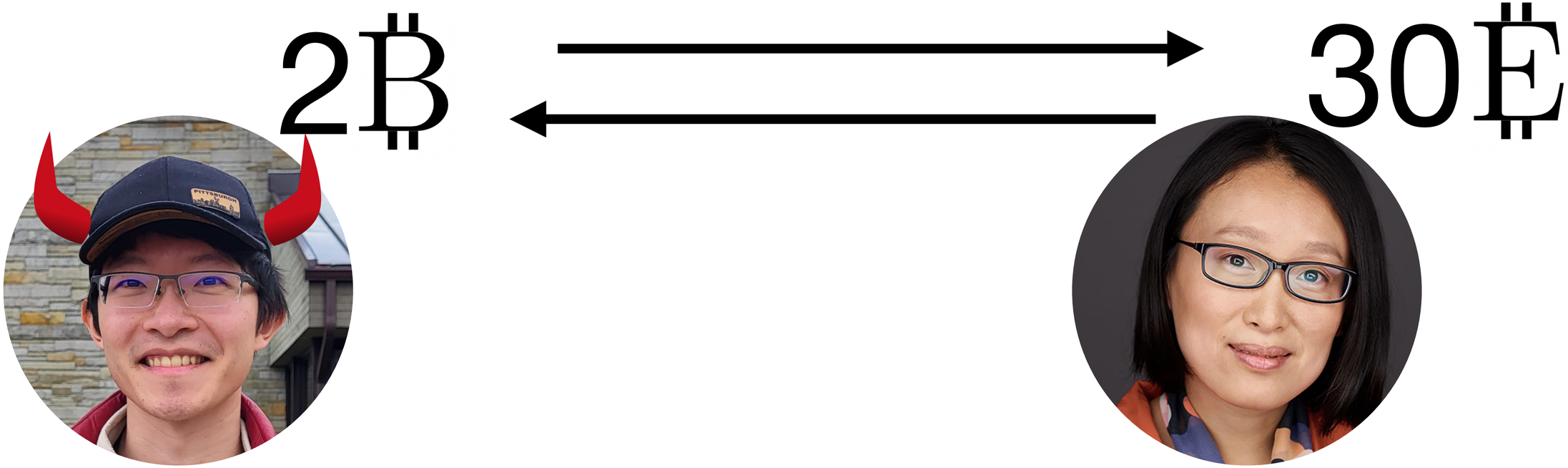
Either both parties get their desired items or neither



Atomic swap

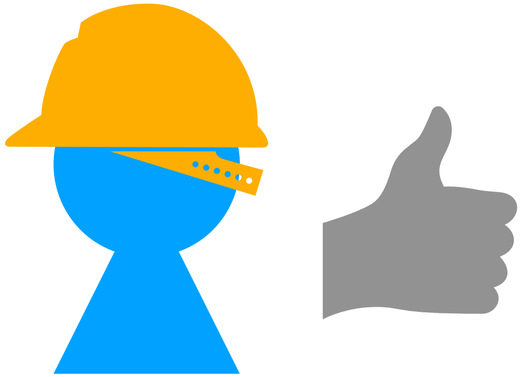
Either both parties get their desired items or neither

even if parties may deviate from the protocol



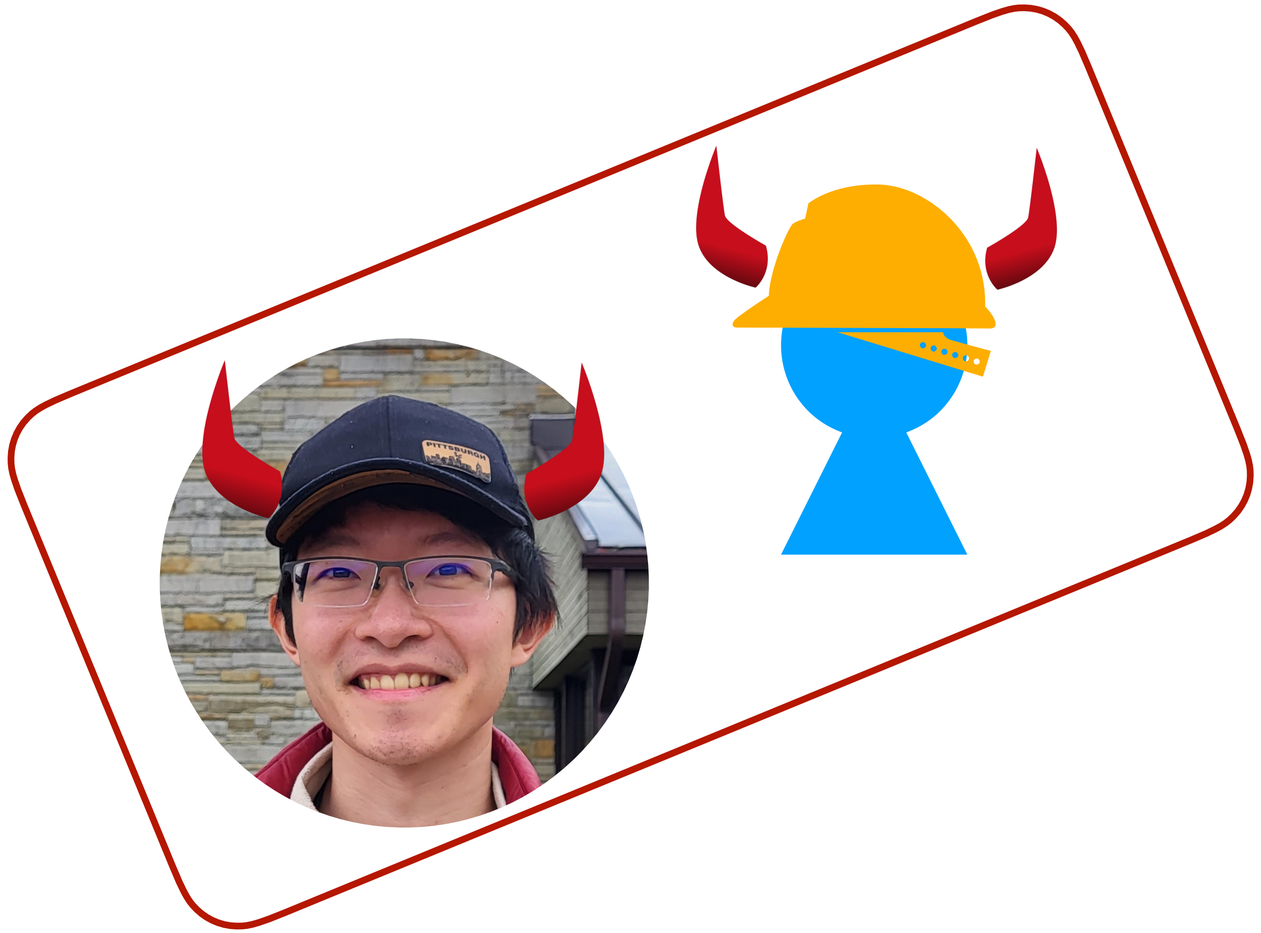
Ideal world: miners are honest

Existing protocol works if miners always follow the protocol



Real world: user-miner coalition

Miners may collude with users and deviate from the protocol



Real world: user-miner coalition

Split the profit through side contract

smart contract

Can we design an atomic swap protocol that defends against arbitrary user-miner coalition?

Roadmap

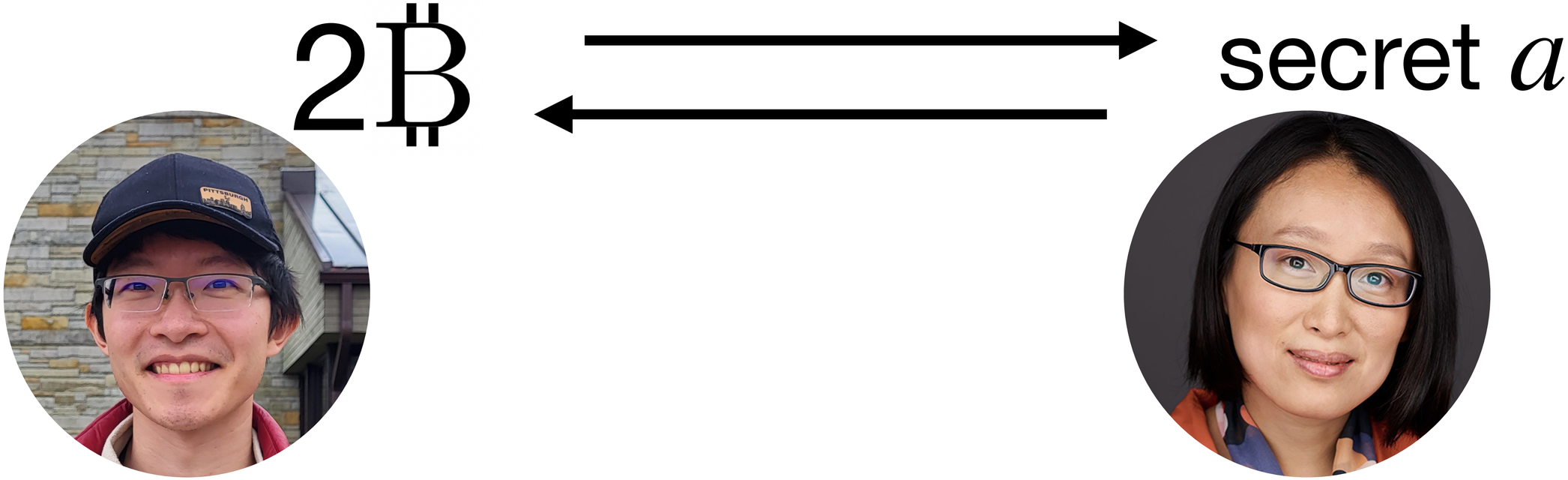
1. Building block: knowledge-coin exchange

   - current protocols are not side-contract resilient

   - our solution

2. From knowledge-coin exchange to atomic swap

Knowledge-coin exchange



Simple protocol achieves side-contract resilient

2฿

secret a

-  deposits 2฿
- On receiving a such that $H(a) = h$, send 2฿ to 

Simple protocol achieves side-contract resilient

2฿

secret a

-  deposits 2฿
- On receiving a such that $H(a) = h$, send 2฿ to 

Coins locked by a hash value

However, it's not dropout resilient

If  drop outs,  's coin is locked forever

-  deposits 2฿
- On receiving a such that $H(a) = h$, send 2฿ to 

What we want for atomic swap protocol?

Side-contract resilience

- no miner-user coalition can increase their joint utility

Dropout resilience

- honest users should not be harmed if the other user drops out anytime

Knowledge-coin exchange

In practice, realized by Hashed Time-Locked Contracts (HTLC)

Knowledge-coin exchange

In practice, realized by Hashed Time-Locked Contracts (HTLC)

-  deposits 2฿

Knowledge-coin exchange

In practice, realized by Hashed Time-Locked Contracts (HTLC)

-  deposits 2฿
- On receiving a such that $H(a) = h$,

  send 2฿ to 

Knowledge-coin exchange

In practice, realized by Hashed Time-Locked Contracts (HTLC)

-  deposits 2฿
- On receiving a such that $H(a) = h$,

  send 2฿ to 
- After time T, receive "OK" from 

  send 2฿ to 

HTLC is vulnerable to  - miner coalition

Miners delay  's tx, and  gets refunded after time T

-  deposits 2฿
- On receiving a such that $H(a) = h$,

  send 2฿ to 
- After time T, receive "OK" from 

  send 2฿ to 

MAD-HTLC

- Users need to put collateral
- Defend against only some specific attacks

MAD-HTLC: Because HTLC is Crazy-Cheap to Attack,
by Itay Tsabary, Matan Yechieli, Alex Manuskin, Ittay Eyal

Roadmap

1. Building block: knowledge-coin exchange

   - current protocols are not side-contract resilient

   - our solution

2. From knowledge-coin exchange to atomic swap

Rapidash: make HTLC side-contract resilient

deposits $\text{฿}v + \text{฿}c$

payment

collateral

Rapidash: make HTLC side-contract resilient

deposits $\text{฿}v + \text{฿}c$

P1

P2

C1

C2

Good case: responsive

deposits $฿v + ฿c$

P1

On receiving a, send $฿v$ to  and send $฿c$ to 

P2

C1

C2

If the secret seller  drops out

 deposits $\text{฿}v + \text{฿}c$

P1 On receiving a, send $\text{฿}v$ to  and send $\text{฿}c$ to 

P2 Time $\geq T_1$, on receiving b, do nothing

C1 Time T_2 after P2, send $\text{฿}v + \text{฿}c$ to 

C2

The buyer cannot learn the secret for free

deposits $\text{฿}v + \text{฿}c$

P1 On receiving a, send $\text{฿}v$ to  and send $\text{฿}c$ to 

P2 Time $\geq T_1$, on receiving b, do nothing

C1 Time T_2 after P2, send $\text{฿}v + \text{฿}c$ to 

C2 On receiving (a, b) from anyone, send it $\text{฿}\epsilon$ and **burn the rest**

The buyer cannot learn the secret for free

deposits $\text{฿}v + \text{฿}c$

P1 On receiving a, send $\text{฿}v$ to  and send $\text{฿}c$ to 

P2 Time $\geq T_1$, on receiving b, do nothing

C1 Time T_2 after P2, send $\text{฿}v + \text{฿}c$ to 

C2 On receiving (a, b) from anyone, send it $\text{฿}\epsilon$ and **burn the rest**

Concurrent work: *He-HTLC: Revisiting Incentives in HTLC* by Sarisht Wadhwa, Jannis Stoeter, Fan Zhang, Kartik Nayak

Rapidash defends against arbitrary side-contract

Rapidash defends against arbitrary side-contract

- Disincentivize 100% miner coalition

Rapidash defends against arbitrary side-contract

- Disincentivize 100% miner coalition
- Bitcoin compatible

How to set up parameters?

- $v > \epsilon$
- $c > \epsilon$
- $\gamma^{T_2} \leq \dfrac{c}{v + c}$, where $\gamma \in [0,1]$ is strategic mining fraction

Example: If γ = 49%, set $c = v/10$, $\epsilon = 0.9v$, $T_2 = 4$

Roadmap

1. Building block: knowledge-coin exchange

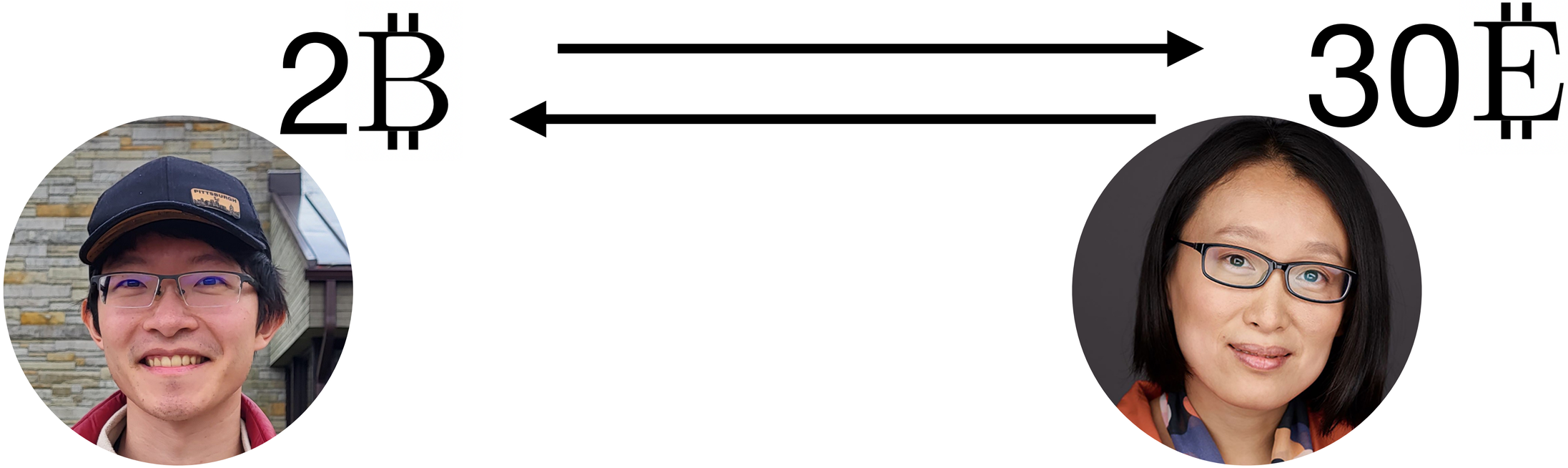
   - current protocols are not side-contract resilient

   - our solution

2. From knowledge-coin exchange to atomic swap

Atomic swap

Either both parties get their desired items or neither



Achieving coin swap

2฿

30Ξ

Achieving coin swap

2฿

30Ξ

1 randomly choose a

Achieving coin swap

2฿

30Ξ

1 randomly choose a

knowledge-coin ex on Ethereum

-  deposits 30Ξ

2

locked by a

Achieving coin swap

2฿

30Ξ

1 randomly choose a

knowledge-coin ex on Bitcoin

-  deposits 2฿ 3

  locked by a

knowledge-coin ex on Ethereum

-  deposits 30Ξ 2

  locked by a

Achieving coin swap

2฿

30Ξ

1 randomly choose a

knowledge-coin ex on Bitcoin

-  deposits 2฿ 3

  locked by a

knowledge-coin ex on Ethereum

-  deposits 30Ξ 2

  locked by a

4  sends a to get 2฿

Achieving coin swap

2฿

30Ξ

1 randomly choose a

knowledge-coin ex on Bitcoin

-  deposits 2฿ 3

  locked by a

knowledge-coin ex on Ethereum

-  deposits 30Ξ 2

  locked by a

4  sends a to get 2฿

5  sends a to get 30Ξ

can attack the other contract after getting collateral back

2Ƀ

30Ξ

1 randomly choose a

knowledge-coin ex on Bitcoin

-  deposits 2Ƀ 3

knowledge-coin ex on Ethereum

-  deposits 30Ξ 2

can attack the other contract after getting collateral back

2Ƀ

30Ξ

1 randomly choose a

knowledge-coin ex on Bitcoin

-  deposits 2Ƀ 3

knowledge-coin ex on Ethereum

-  deposits 30Ξ 2

4  after timeout, get 30Ξ

can attack the other contract after getting collateral back

2Ƀ

30Ξ

1 randomly choose a

knowledge-coin ex on Bitcoin

-  deposits 2Ƀ 3

knowledge-coin ex on Ethereum

-  deposits 30Ξ 2

5  ’s tx is delayed

4  after timeout, get 30Ξ

can attack the other contract after getting collateral back

2Ƀ

30Ξ

1 randomly choose a

knowledge-coin ex on Bitcoin

-  deposits 2Ƀ 3

knowledge-coin ex on Ethereum

-  deposits 30Ξ 2

5  ’s tx is delayed

6  send a to get 2Ƀ

4  after timeout, get 30Ξ

can attack the other contract after getting collateral back

2Ƀ

30Ξ

1 randomly choose a

knowledge-coin ex on Bitcoin

-  deposits 2Ƀ 3

knowledge-coin ex on Ethereum

-  deposits 30Ξ 2

5  's tx is delayed

4  after timeout, get 30Ξ

6  send a to get 2Ƀ

The secret a worths nothing now!

Directly combining two Rapidashs

does not give you side-contract

resilient coin swap

Achieving side-contract resilient

2฿

30Ξ

knowledge-coin ex on Bitcoin

-  deposits 2฿

knowledge-coin ex on Ethereum

-  deposits 30Ξ

Achieving side-contract resilient

2฿

30Ξ

knowledge-coin ex on Bitcoin

-  deposits 2฿

knowledge-coin ex on Ethereum

-  deposits 30Ξ

more possibilities to invoke the bomb

Achieving side-contract resilient

2฿

30Ξ

knowledge-coin ex on Bitcoin

-  deposits 2฿

knowledge-coin ex on Ethereum

-  deposits 30Ξ

one more hash value to protect the coins

more possibilities to invoke the bomb

More in our paper

More in our paper

Full coin swap protocol

More in our paper

Full coin swap protocol

Resilience against external incentives

More in our paper

Full coin swap protocol

Resilience against external incentives

- secure against arbitrary but bounded external incentives

More in our paper

Full coin swap protocol

Resilience against external incentives

- secure against arbitrary but bounded external incentives

Bitcoin instantiation

More in our paper

Full coin swap protocol

Resilience against external incentives

- secure against arbitrary but bounded external incentives

Bitcoin instantiation

eprint 2022/1063

email: haochung@andrew.cmu.edu

Thank you!