BlindHub: Bitcoin-Compatible Privacy-Preserving Payment Channel Hubs Supporting Variable Amounts

Xianrui Qin, Shimin Pan, Arash Mirzaei, Zhimei Sui, Oguzhan Ersoy, Amin Sakzad, Muhammed F. Esgin, Joseph K. Liu, Jiangshan Yu, Tsz Hon Yuen

MONASH University

Radboud Universiteit

TU Delft Delft University of Technology

Outline

- Introduction

Outline

- Introduction
  - Private payments

Outline

- Introduction
  - Private payments
    - Private payments on Bitcoin Network

Outline

- Introduction
  - Private payments
    - Private payments on Bitcoin Network
  - Our solutions

Outline

- Introduction
  - Private payments
    - Private payments on Bitcoin Network
  - Our solutions
  - Comments on this line of work

Outline

- Introduction
  - Private payments
    - Private payments on Bitcoin Network
- Our solutions
- Comments on this line of work
- Future

Payments

Private Payments

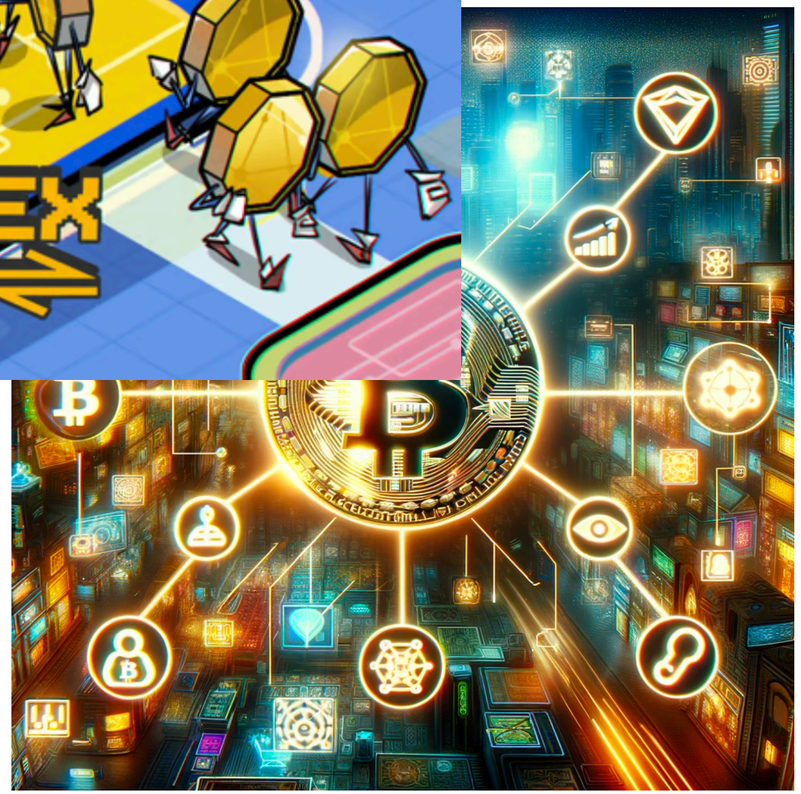
Private Payments

Bitcoin !

Bitcoin !

Bitcoin !

Bitcoin !



Bitcoin:
To The Moon!

Congestion…

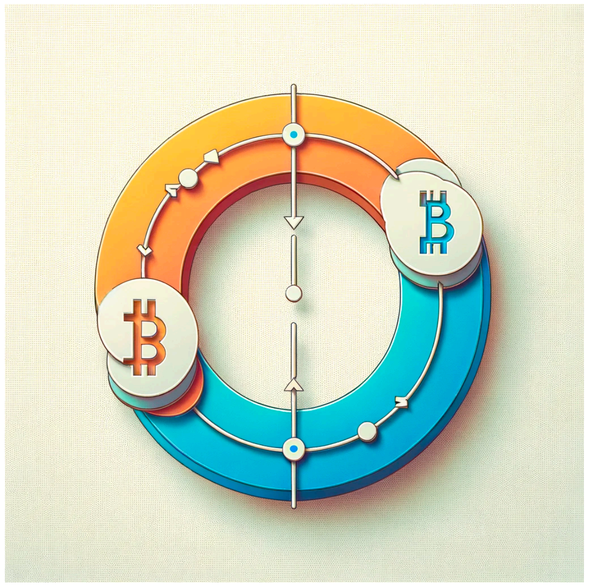
Scaling Bitcoin

Scaling Bitcoin

Payment Channel
(Lghtning Network)

Scaling Bitcoin

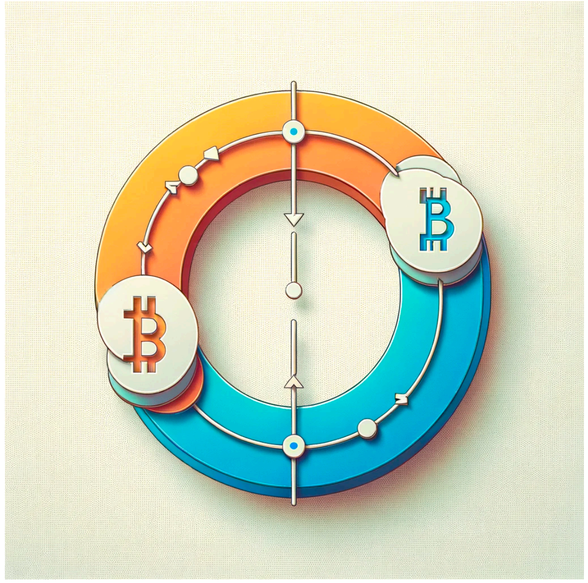
Payment Channel
(Lghtning Network)



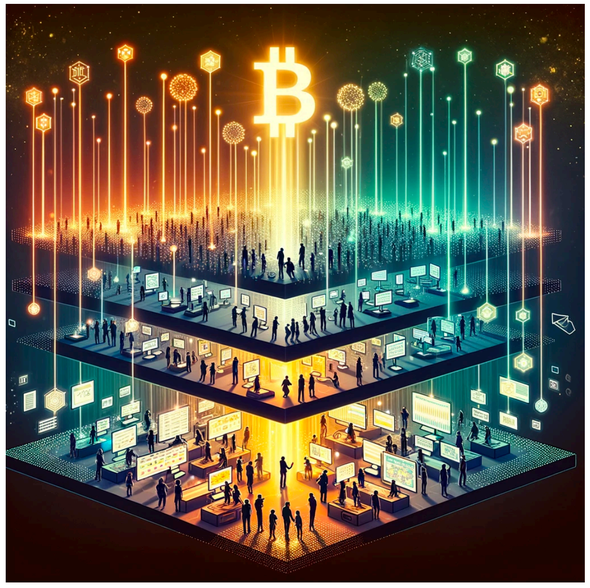
Side Chain
(Liquid Network)

Scaling Bitcoin

Payment Channel
(Lghtning Network)



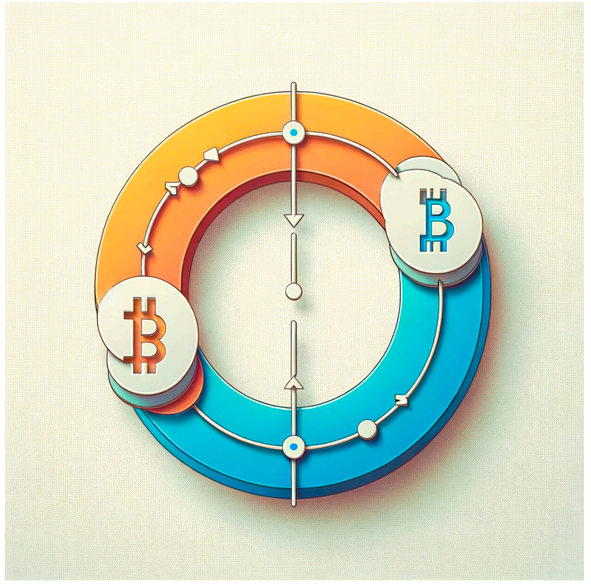
Side Chain
(Liquid Network)



RGB, BitVM,
Bitcoin Rollup…

Scaling Bitcoin

Payment Channel
(Lghtning Network)

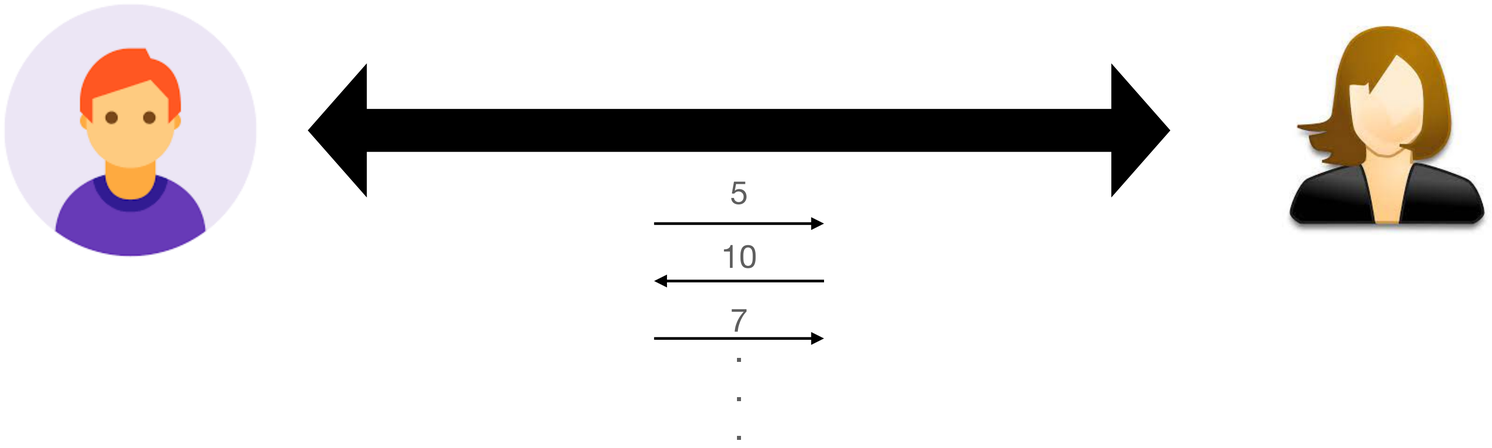


Side Chain
(Liquid Network)

RGB, BitVM,
Bitcoin Rollup…

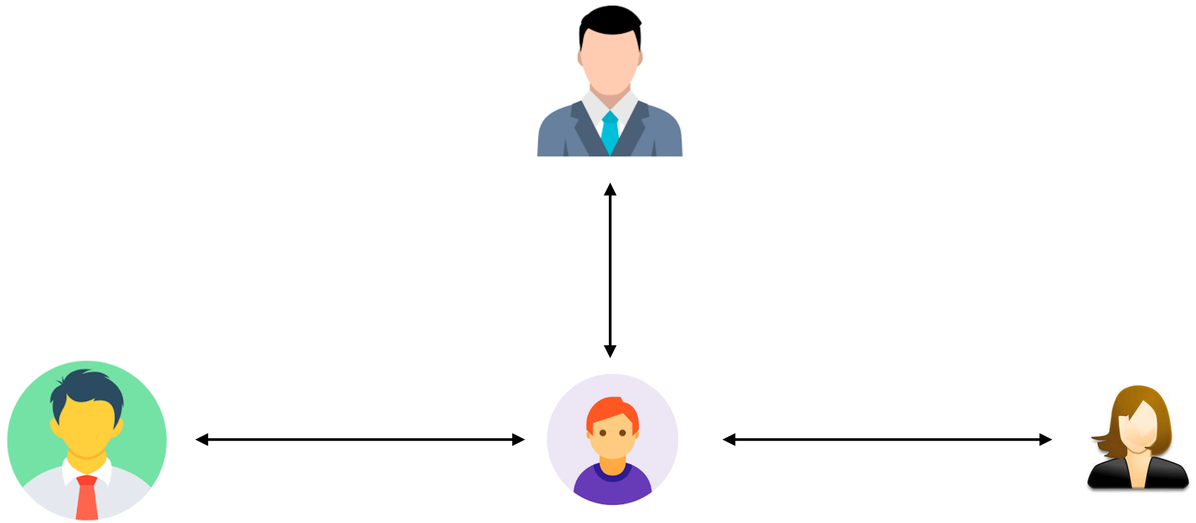
Payment Channel

- Payment channel is regarded as one of the most promising solutions for addressing scalability problem
  - Payment channels allow for unlimited off-chain payments, with only the channel's opening and closing recorded on the blockchain

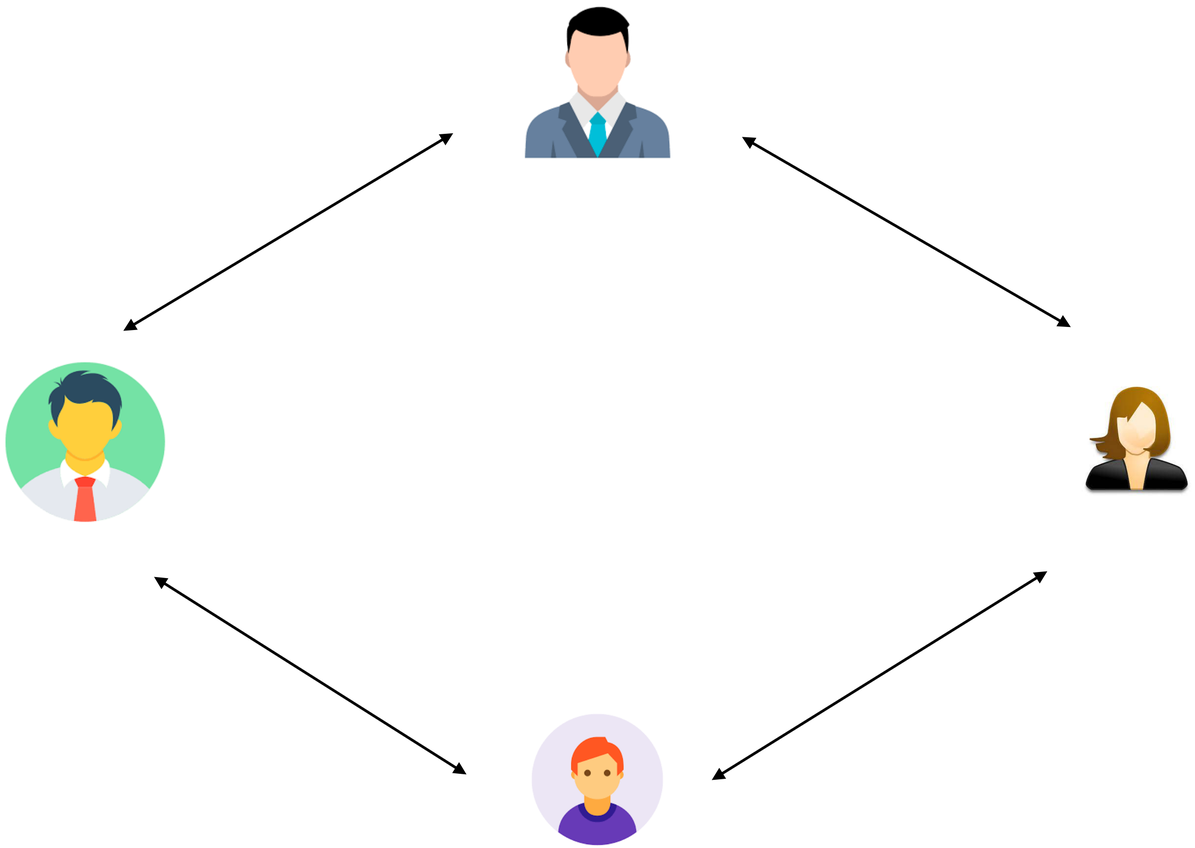


Payment Channel

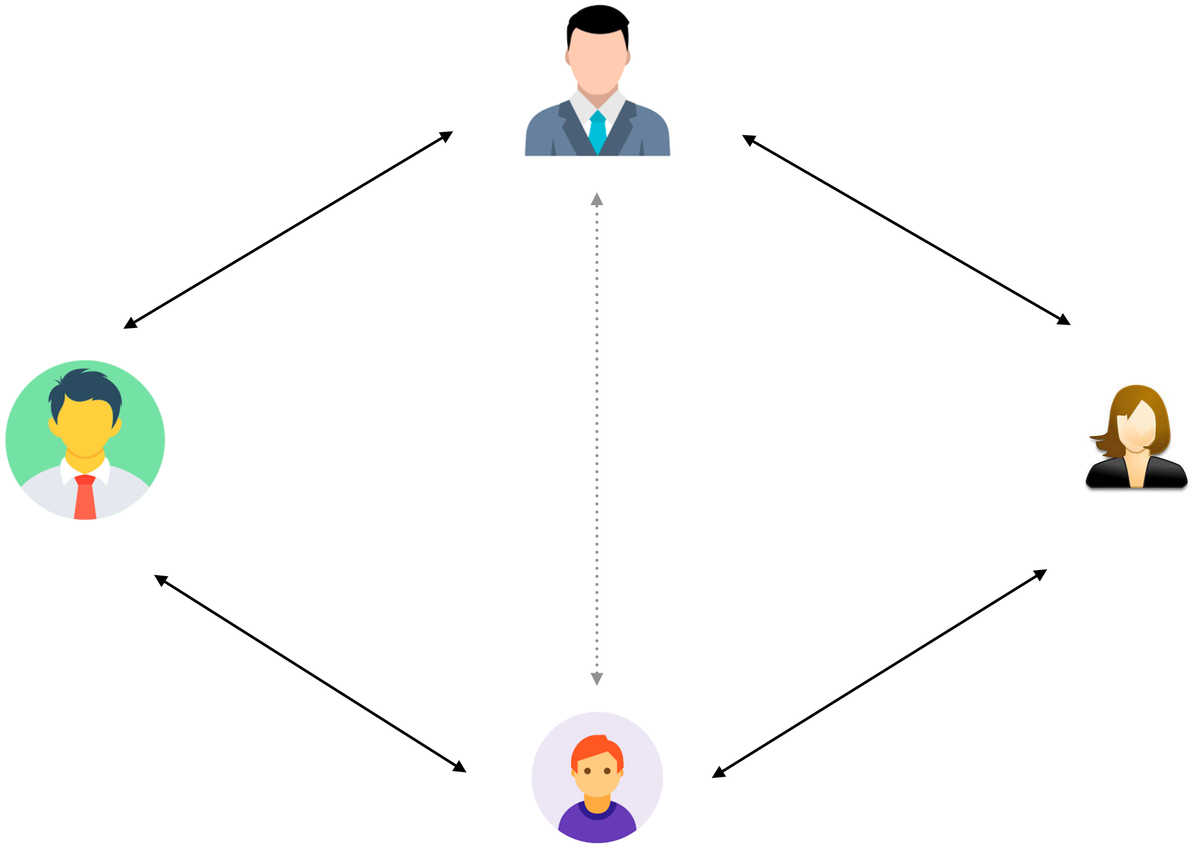
- Payment channel is regarded as one of the most promising solutions for addressing scalability problem
  - Payment channels allow for unlimited off-chain payments, with only the channel's opening and closing recorded on the blockchain
  - Financially infeasible to build channel with everyone



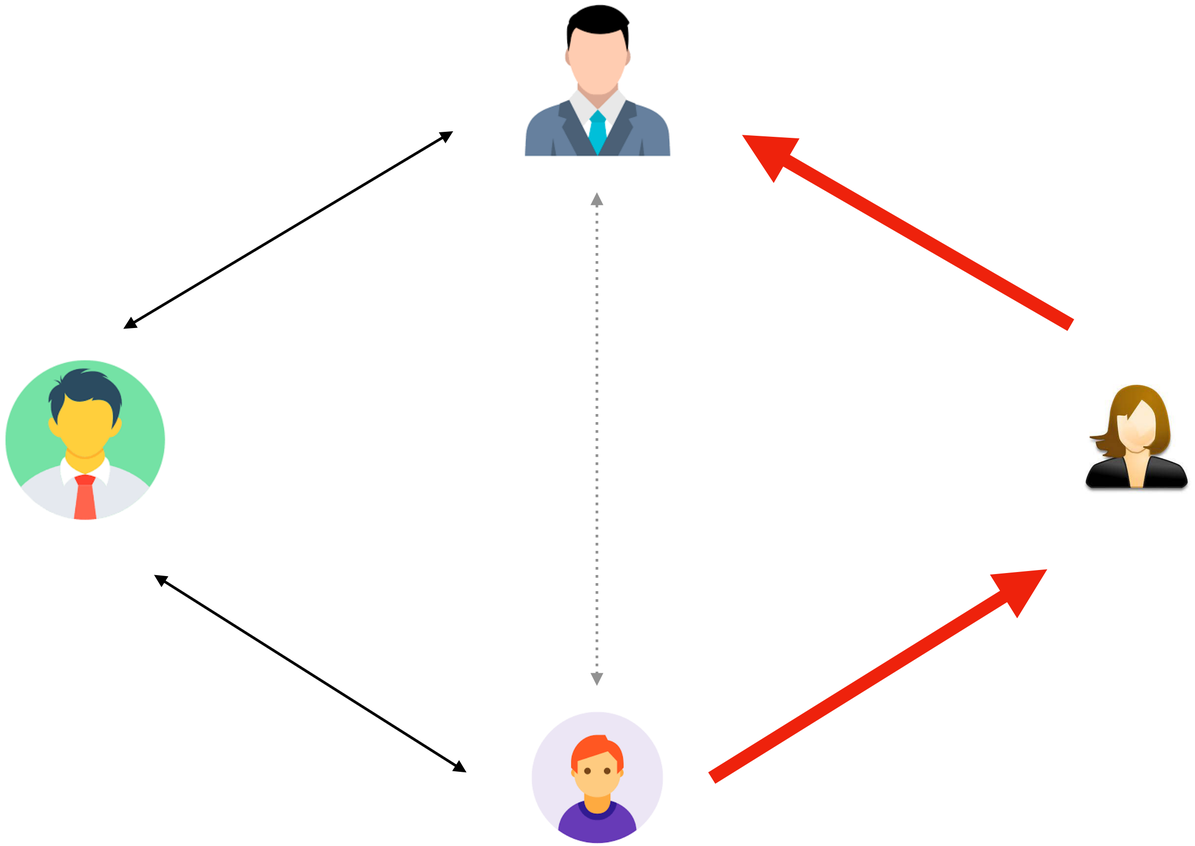
Payment Channel Network



Payment Channel Network

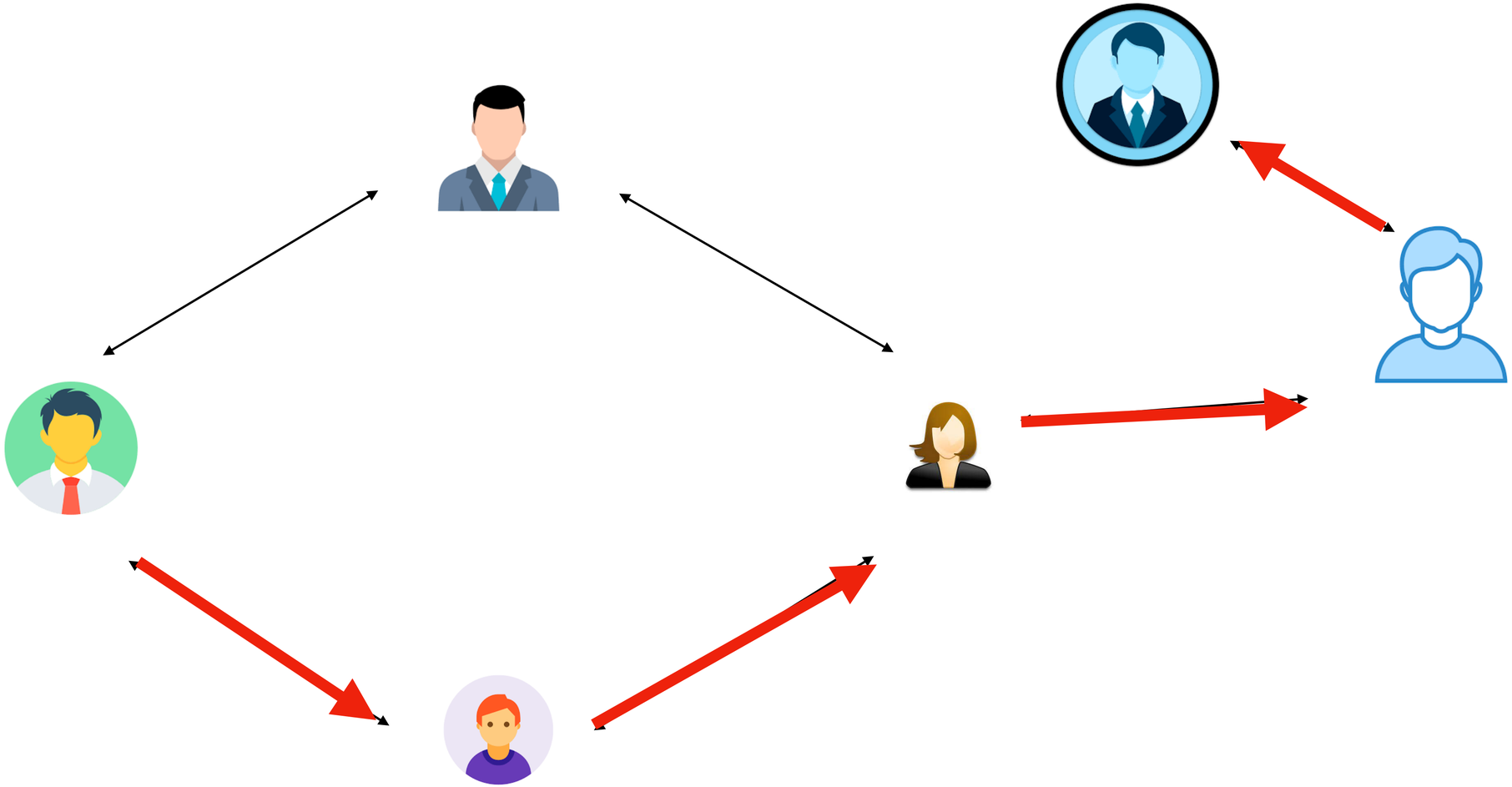


Payment Channel Network

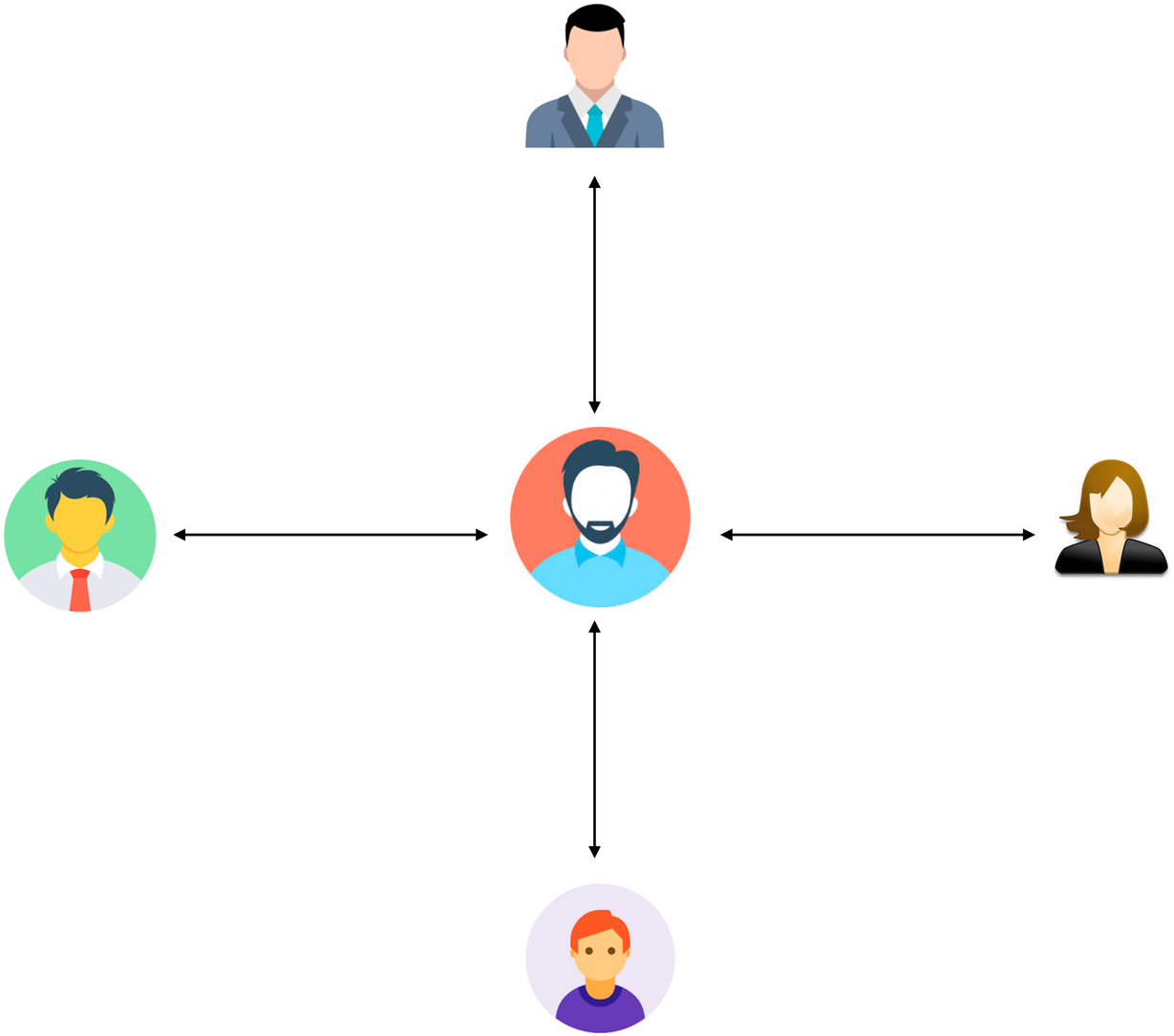


Payment Channel Network

- Require routing, active participation of parties

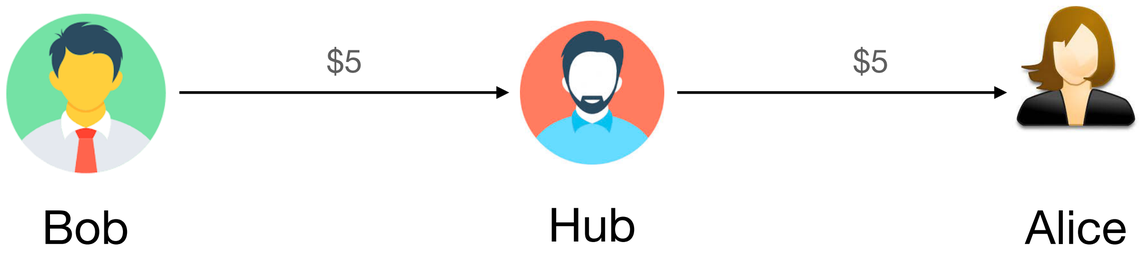


Payment Channel Hub

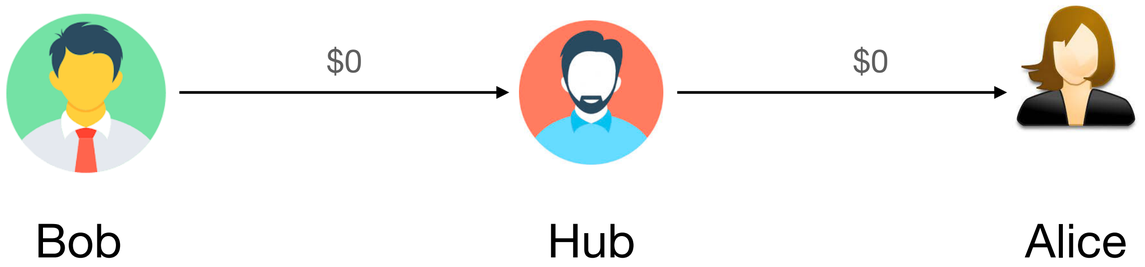


Payment Channel Hub

- Atomicity: Either Alice receives m coins from hub and hub receives m coins from Bob, or both parties receive none.

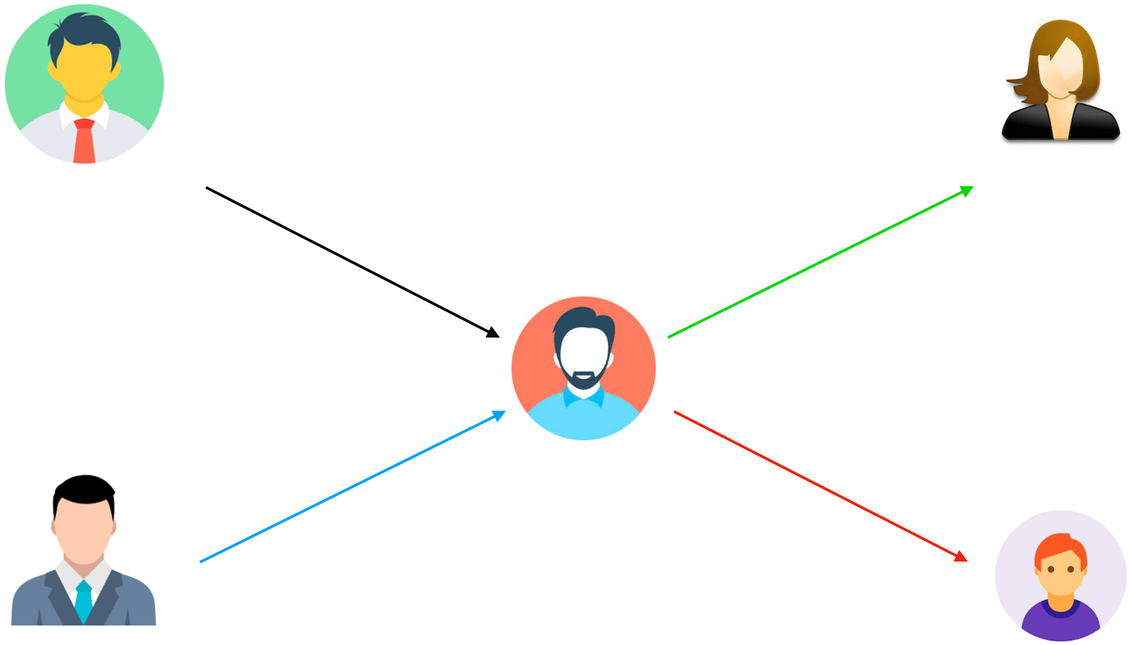


Or



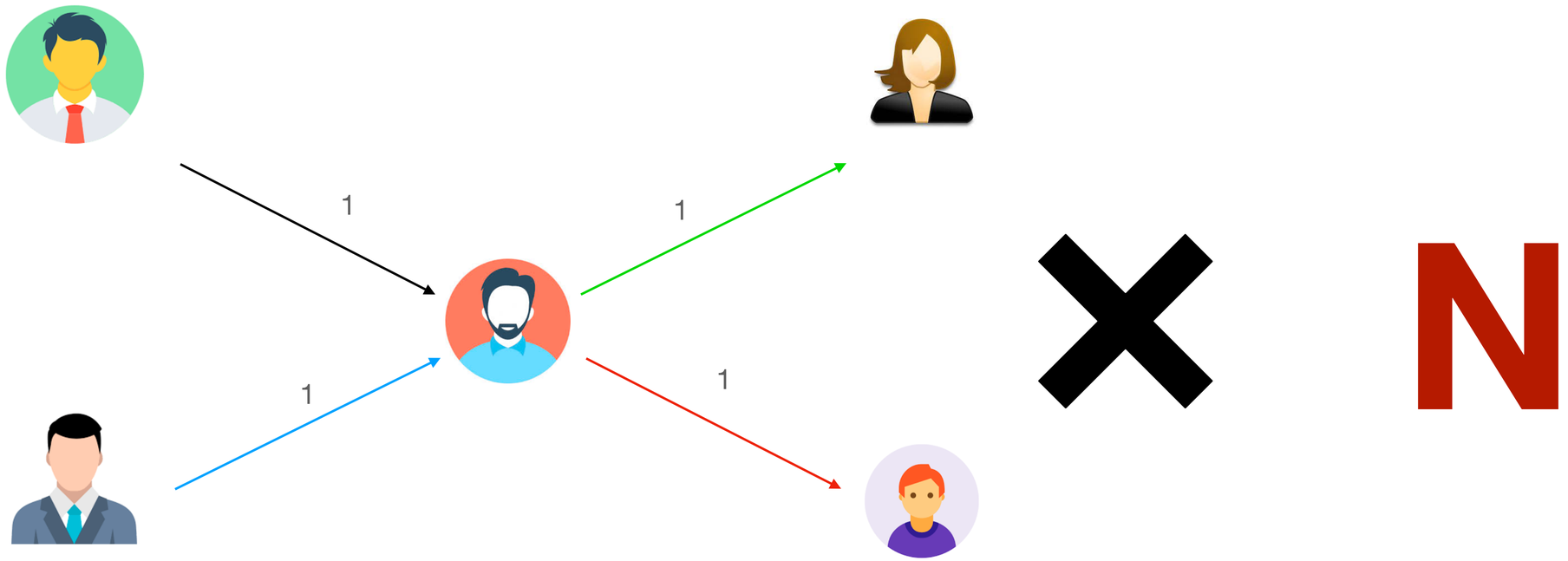
Payment Channel Hub

- Relationship Anonymity: the hub should not learn who is paying to whom



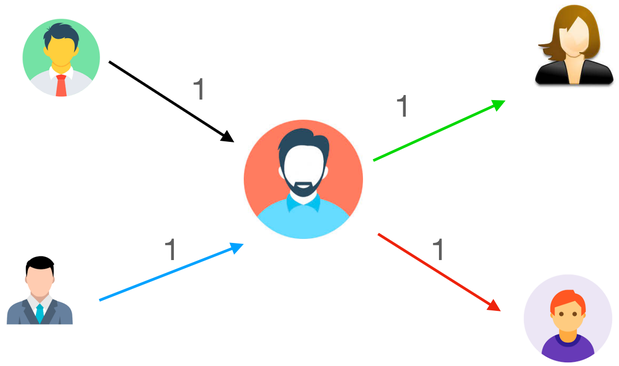
Payment Channel Hub

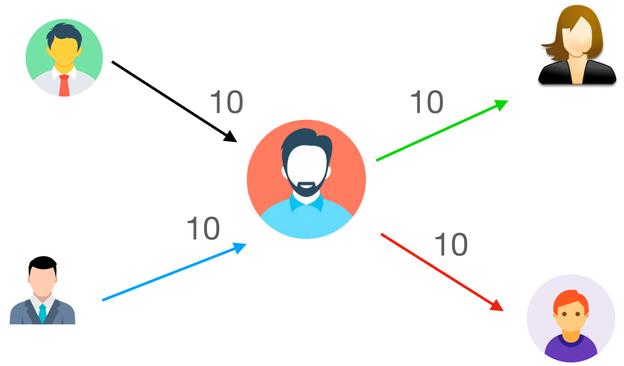
- Relationship Anonymity: the hub should not learn who is paying to whom

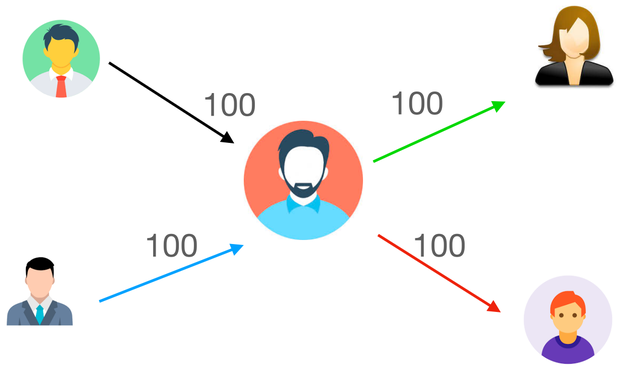


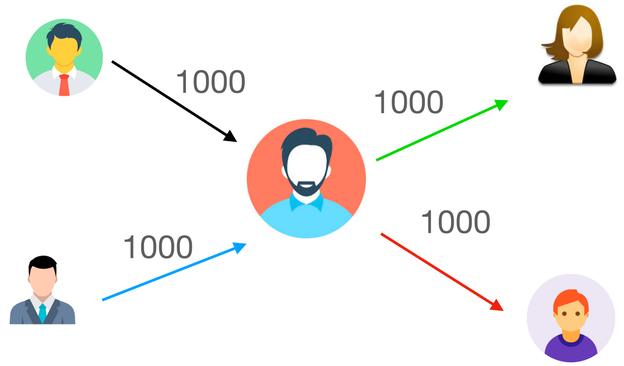
Payment Channel Hub

- Relationship Anonymity: the hub should not learn who is paying to whom



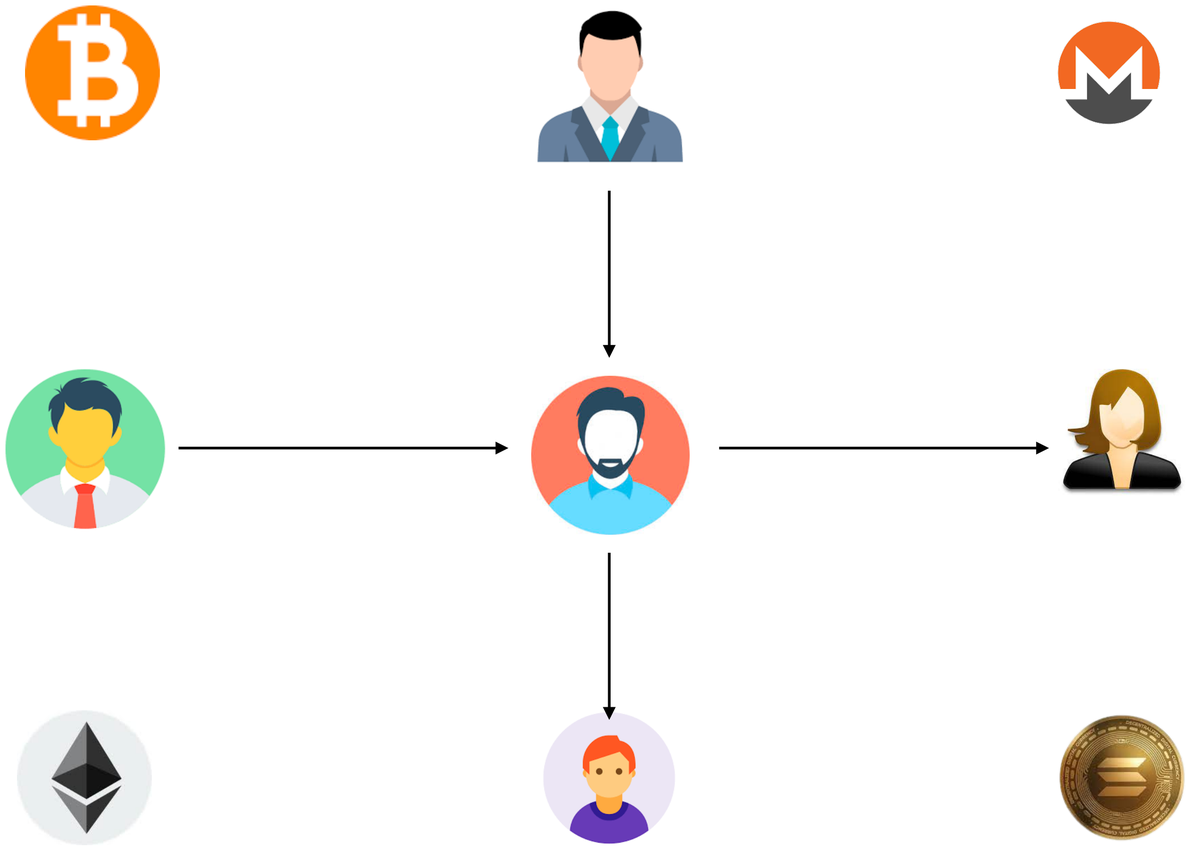






Payment Channel Hub

- Interoperability: The PCH should support as many cryptocurrencies as possible.



State-of-the-art and Comparison

	Bitcoin Compatible	Relationship Anonymous	Atomic	Flexible (Variable Amount)
A2L [TMM 21, S&P] TumbleBit [HABSG 17, NDSS]				
BOLT [GM 17, CCS]				
This Work				

State-of-the-art and Comparison

	Bitcoin Compatible	Relationship Anonymous	Atomic	Flexible (Variable Amount)
A2L [TMM 21, S&P] TumbleBit [HABSG 17, NDSS]				
BOLT [GM 17, CCS]				
This Work				

State-of-the-art and Comparison

	Bitcoin Compatible	Relationship Anonymous	Atomic	Flexible (Variable Amount)
A2L [TMM 21, S&P] TumbleBit [HABSG 17, NDSS]	✓	✓		
BOLT [GM 17, CCS]				
This Work				

State-of-the-art and Comparison

	Bitcoin Compatible	Relationship Anonymous	Atomic	Flexible (Variable Amount)
A2L [TMM 21, S&P] TumbleBit [HABSG 17, NDSS]	✓	✓	✓	
BOLT [GM 17, CCS]				
This Work				

State-of-the-art and Comparison

	Bitcoin Compatible	Relationship Anonymous	Atomic	Flexible (Variable Amount)
A2L [TMM 21, S&P] TumbleBit [HABSG 17, NDSS]	✓	✓	✓	✗
BOLT [GM 17, CCS]				
This Work				

State-of-the-art and Comparison

	Bitcoin Compatible	Relationship Anonymous	Atomic	Flexible (Variable Amount)
A2L [TMM 21, S&P] TumbleBit [HABSG 17, NDSS]				
BOLT [GM 17, CCS]				
This Work				

State-of-the-art and Comparison

	Bitcoin Compatible	Relationship Anonymous	Atomic	Flexible (Variable Amount)
A2L [TMM 21, S&P] TumbleBit [HABSG 17, NDSS]	✓	✓	✓	✗
BOLT [GM 17, CCS]			✓	✓
This Work				

State-of-the-art and Comparison

	Bitcoin Compatible	Relationship Anonymous	Atomic	Flexible (Variable Amount)
A2L [TMM 21, S&P] TumbleBit [HABSG 17, NDSS]	✓	✓	✓	✗
BOLT [GM 17, CCS]		✓	✓	✓
This Work				

State-of-the-art and Comparison

	Bitcoin Compatible	Relationship Anonymous	Atomic	Flexible (Variable Amount)
A2L [TMM 21, S&P] TumbleBit [HABSG 17, NDSS]	✓	✓	✓	✗
BOLT [GM 17, CCS]	✗	✓	✓	✓
This Work				

State-of-the-art and Comparison

	Bitcoin Compatible	Relationship Anonymous	Atomic	Flexible (Variable Amount)
A2L [TMM 21, S&P] TumbleBit [HABSG 17, NDSS]	✓	✓	✓	✗
BOLT [GM 17, CCS]	✗	✓	✓	✓
This Work	✓	✓	✓	✓

Our Solution

BlindChannel—Hiding the amount

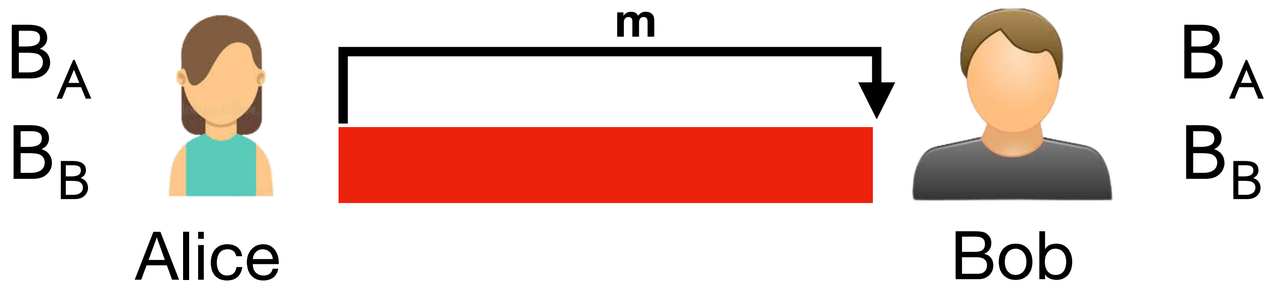
BlindChannel

BlindChannel

Recall normal payment channel…

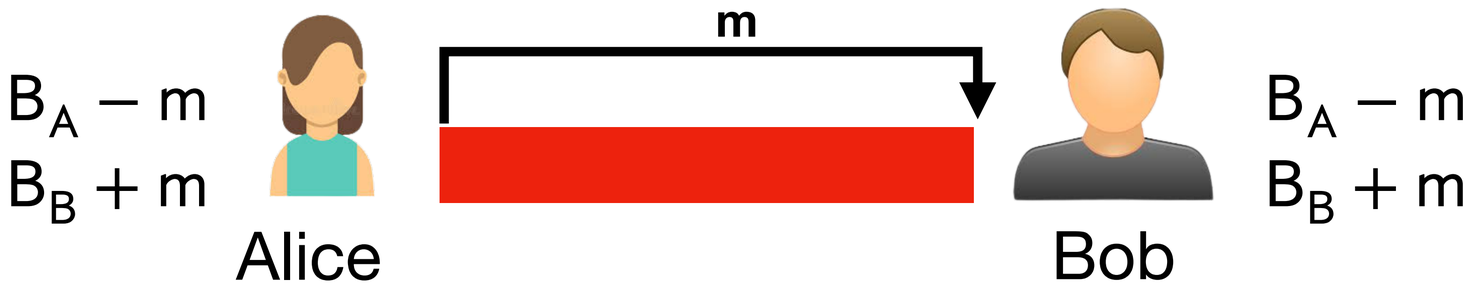
BlindChannel

Recall normal payment channel…



BlindChannel

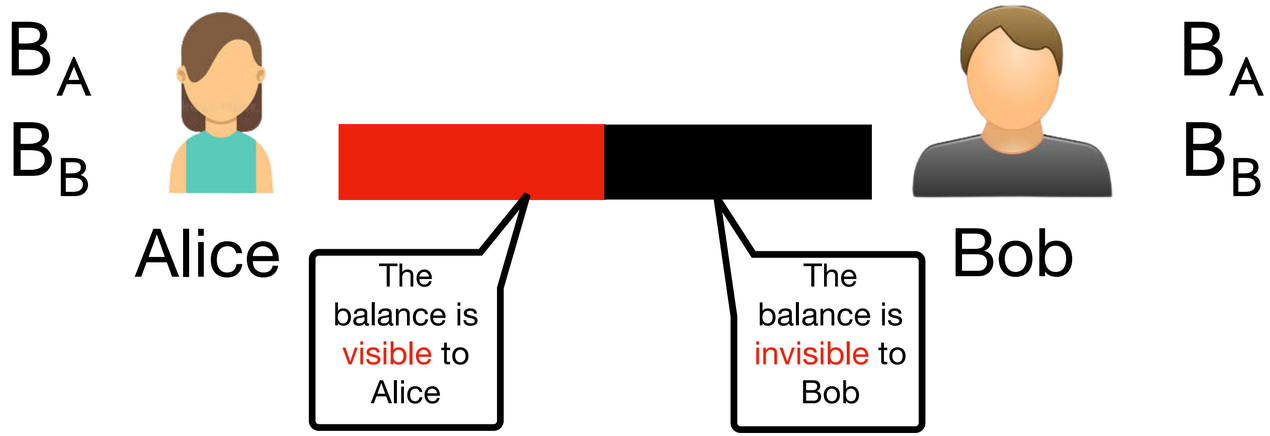
Recall normal payment channel…



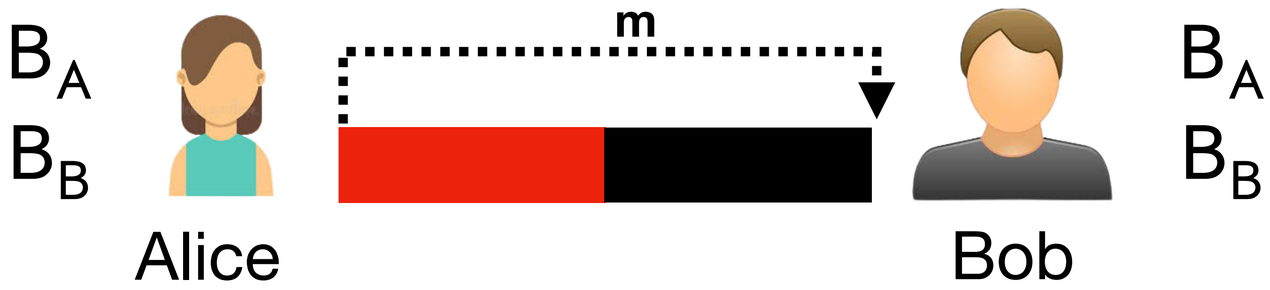
BlindChannel

BlindChannel

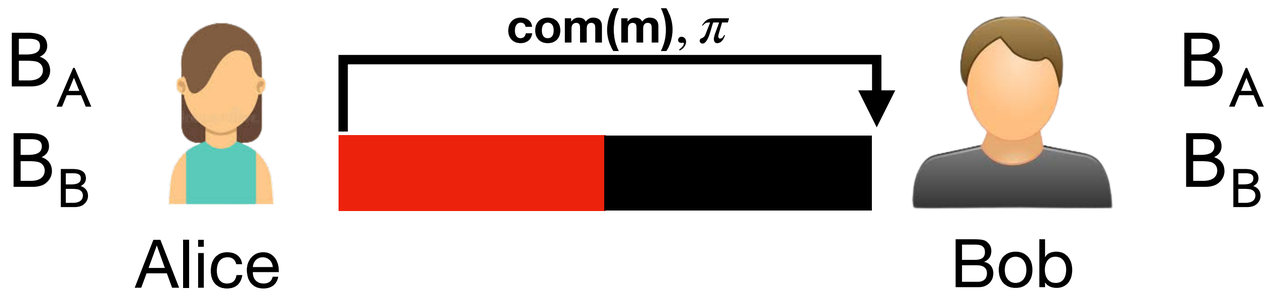
BlindChannel



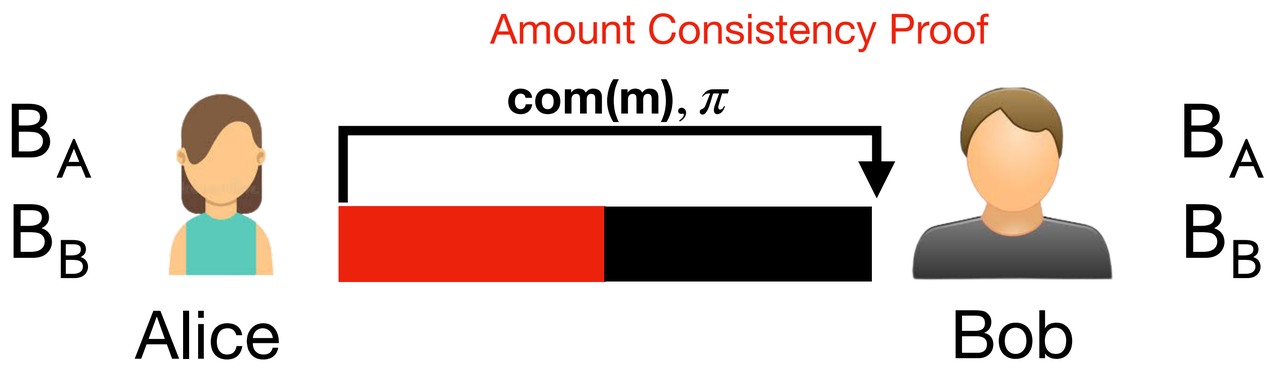
BlindChannel



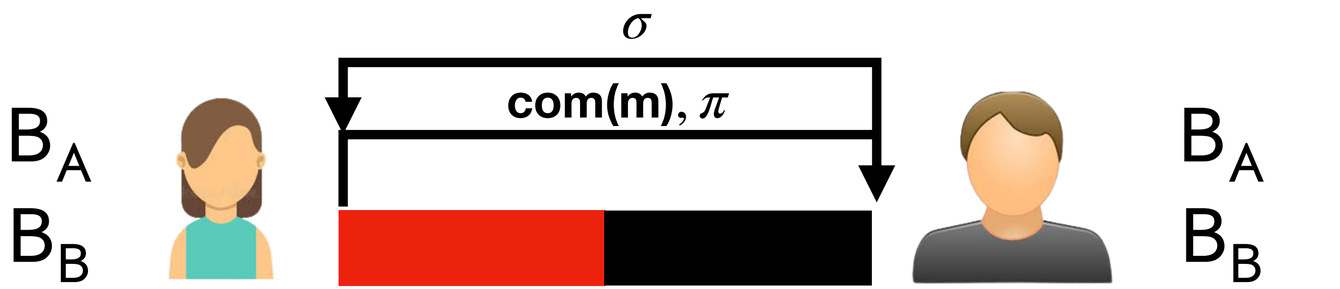
BlindChannel



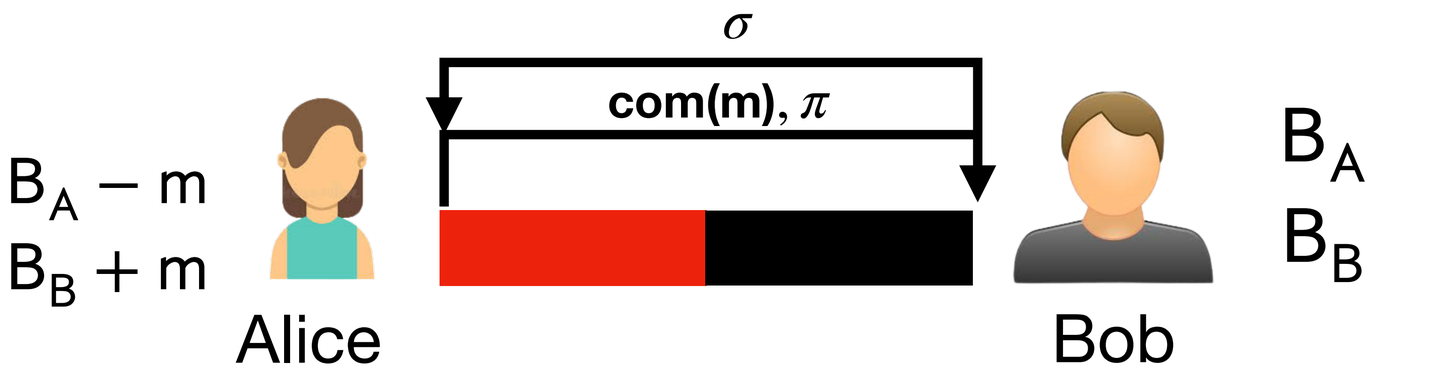
BlindChannel



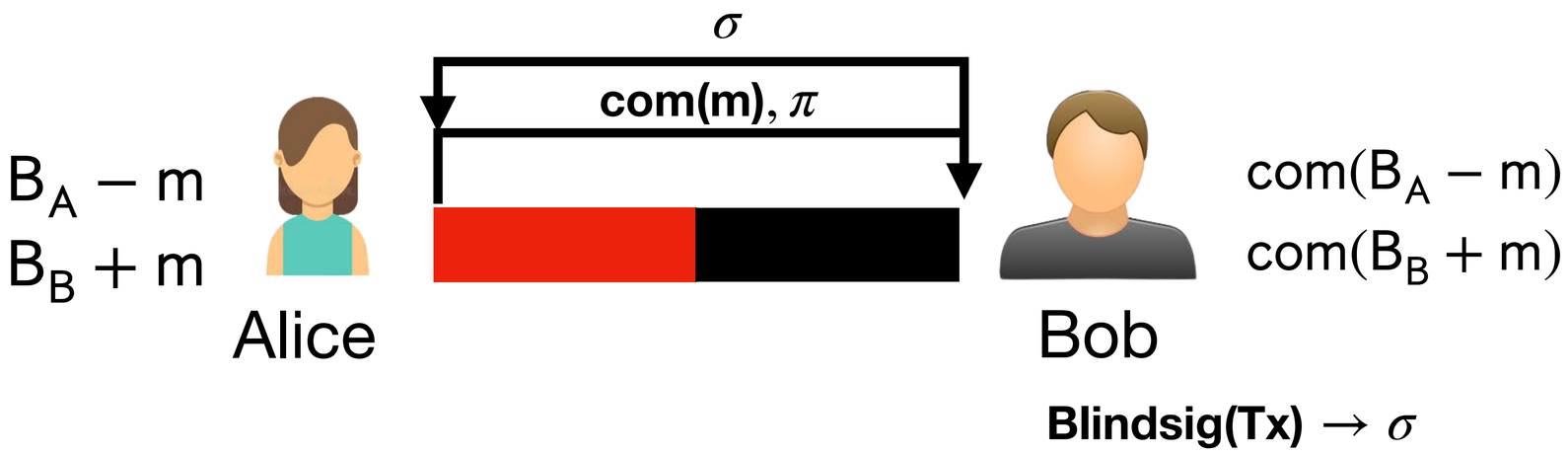
BlindChannel



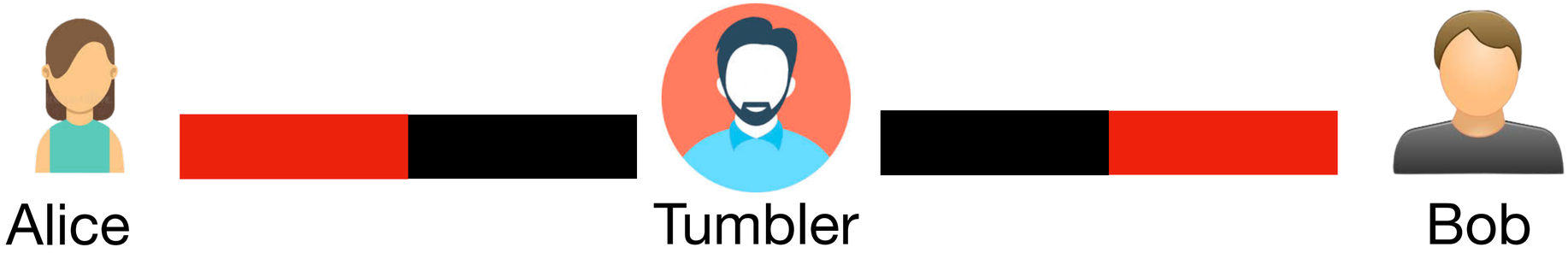
BlindChannel



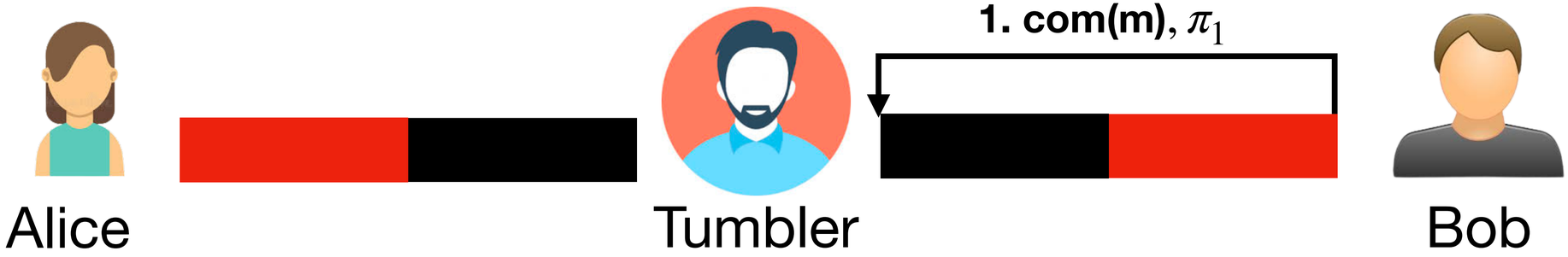
BlindChannel



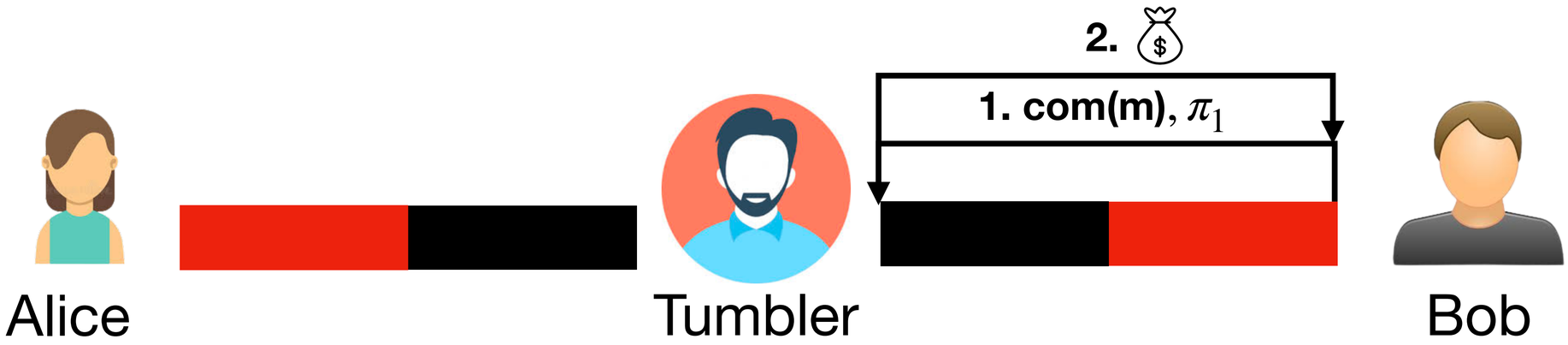
PCH with BlindChannel (Naive version)



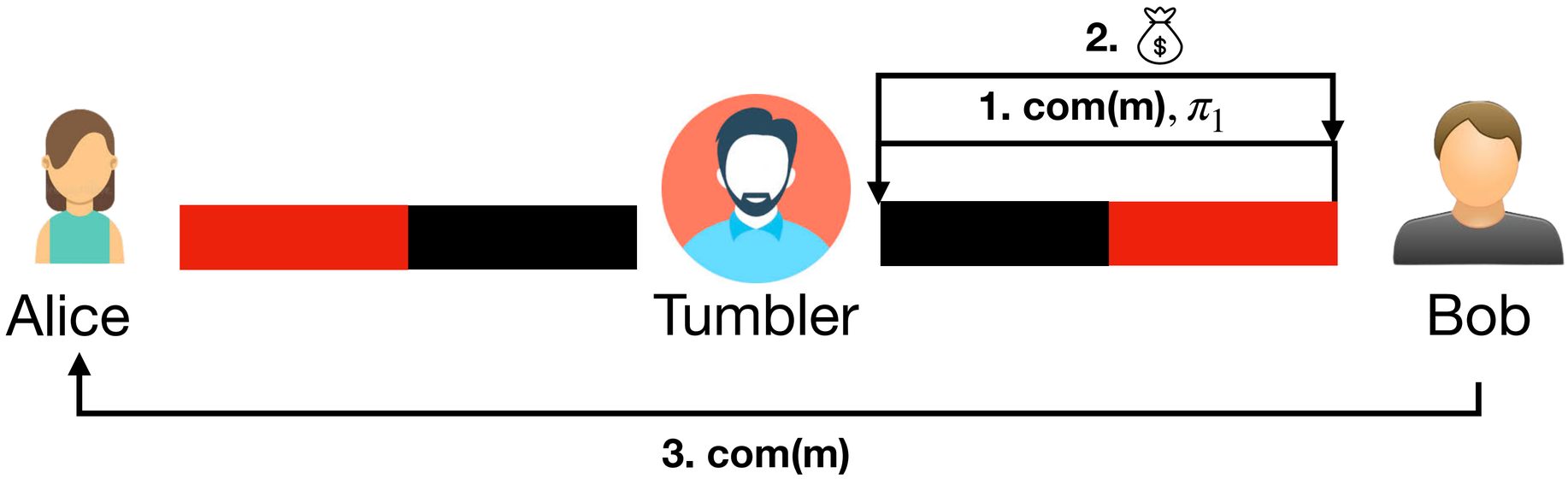
PCH with BlindChannel (Naive version)



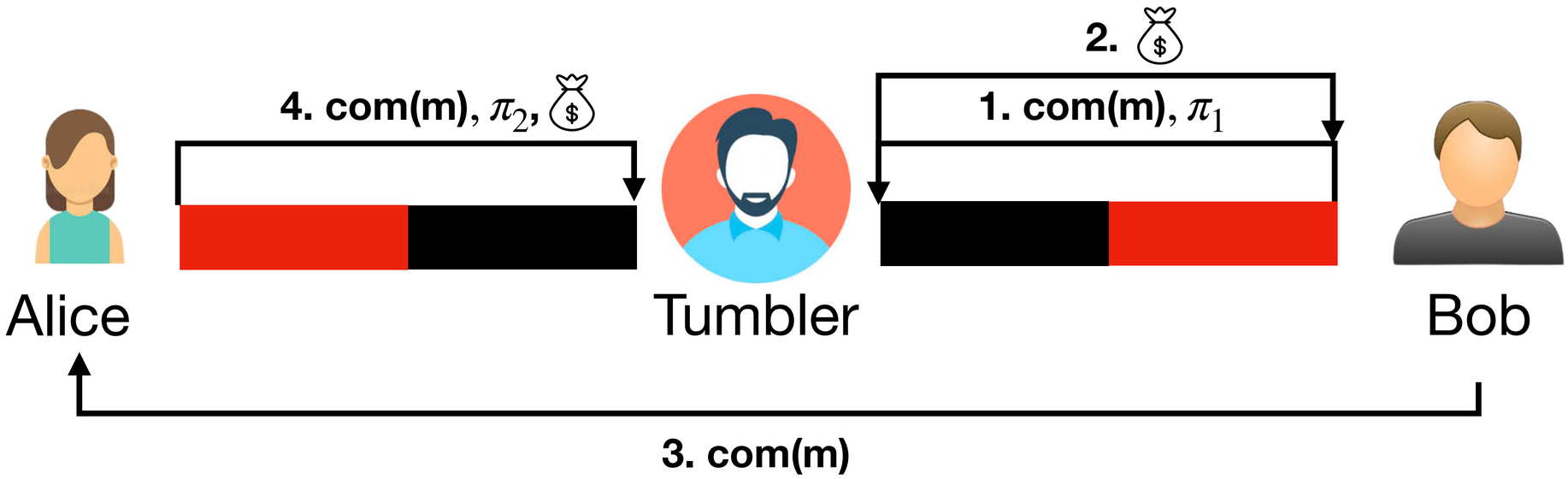
PCH with BlindChannel (Naive version)



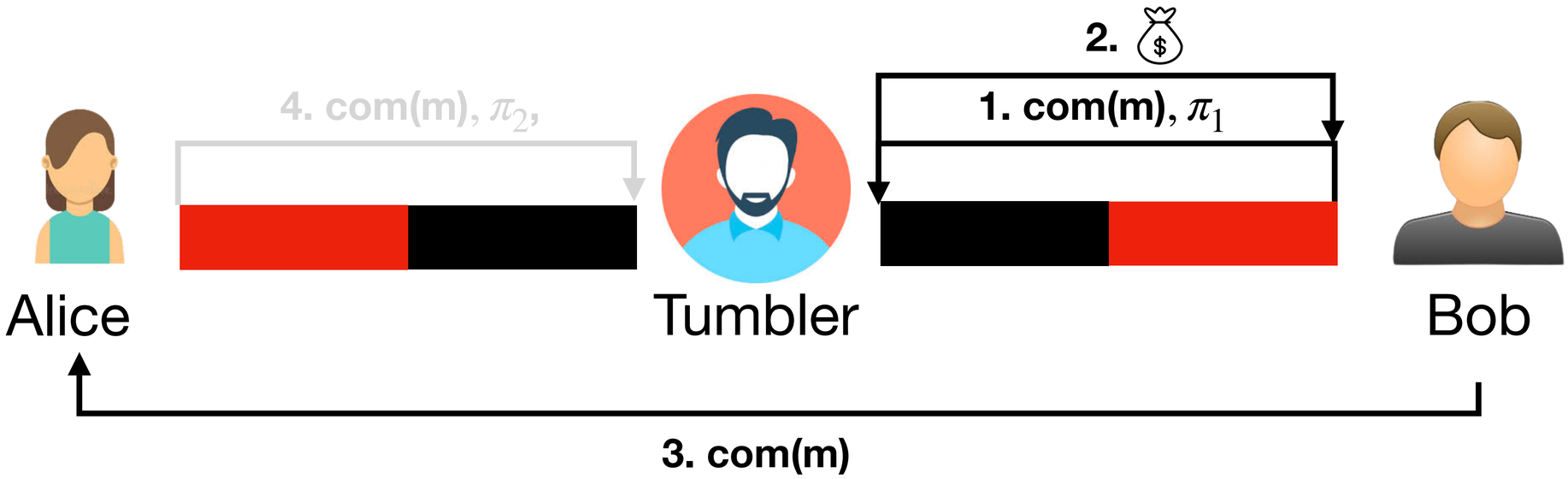
PCH with BlindChannel (Naive version)



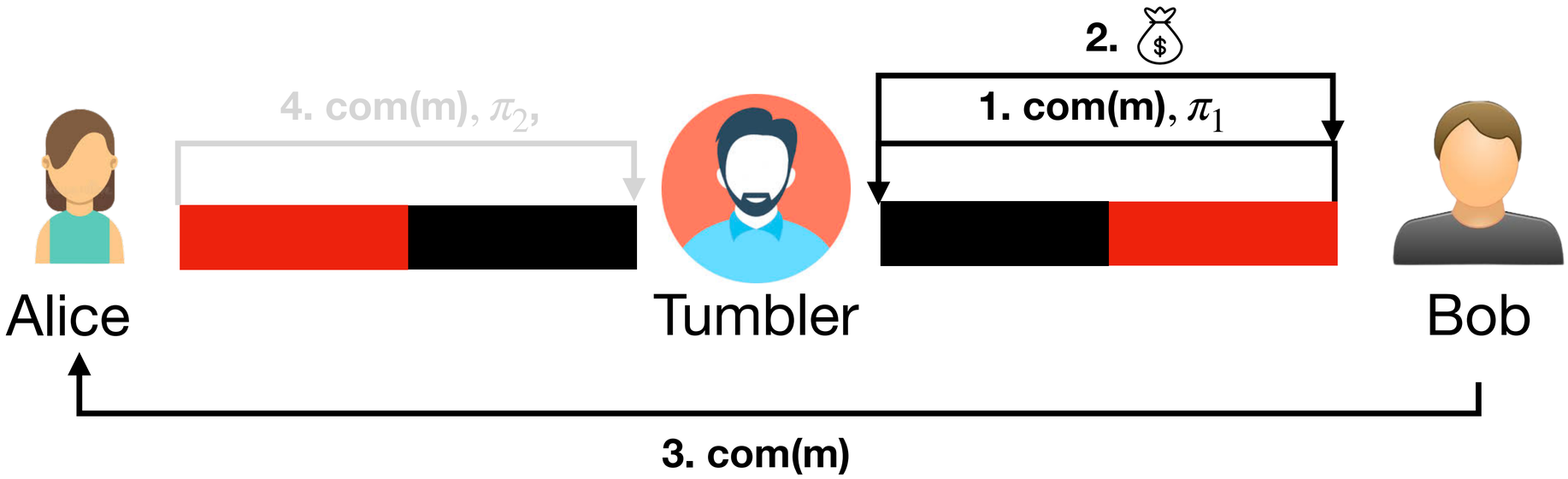
PCH with BlindChannel (Naive version)



PCH with BlindChannel (Naive version)



PCH with BlindChannel (Naive version)



No Atomicity!

Prelim: Adaptor Signature [AEEFHMMR’ 20]

Relation

$(Y, y) \in R$

(sk, pk)

Prelim: Adaptor Signature [AEEFHMMR’ 20]

Relation

$(Y, y) \in R$

(sk, pk)

Y, m

Prelim: Adaptor Signature [AEEFHMMR' 20]

Relation

$(Y, y) \in R$

(sk, pk)

Y, m

PreSig$(m, \mathsf{sk}, Y) \to \hat{\sigma}$

Incomplete Signature

Prelim: Adaptor Signature [AEEFHMMR' 20]

Relation

$(Y, y) \in R$

(sk, pk)

Y, m

PreSig$(m, \mathsf{sk}, Y) \to \hat{\sigma}$

$\hat{\sigma}$

Incomplete Signature

Prelim: Adaptor Signature [AEEFHMMR' 20]

Relation

$(Y, y) \in R$

(sk, pk)

Y, m

$\text{PreSig}(m, \text{sk}, Y) \to \hat{\sigma}$

$\hat{\sigma}$

$\text{PreVfy}(m, \text{pk}, Y, \hat{\sigma}) \to 0/1$

$\text{Adapt}(\hat{\sigma}, y) \to \sigma$

Incomplete Signature

Complete Signature

Prelim: Adaptor Signature [AEEFHMMR' 20]

Relation

$(Y, y) \in R$

(sk, pk)

Y, m

$\mathsf{PreSig}(m, \mathsf{sk}, Y) \to \hat{\sigma}$

Incomplete Signature

$\hat{\sigma}$

$\mathsf{PreVfy}(m, \mathsf{pk}, Y, \hat{\sigma}) \to 0/1$

$\mathsf{Adapt}(\hat{\sigma}, y) \to \sigma$

Complete Signature

m, σ

Prelim: Adaptor Signature [AEEFHMMR' 20]

Relation

$(Y, y) \in R$

(sk, pk)

Y, m

$\text{PreSig}(m, \text{sk}, Y) \to \hat{\sigma}$

Incomplete Signature

$\hat{\sigma}$

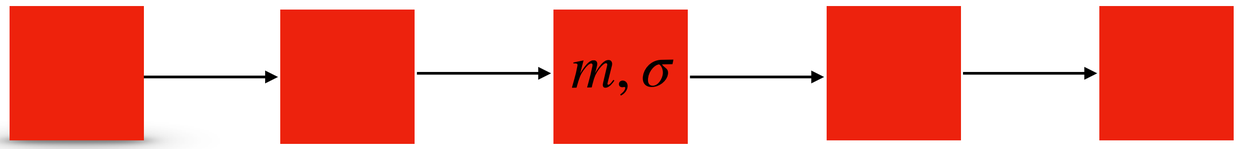
$\text{PreVfy}(m, \text{pk}, Y, \hat{\sigma}) \to 0/1$

$\text{Adapt}(\hat{\sigma}, y) \to \sigma$

Complete Signature

m, σ

σ



Prelim: Adaptor Signature [AEEFHMMR' 20]

Relation

$(Y, y) \in R$

(sk, pk)

Y, m

$\text{PreSig}(m, \text{sk}, Y) \to \hat{\sigma}$

$\hat{\sigma}$

$\text{PreVfy}(m, \text{pk}, Y, \hat{\sigma}) \to 0/1$

Incomplete Signature

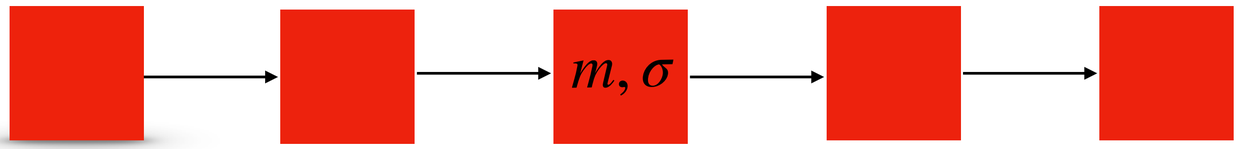
$\text{Adapt}(\hat{\sigma}, y) \to \sigma$

$\text{Extract}(\hat{\sigma}, \sigma) \to y$

m, σ

σ

Complete Signature



Prelim: Adaptor Signature [AEEFHMMR' 20]

Relation

$(Y, y) \in R$

(sk, pk)

Y, m

$\text{PreSig}(m, \text{sk}, Y) \to \hat{\sigma}$

$\hat{\sigma}$

$\text{PreVfy}(m, \text{pk}, Y, \hat{\sigma}) \to 0/1$

Incomplete Signature

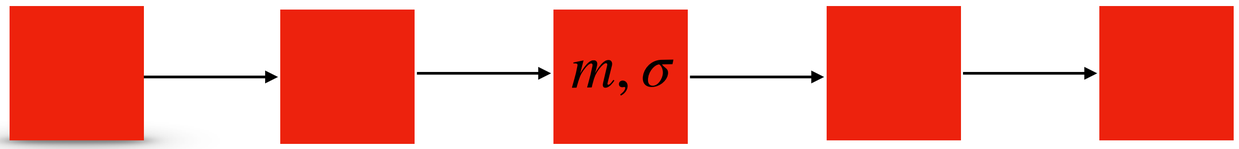
$\text{Adapt}(\hat{\sigma}, y) \to \sigma$

$\text{Extract}(\hat{\sigma}, \sigma) \to y$

m, σ

σ

Complete Signature



Blind Adaptor Signature

Relation

$(Y, y) \in R$

(sk, pk)

Y, m

$\text{PreSig}(m, \text{sk}, Y) \to \hat{\sigma}$

$\hat{\sigma}$

$\text{PreVfy}(m, \text{pk}, Y, \hat{\sigma}) \to 0/1$

Incomplete Signature

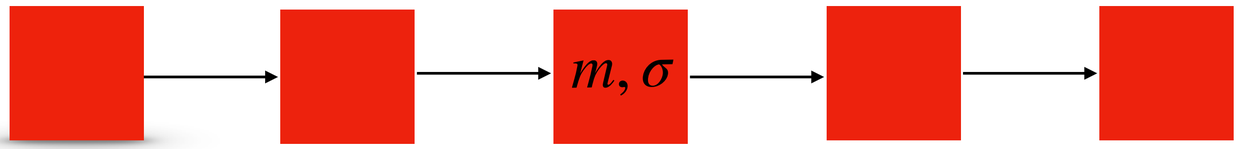
$\text{Adapt}(\hat{\sigma}, y) \to \sigma$

$\text{Adapt}(\hat{\sigma}, y) \to \sigma$

m, σ

σ

Complete Signature



Blind Adaptor Signature

Relation

$(Y, y) \in R$

(sk, pk)

$Y, \text{com}(m), \pi$

$\text{PreSig}(\text{com}(m), \text{sk}, Y) \rightarrow \hat{\sigma}$

$\hat{\sigma}$

$\text{PreVfy}(m, \text{pk}, Y, \hat{\sigma}) \rightarrow 0/1$

$\text{Adapt}(\hat{\sigma}, y) \rightarrow \sigma$

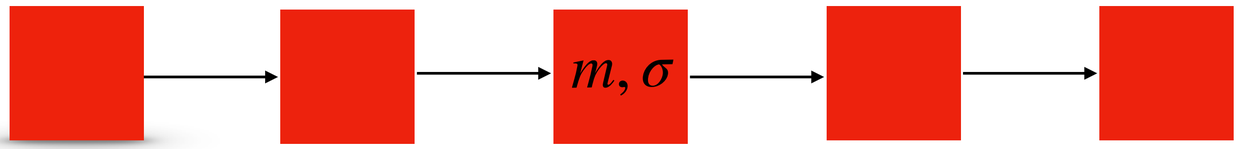
Incomplete Signature

Complete Signature

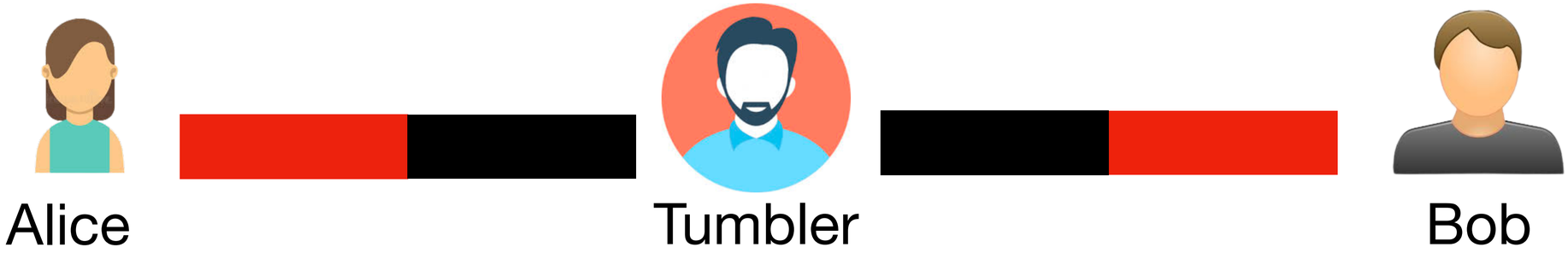
m, σ

σ

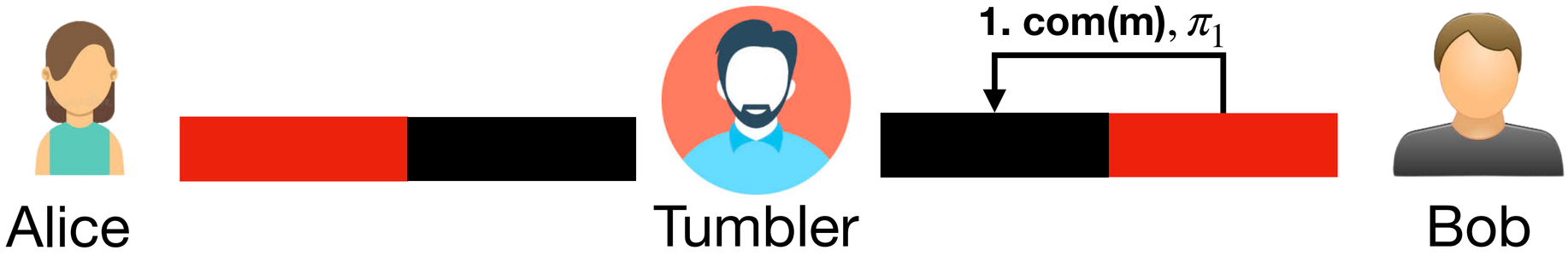
$\text{Adapt}(\hat{\sigma}, y) \rightarrow \sigma$



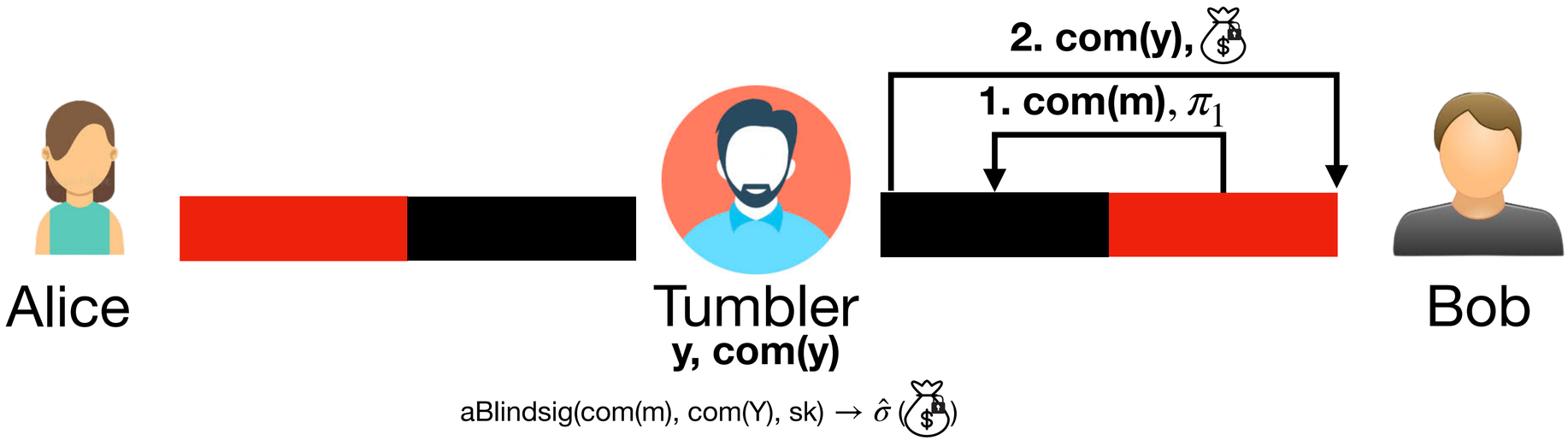
PCH with BlindChannel+Atomicity



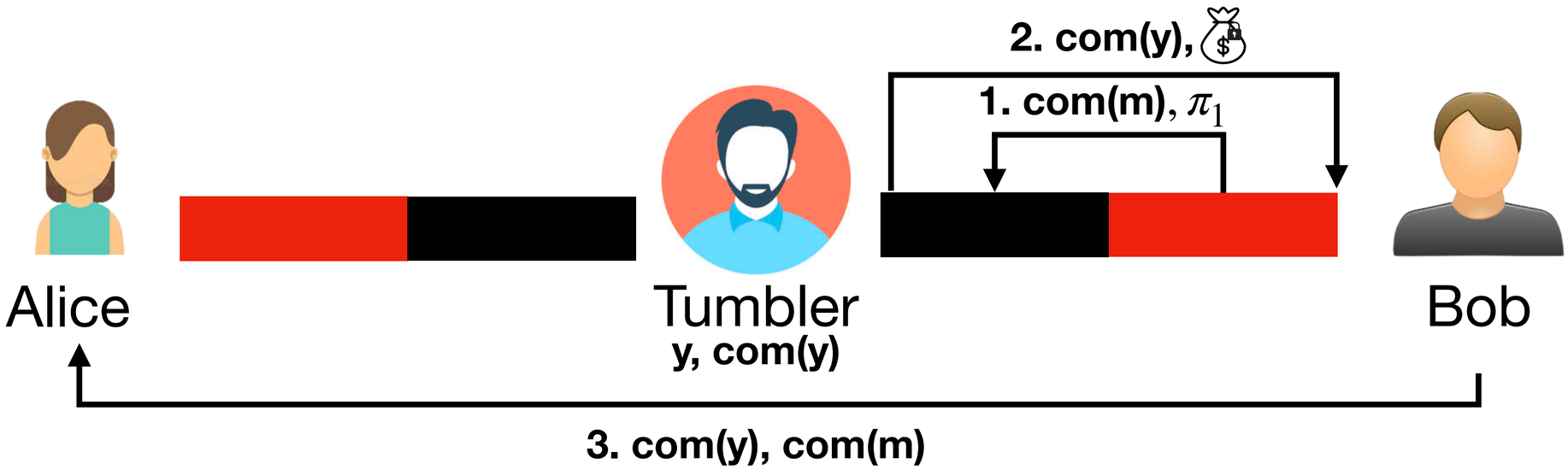
PCH with BlindChannel+Atomicity



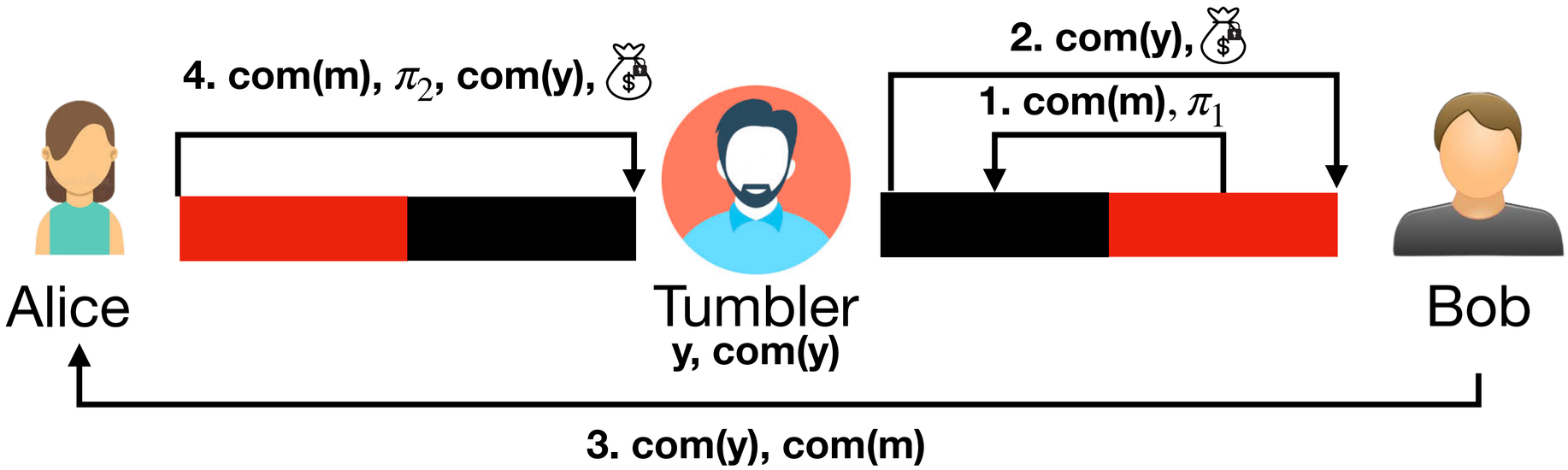
PCH with BlindChannel+Atomicity



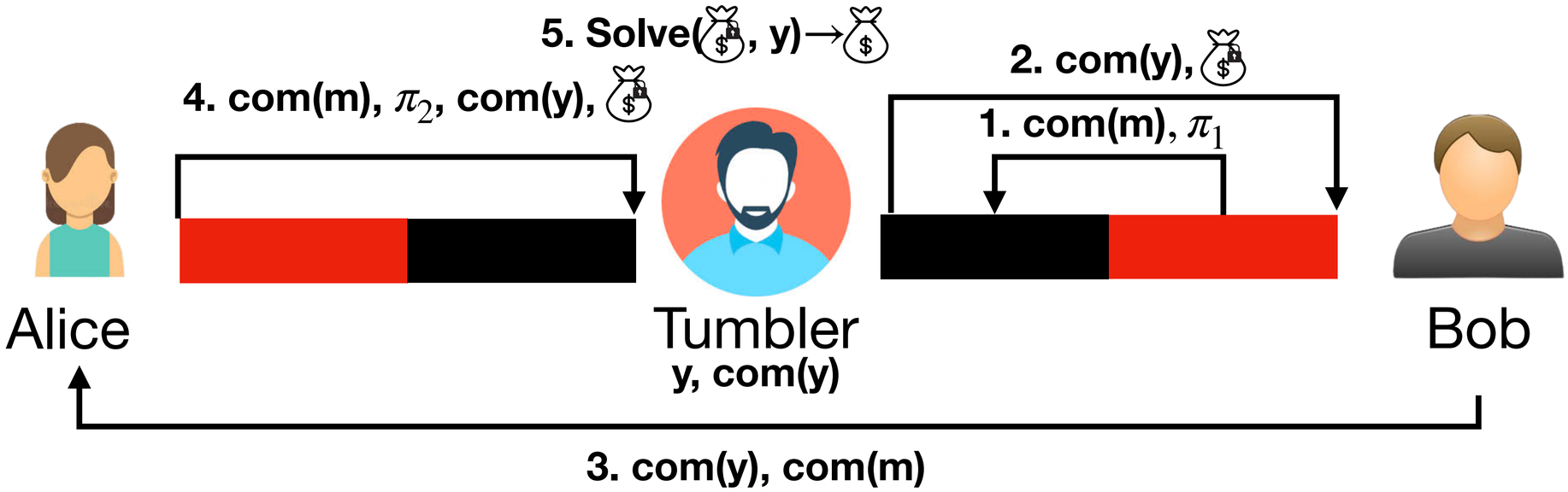
PCH with BlindChannel+Atomicity



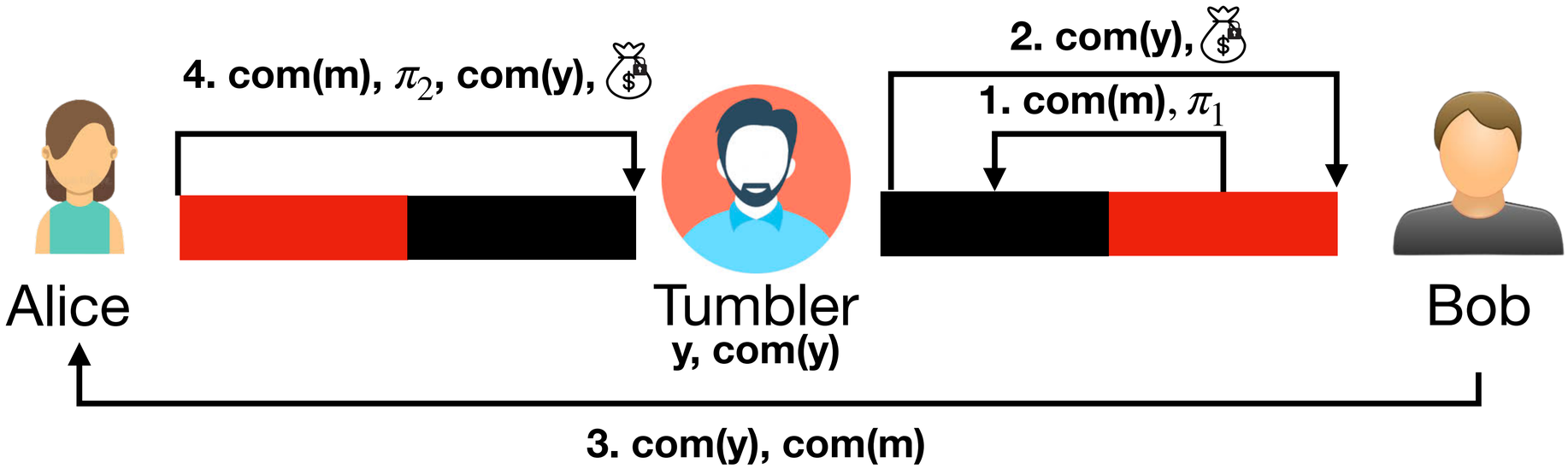
PCH with BlindChannel+Atomicity



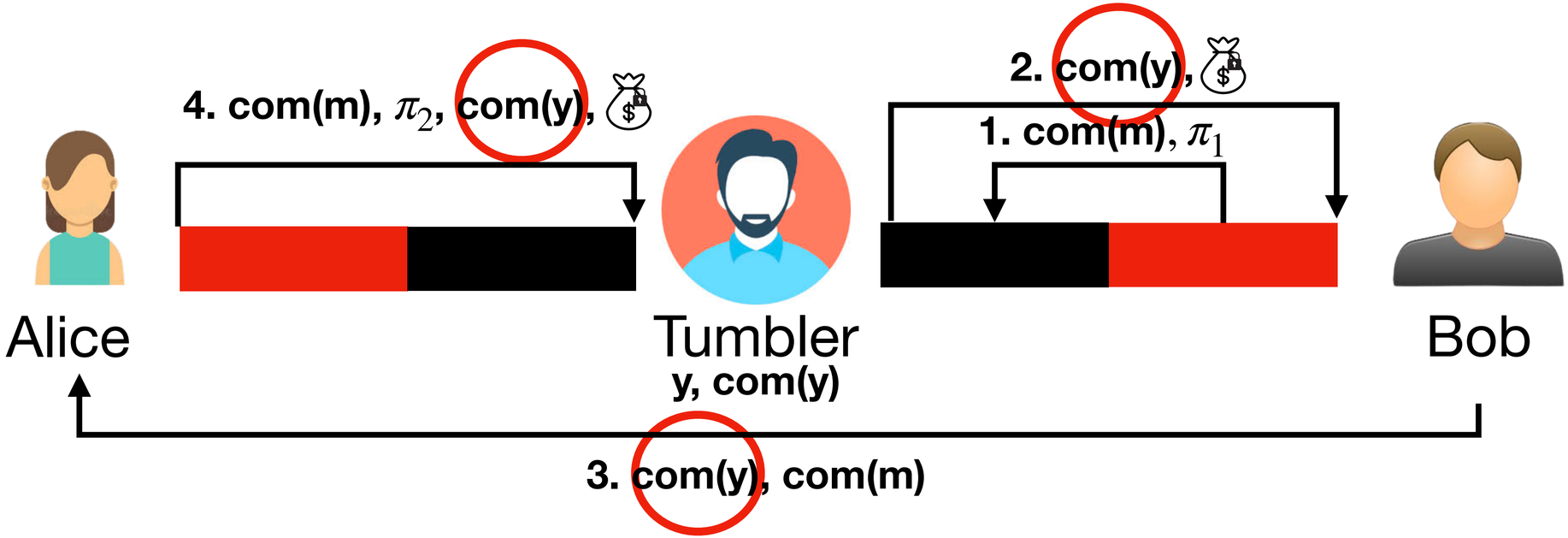
PCH with BlindChannel+Atomicity



PCH with BlindChannel+Atomicity+Privacy



PCH with BlindChannel+Atomicity+Privacy



Building blocks for Privacy

- Randomizable puzzle

Building blocks for Privacy

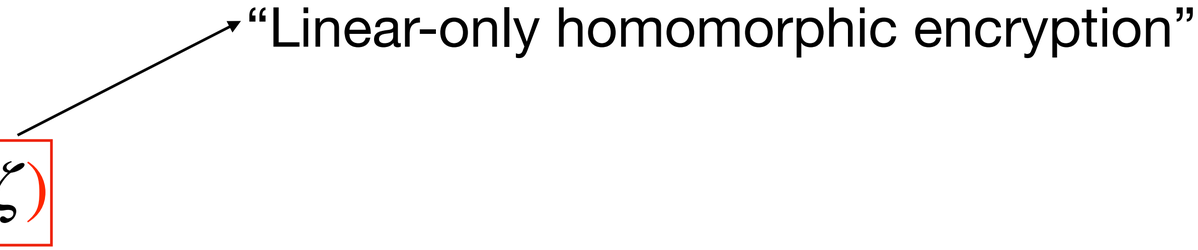
- Randomizable puzzle

$$com(\zeta), enc(\zeta) \rightarrow com(\zeta), enc(\zeta)$$

Building blocks for Privacy

- Randomizable puzzle

$$com(\zeta), enc(\zeta) \rightarrow com(\zeta), enc(\zeta)$$



Building blocks for Privacy

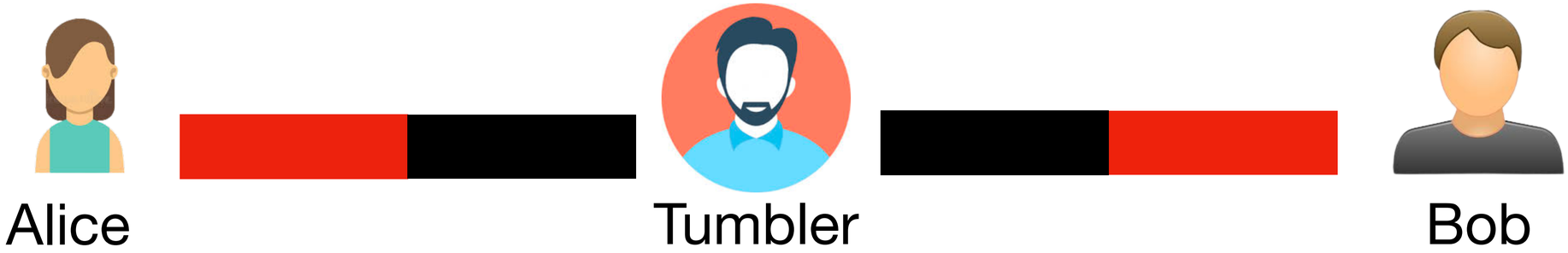
- Randomizable puzzle

$$com(\zeta), enc(\zeta) \rightarrow com(\zeta), enc(\zeta)$$

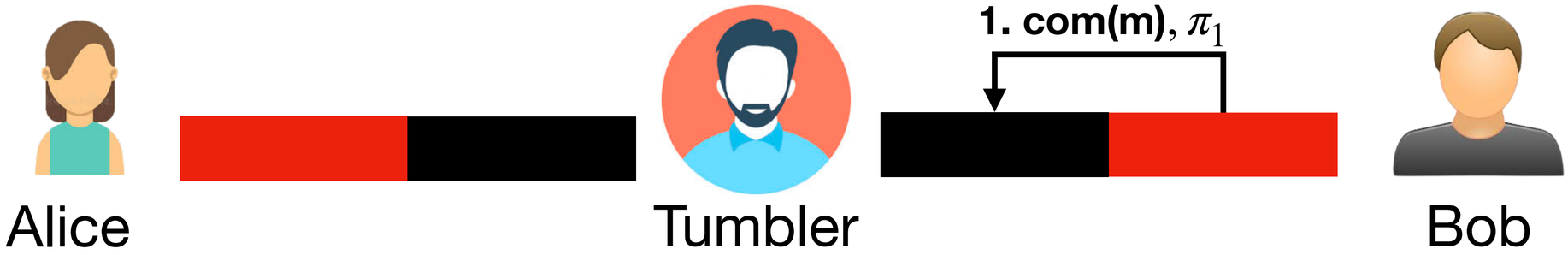
- Randomizable signature on randomizable commitment

$$(\sigma, com(\zeta), com(\zeta)) \rightarrow (\sigma, com(\zeta), com(\zeta))$$

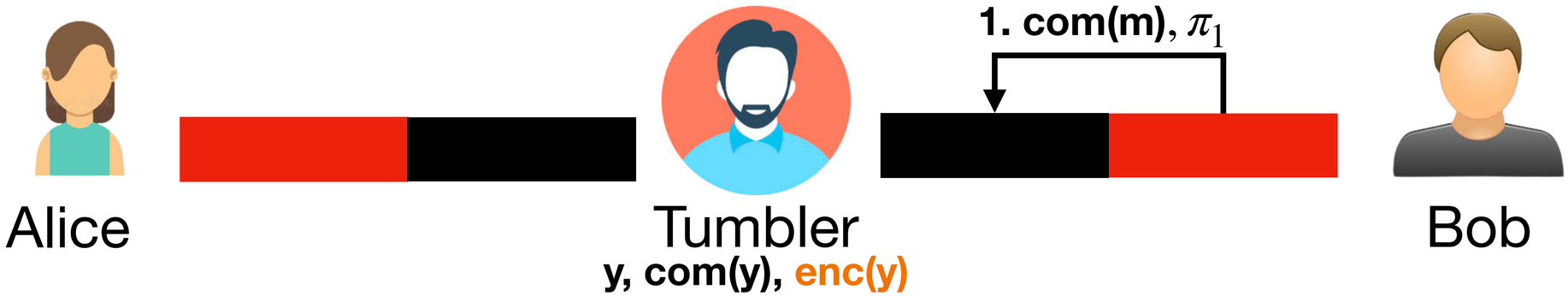
PCH with BlindChannel+Atomicity+Privacy



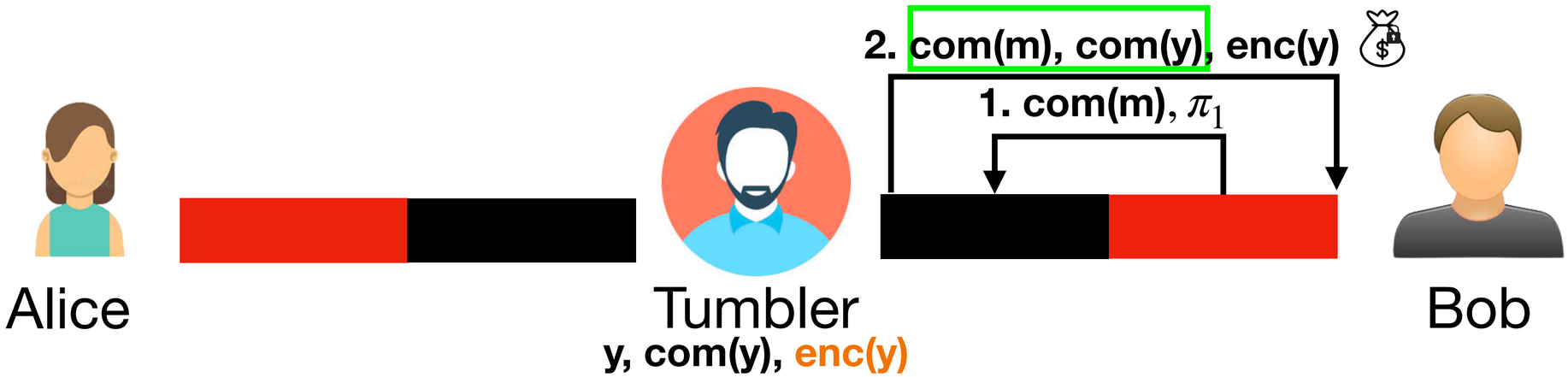
PCH with BlindChannel+Atomicity+Privacy



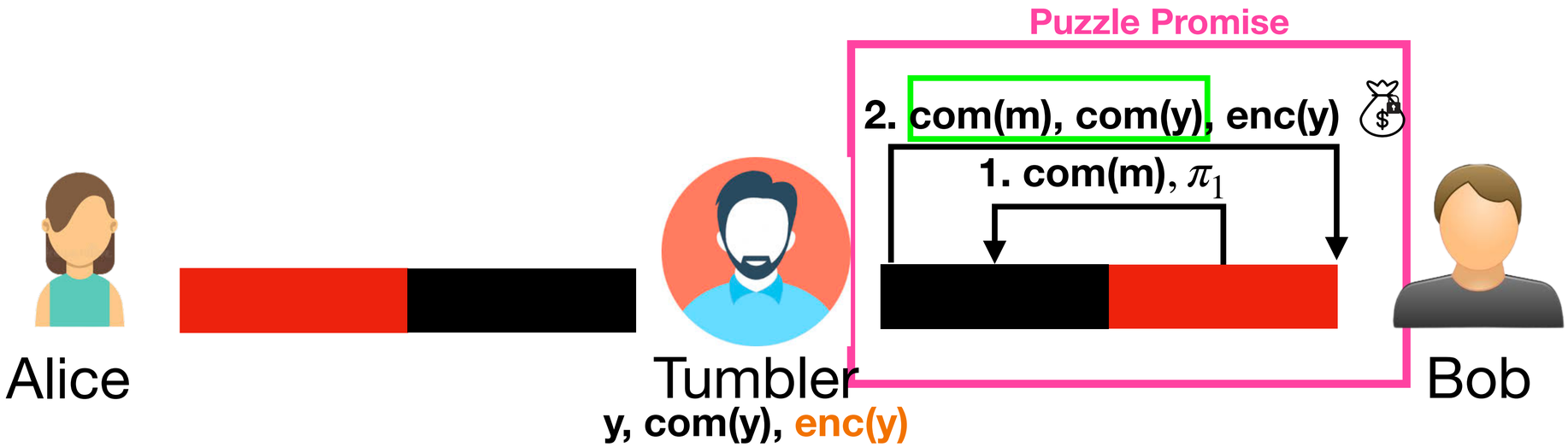
PCH with BlindChannel+Atomicity+Privacy



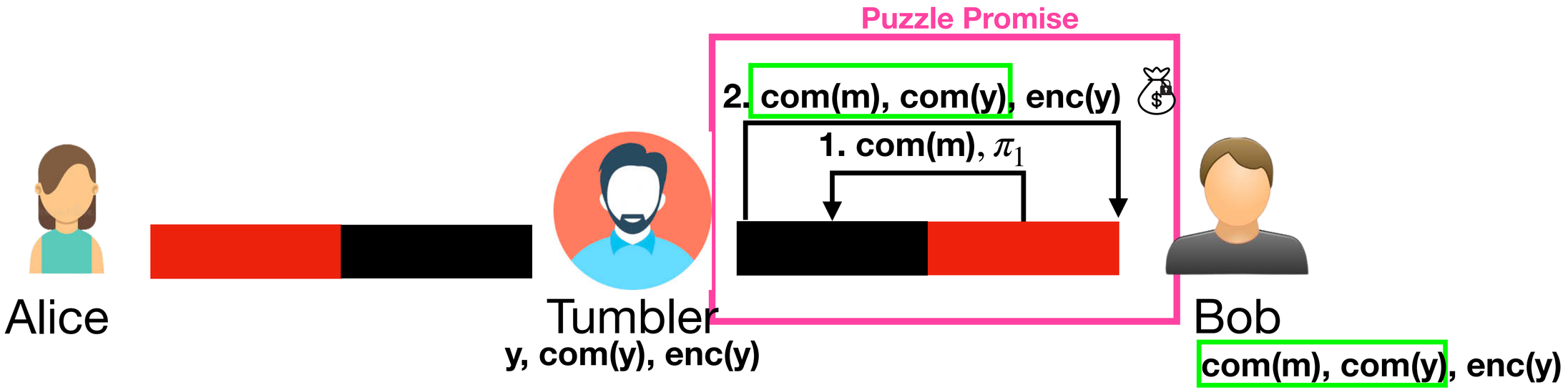
PCH with BlindChannel+Atomicity+Privacy



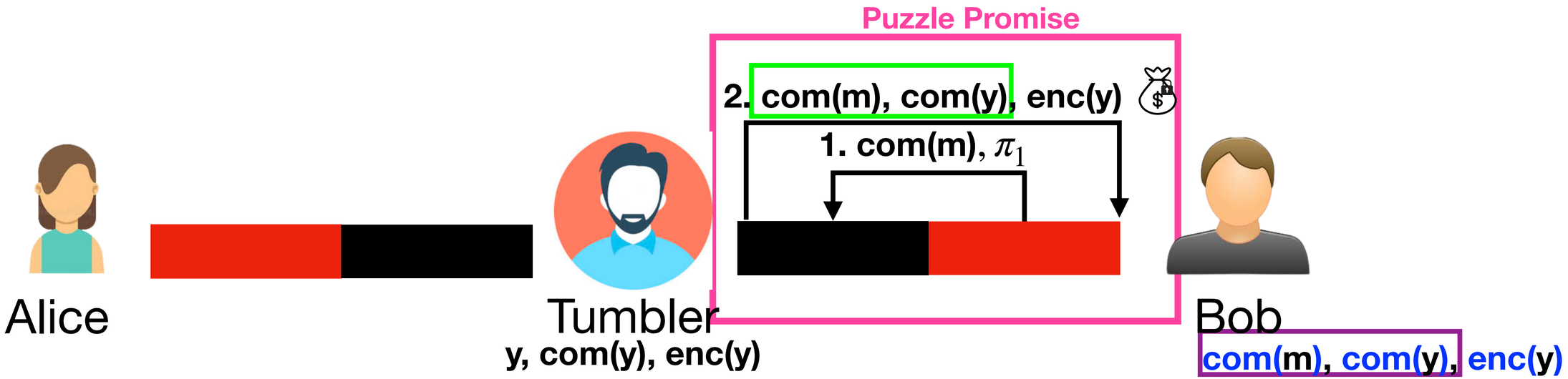
PCH with BlindChannel+Atomicity+Privacy



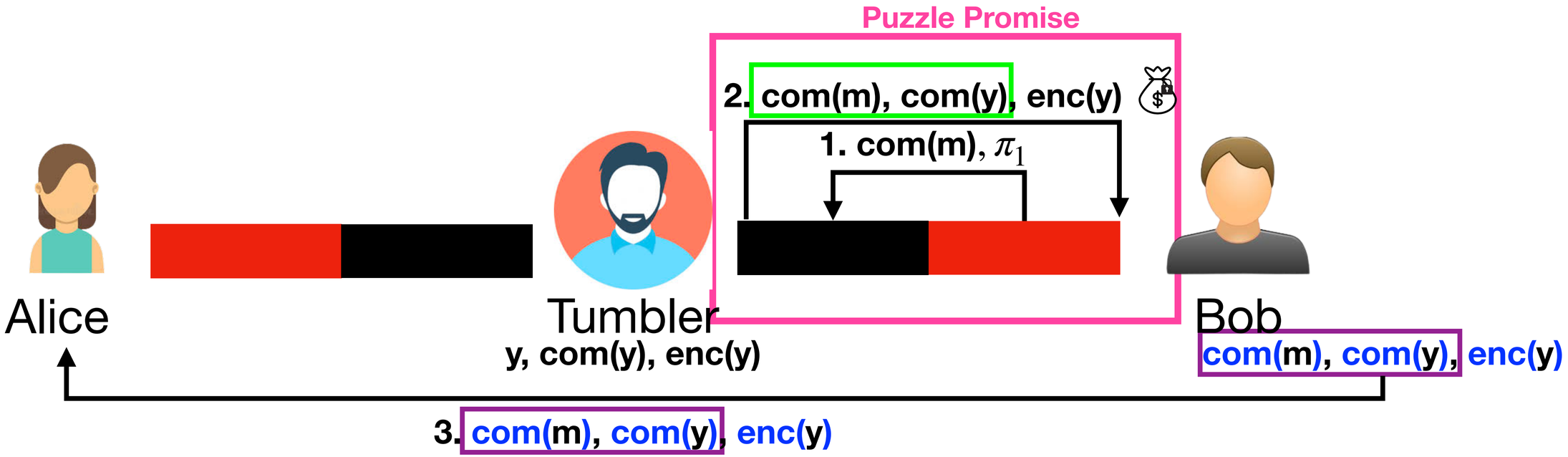
PCH with BlindChannel+Atomicity+Privacy



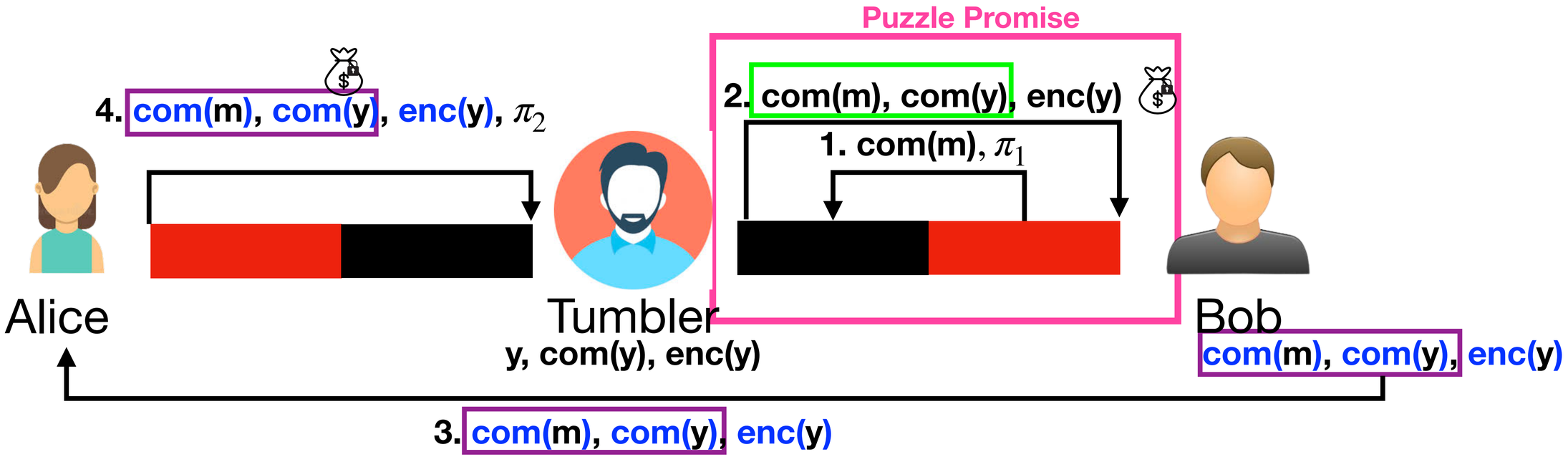
PCH with BlindChannel+Atomicity+Privacy



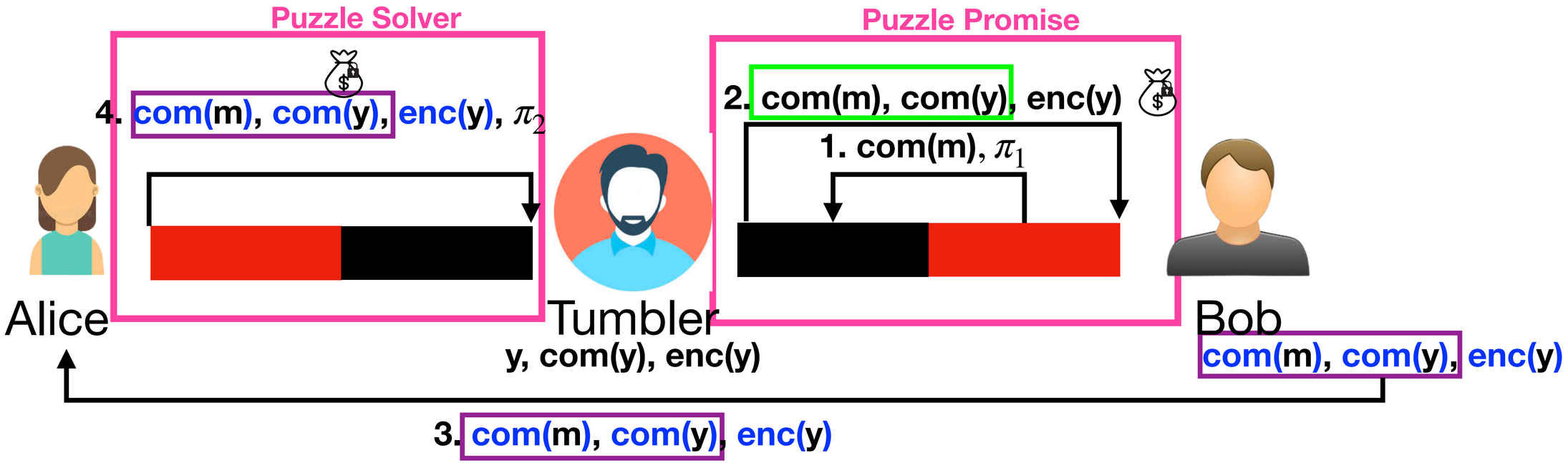
PCH with BlindChannel+Atomicity+Privacy



PCH with BlindChannel+Atomicity+Privacy

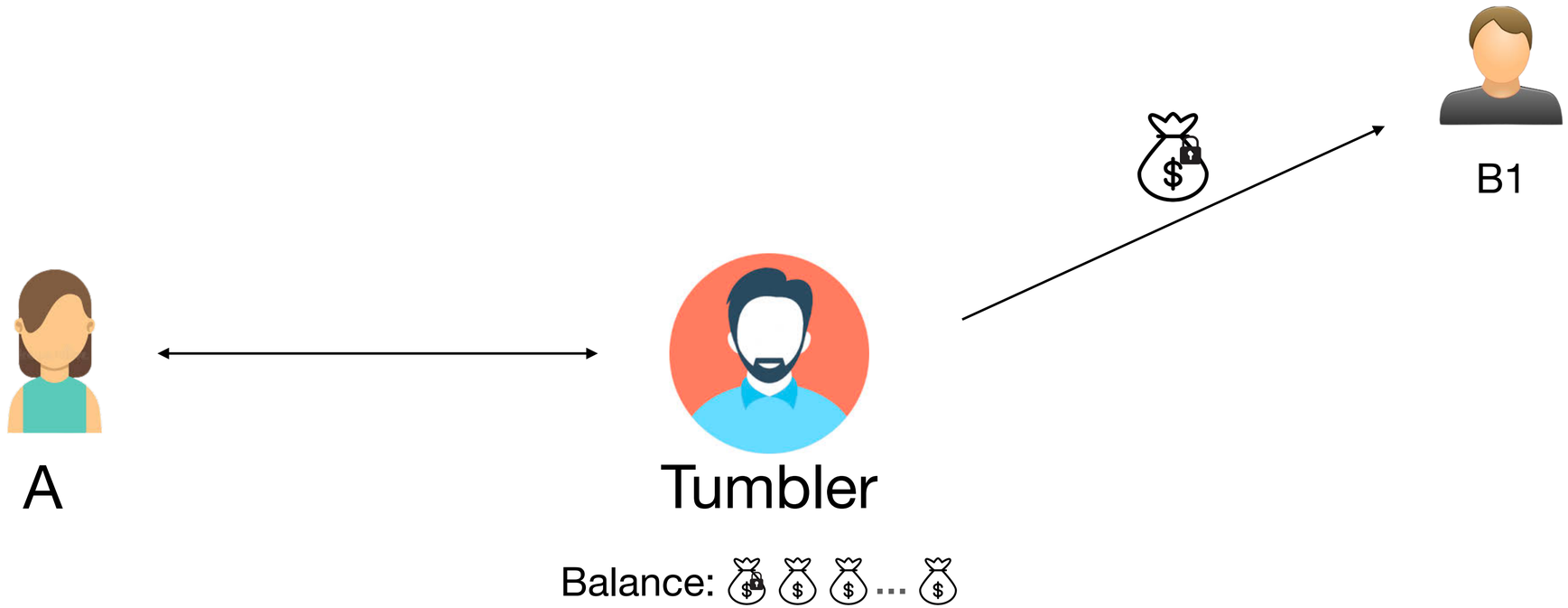


PCH with BlindChannel+Atomicity+Privacy



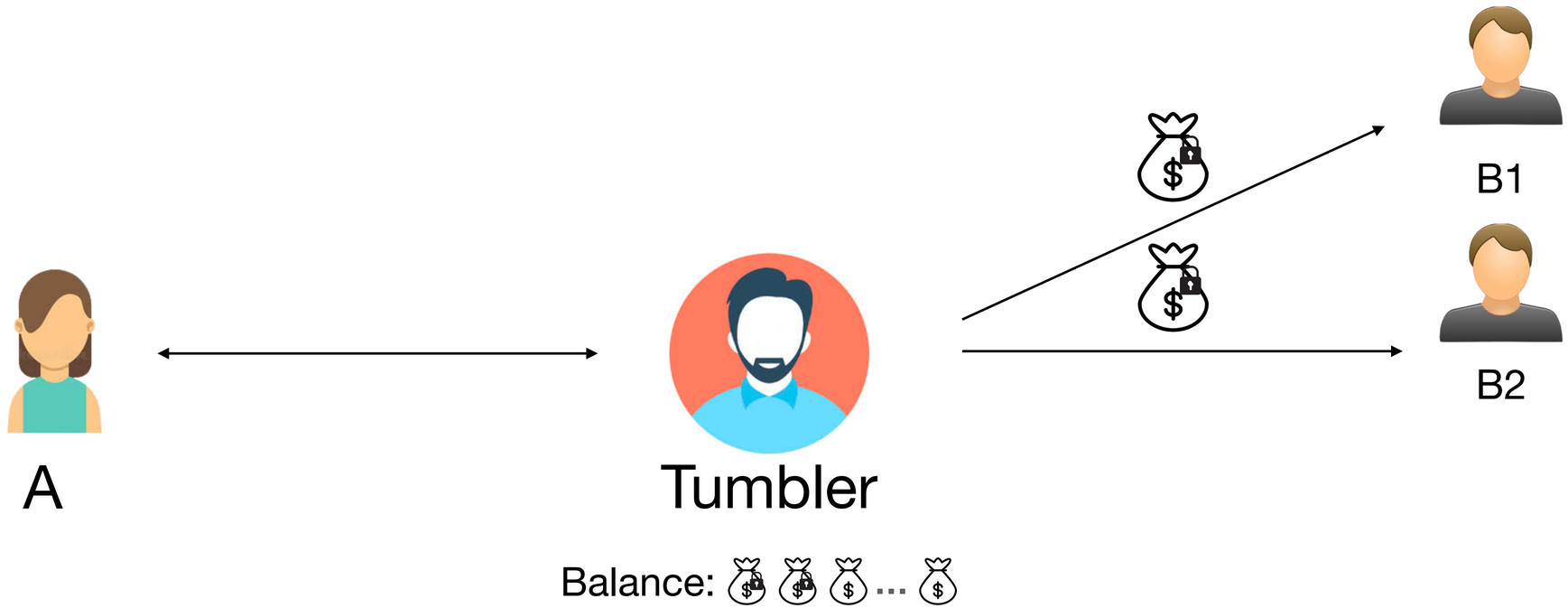
PCH with BlindChannel+Atomicity+Privacy+Griefing Resistance

Griefing Attack



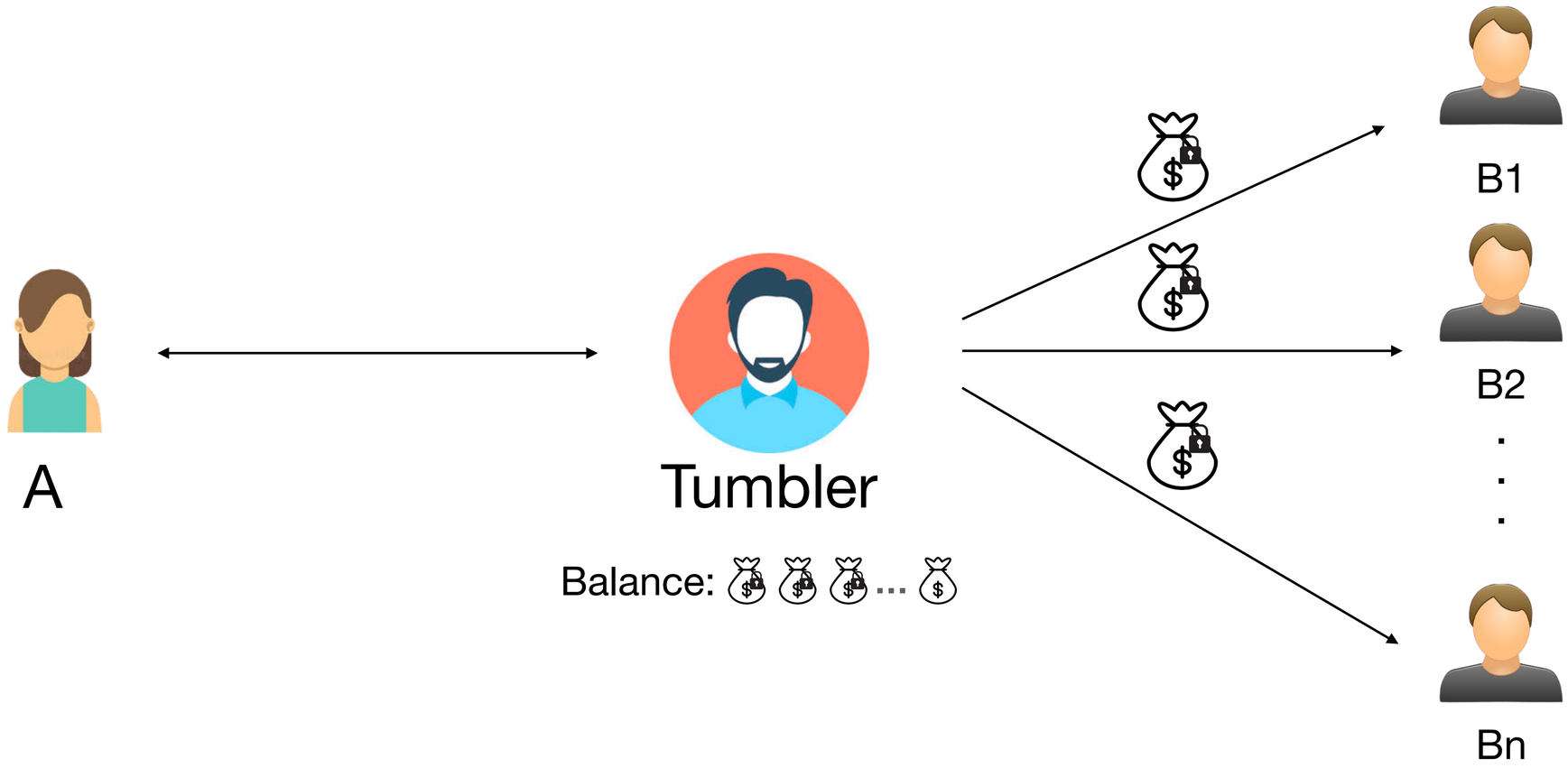
PCH with BlindChannel+Atomicity+Privacy+Griefing Resistance

Griefing Attack



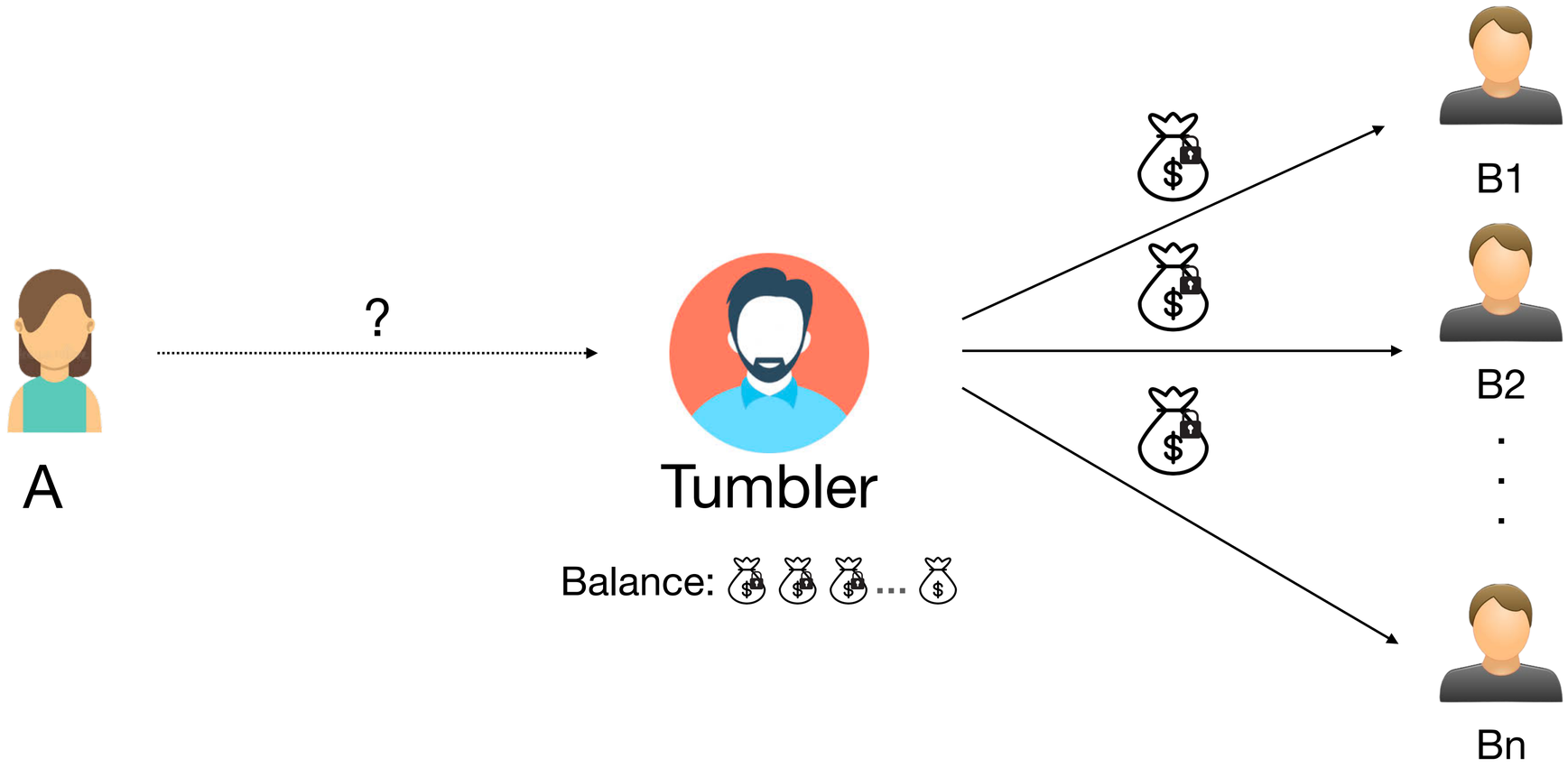
PCH with BlindChannel+Atomicity+Privacy+Griefing Resistance

Griefing Attack



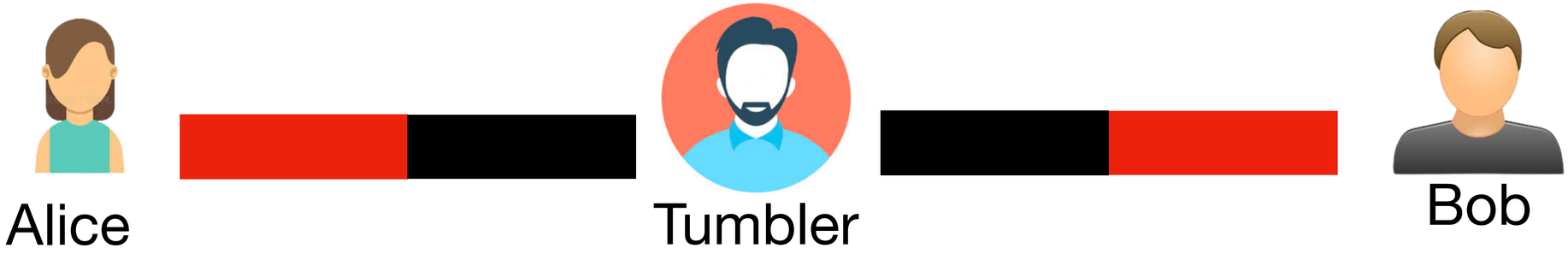
PCH with BlindChannel+Atomicity+Privacy+Griefing Resistance

Griefing Attack



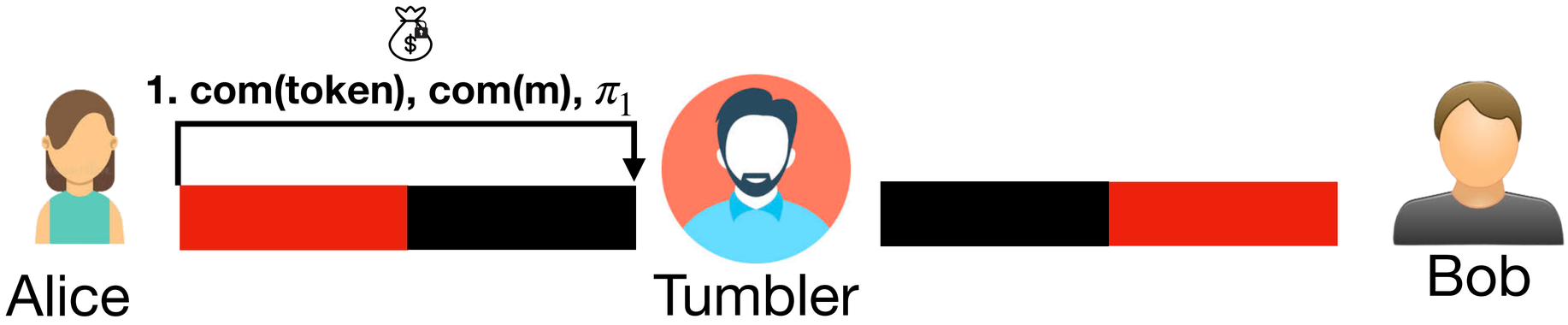
PCH with BlindChannel+Atomicity+Privacy+Griefing Resistance

Registration



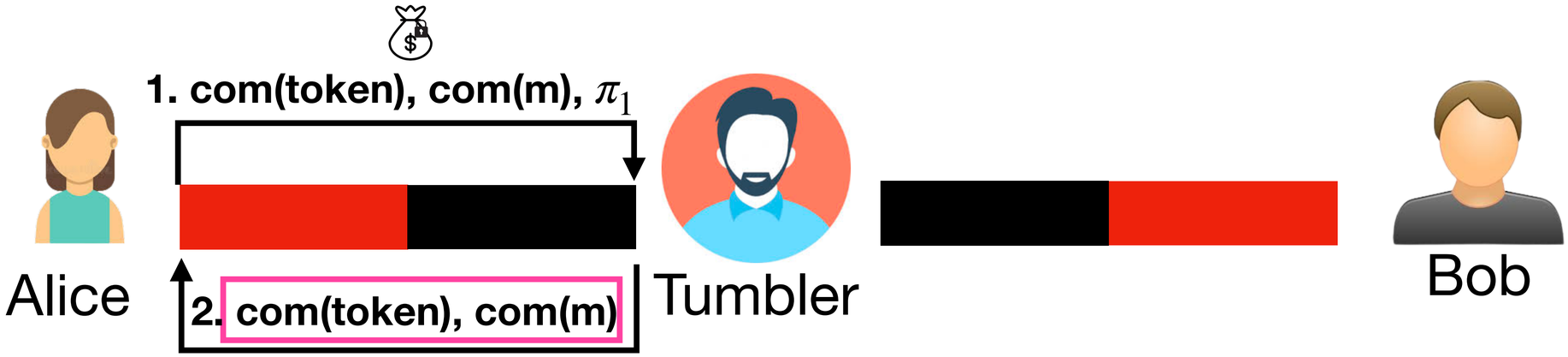
PCH with BlindChannel+Atomicity+Privacy+Griefing Resistance

Registration



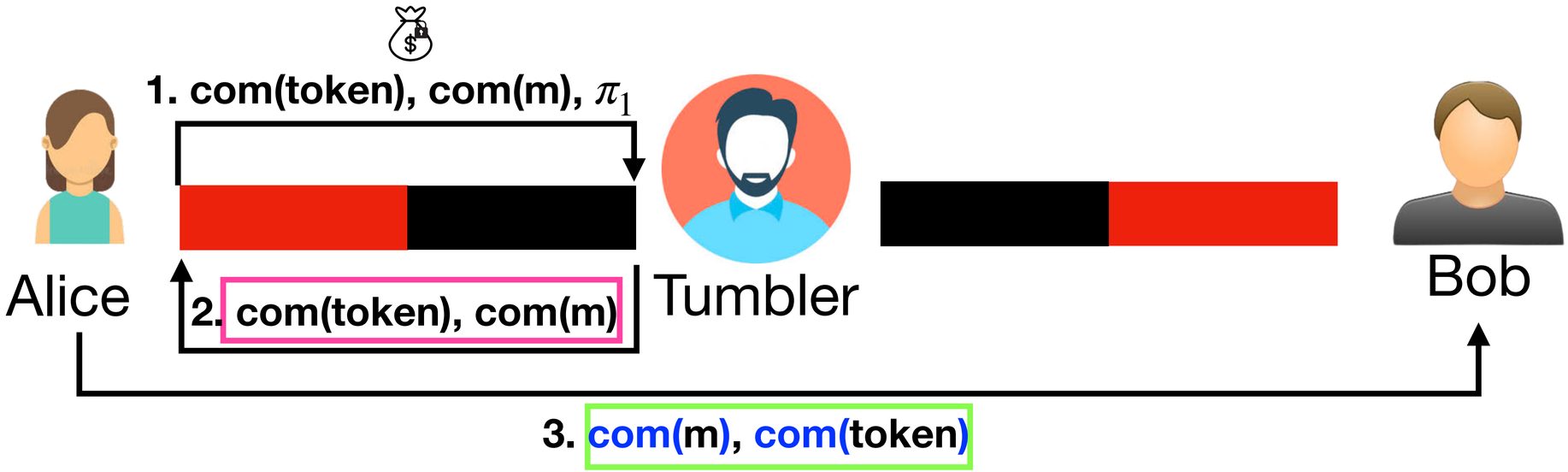
PCH with BlindChannel+Atomicity+Privacy+Griefing Resistance

Registration



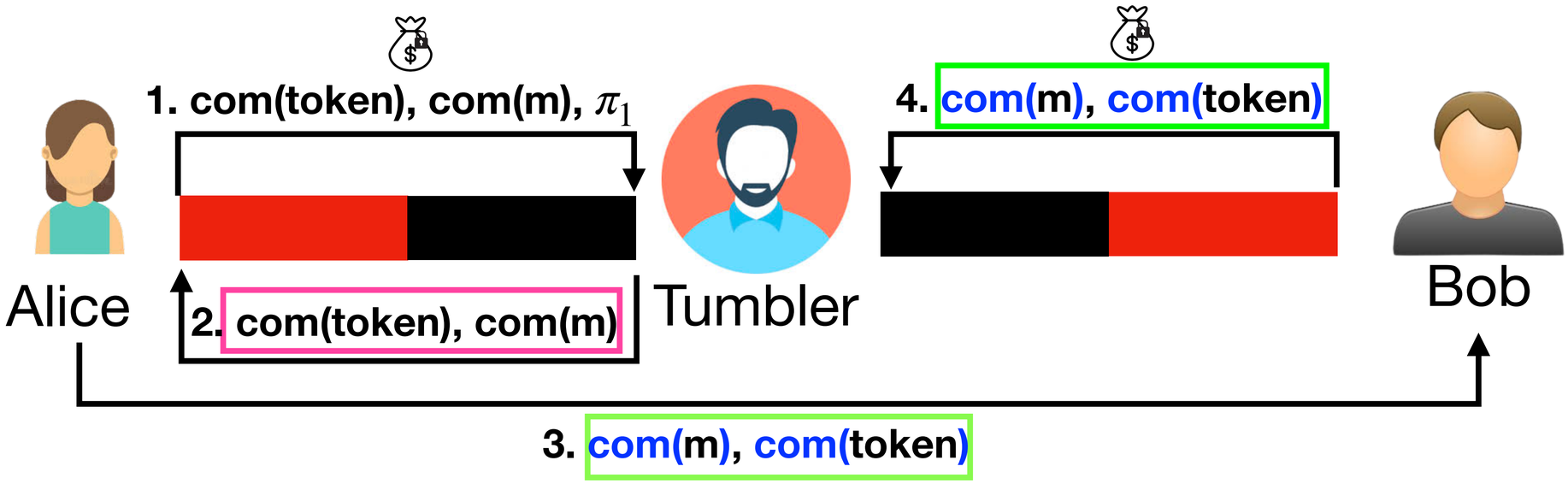
PCH with BlindChannel+Atomicity+Privacy+Griefing Resistance

Registration

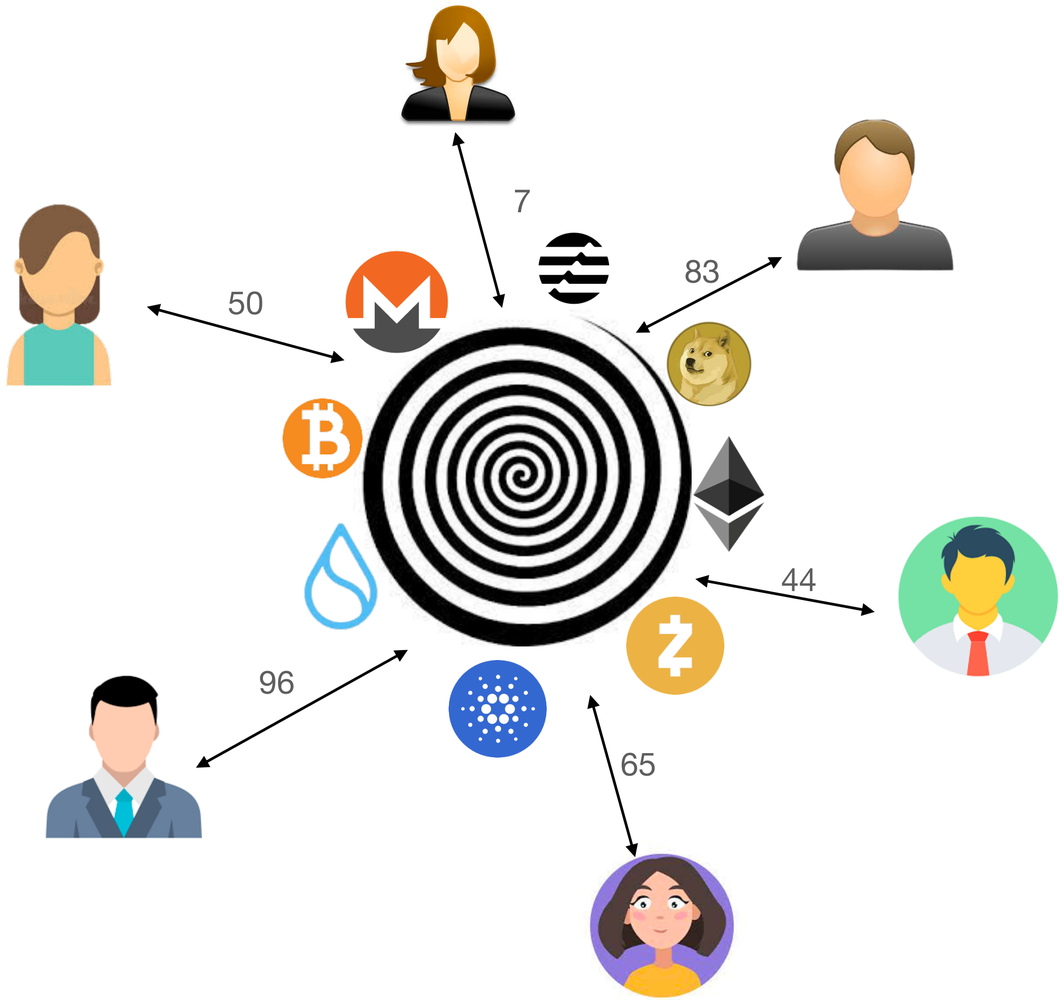


PCH with BlindChannel+Atomicity+Privacy+Griefing Resistance

Registration



PCH with BlindChannel+Atomicity+Privacy+Griefing Resistance = Blindhub



Performance

Role	Bandwidth (KB)	Comp. (ms)	Optimized Comp. (ms)
Sender	55843	8172	3083
Tumbler	87855	16245	8160
Receiver	32017	9063	6067

Phase	Bandwidth (KB)	Comp. (ms)	Optimized Comp. (ms)
Register	55843	8172	594
Promise	87855	16245	5773
Solver	32017	9063	2267
Open	16357	2284	520
Total	87860	17239	9154

Comment and comparison

- Limitation of our work

Comment and comparison

- Limitation of our work
  - Not UC secure

Comment and comparison

- Limitation of our work
  - Not UC secure
  - …

Comment and comparison

- My comment to this line of work
  -

Comment and comparison

- My comment to this line of work
  - Heavily rely on the honesty of the hub

Comment and comparison

- My comment to this line of work
  - Heavily rely on the honesty of the hub
    - Multiple hubs?

Comment and comparison

- My comment to this line of work
  - Heavily rely on the honesty of the hub
    - Multiple hubs?
  - K-anonymity

Comment and comparison

- Comparison

Comment and comparison

- Comparison
  - Tornado Cash
    - Payee can withdraw the coins whenever she wants (no time limits)
    - Rely on Turing-complete blockchain

Comment and comparison

- Comparison
  - Tornado Cash
    - Payee can withdraw the coins whenever she wants (no time limits)
    - Rely on Turing-complete blockchain
  - RGB
    - More Private, without relying on hub
    - Could not support Bitcoin itself

Future

- Compliance
  - Accountable Privacy
    - Example (paper) :
      - UTT (https://eprint.iacr.org/2022/452.pdf)
      - Pisces (https://eprint.iacr.org/2023/1317.pdf)

Thank you!

Full Version: https://eprint.iacr.org/2022/1735.pdf
Email: xrqin@cs.hku.hk