Sybil-Resistant Mixing for Bitcoin

George Bissias, **A. Pinar Ozisik**,
Brian N. Levine & Marc Liberatore

School of Computer Science
University of Massachusetts Amherst

Bitcoin Overview

Alice

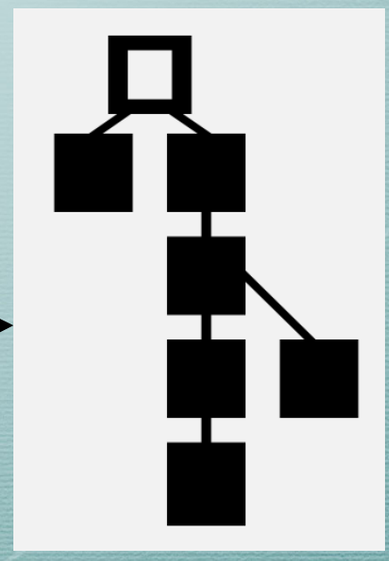
Bob

TX-1

TX

Input: Alice's Address, Prev. Tx, Sig

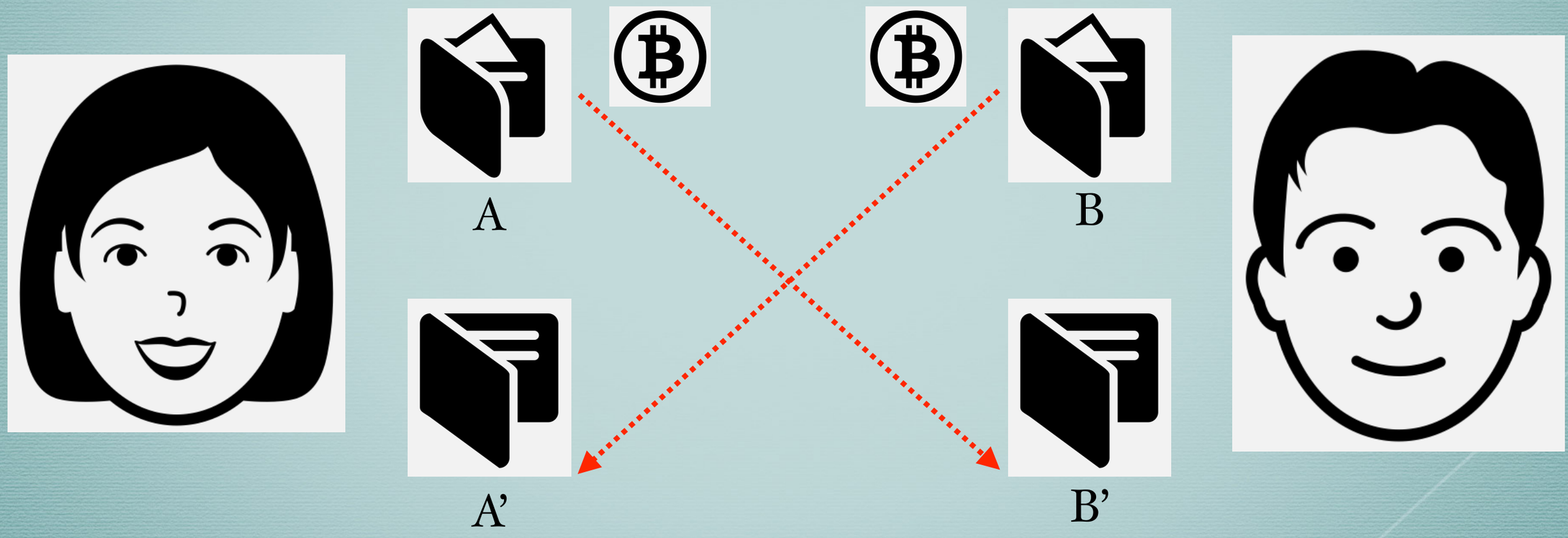
Output: Bob's Address, Bitcoin



Problem Definition

- Movement of coin from address to address is public
- Susceptible to inference attack
- Solution: **Mixing**

What is Mixing?



What should Mixing accomplish?

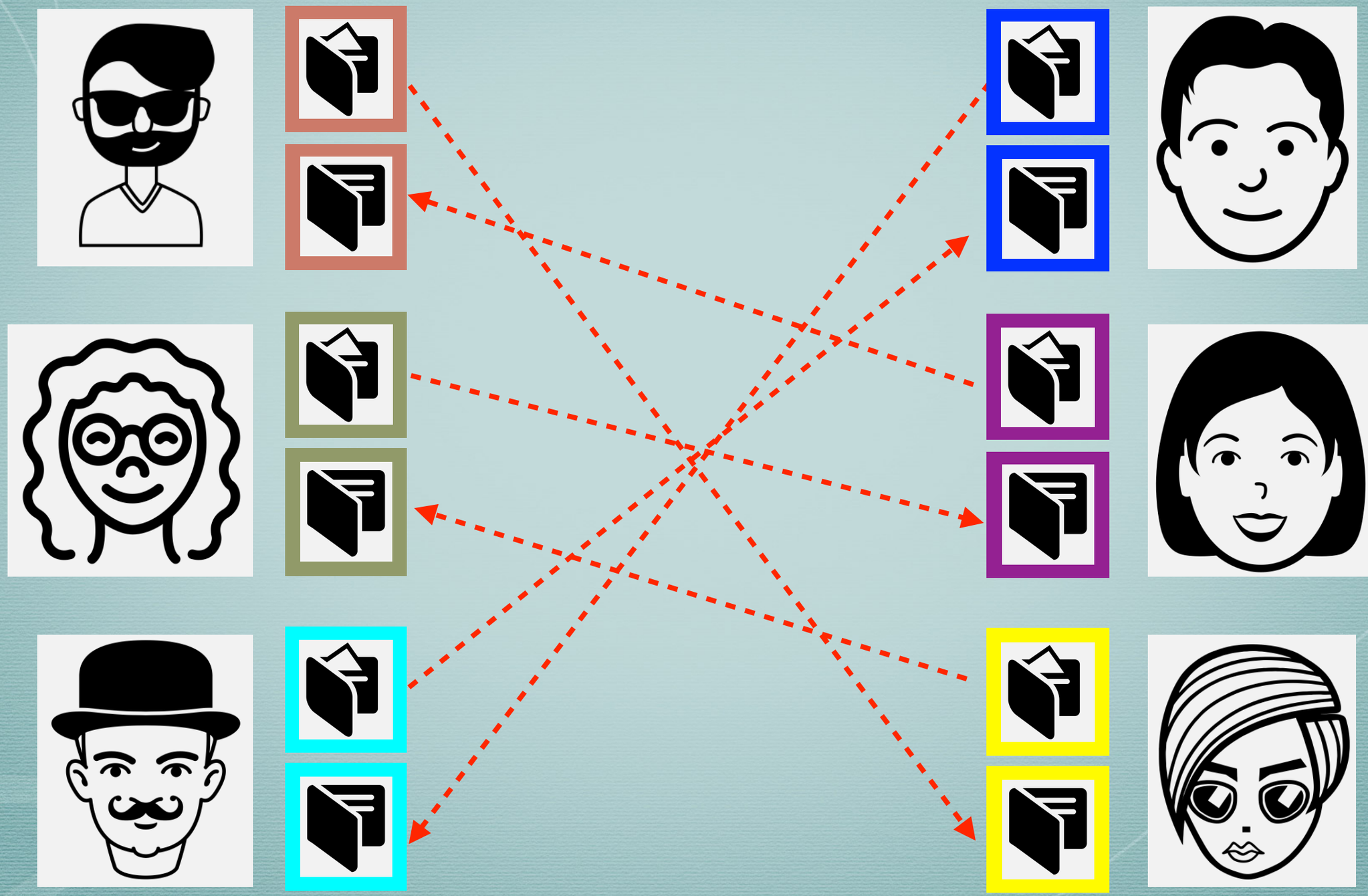
- Provide **matchmaking**
- Alice can't cheat Bob, vice versa
- No evidence on public block chain
- **Resistant** to DoS attack

Past Work

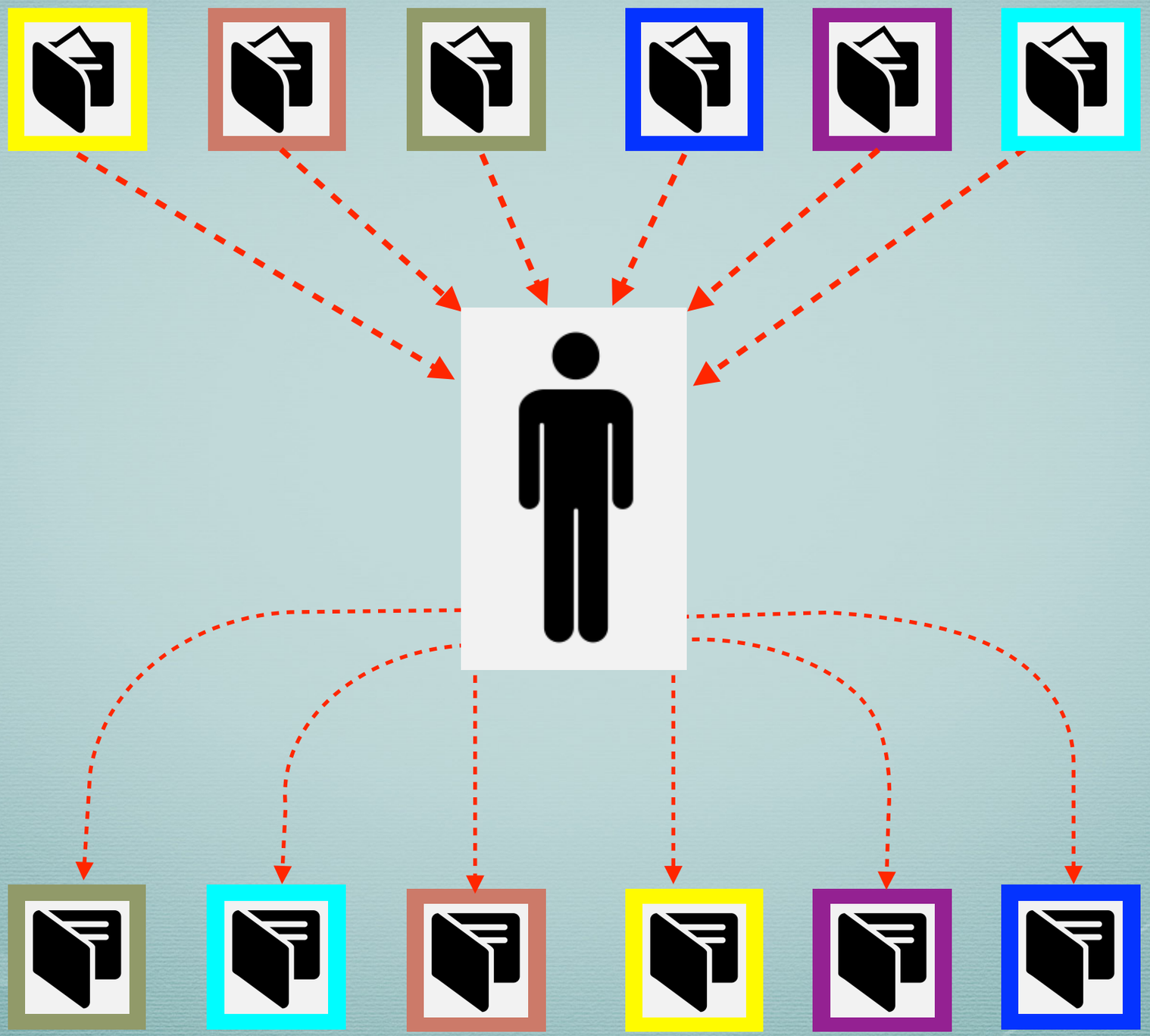
- CoinJoin[1]
- Barber et. al[2]

[1] Coinjoin. http://bitcointalk.org/index.php?topic=279249.0, May 2014
[2] S. Barber, X. Boyen, E. Shi, and E. Uzun. Bitter to Better —How to Make Bitcoin a Better Currency. In Proc. Financial Crypto. & Data Security, pages 399-414, Feb 2012.

Centralized CoinJoin



Centralized CoinJoin



Vulnerabilities in Centralized CoinJoin

- Participant list on block chain
- One participant deters, entire scheme fails
- DoS, Sybil & Profiling Attacks

Building Block for FairExchange

- **FairExchange:** Parties agree to deliver an item if and only if they receive an item in return
- **Barber et. al**: Cut & choose protocol for fair exchange using blind signatures

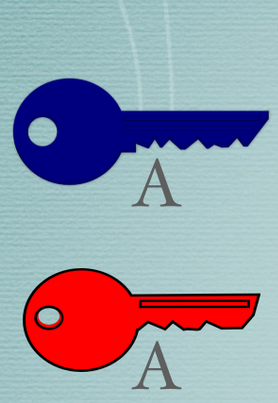
Limitations of Barber et. al.

- No mechanism for pairing participants
- No cost for bailing or participating
- No Sybil prevention

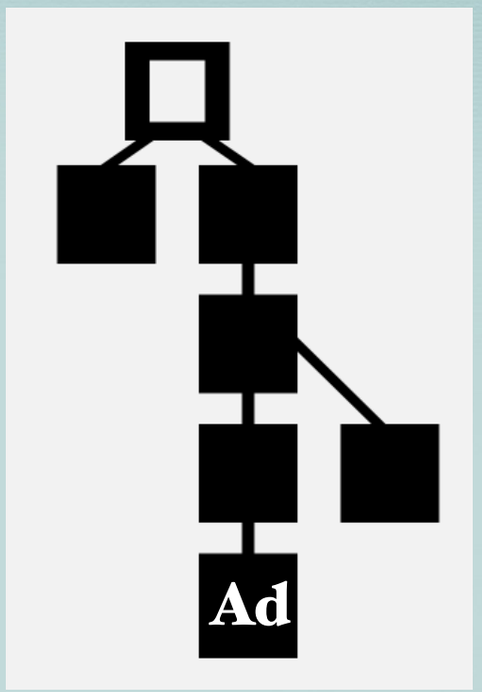
The Xim Protocol

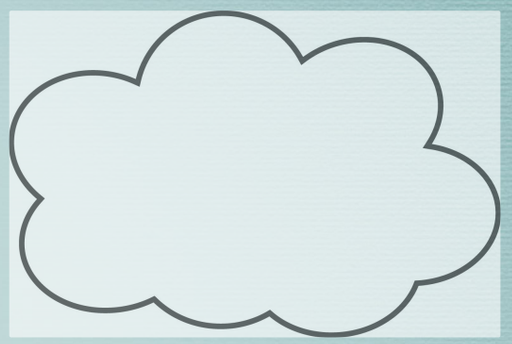
- Consists of:
  - Anonymous public matchmaking
  - FairExchange

Public Matchmaking

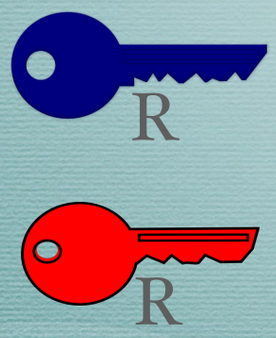


Address *A*

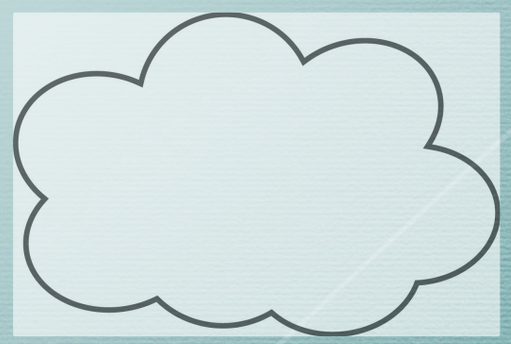




Tor Hidden Service α_A



Address *R*



Tor Hidden Service α_R

Overview
Public Matchmaking

3-way Handshake

1) Alice places an ad with a unique identifier

2) Bob responds to ad with another unique identifier

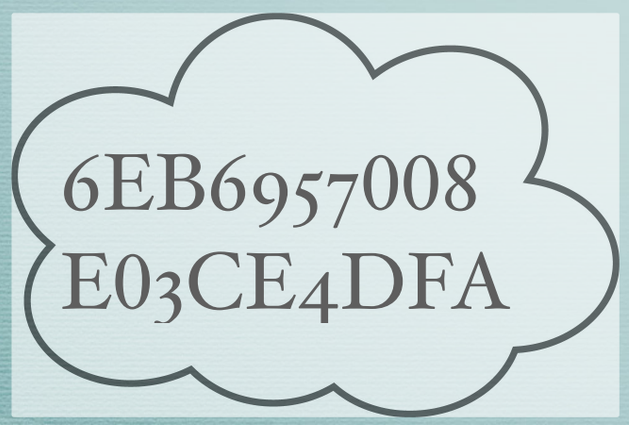
3) Alice confirms Bob's response with a hidden commitment

Public Matchmaking

1.

AD TX_1
Input: A, Prev. Tx
Text: loc = α_a, nonce = N_a
Output: A, $\tau/2$

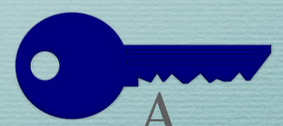
2.



α_A

Encrypt

N_a, N_r, α_R

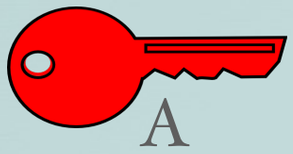


A

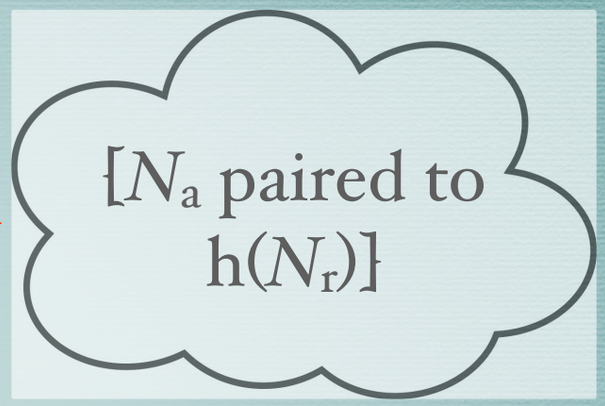
Public Matchmaking

3.

N_a paired to h(N_r)



Sig



α_A

4.

RESPONSE TX2

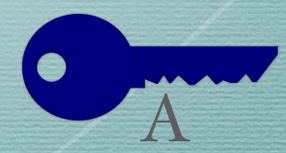
Input: *R*, Prev. Tx

Text: id = AD54FD190344BEC57

Output: *R*, τ

Encrypt

N_a, N_r



If all goes well…

5.

APPROVAL TX$_3$
Input: A, Prev. Tx
Text: lock = (N_a, h(N_r))
Output: A, $\tau/2$

Both parties can carry out a fair exchange.

Failure Recovery: Evil Responder

RESPONSE TX2

Input: *R*, Prev Tx

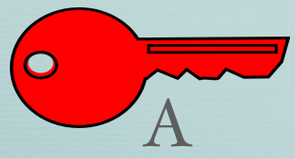
Text: id = AD54FDI[illegible]44BEC57

Output: *R*, τ

Failure Recovery

N_a unpaired from h(N_r)

Sig



A

{N_a unpaired from h(N_r)}

α_A

Failure Recovery: Evil Advertiser

APPROVAL TX$_3$
Input: *A*, Prev Tx
Text: lock = (N_r, h(N_r))
Output: *A*, τ/2

Failure Recovery

N_a aborted h(N_r)
proof: N_r

α_A

N_a aborted h(N_r)
proof: N_r

α_R

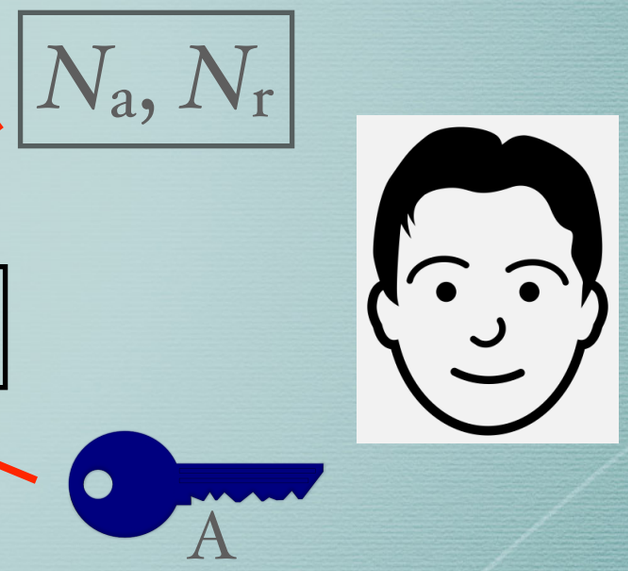
Failure Recovery

4. **RESPONSE TX2**

Input: R, Prev. Tx

Text: id = AD54FD190344BEC57

Output: R, τ



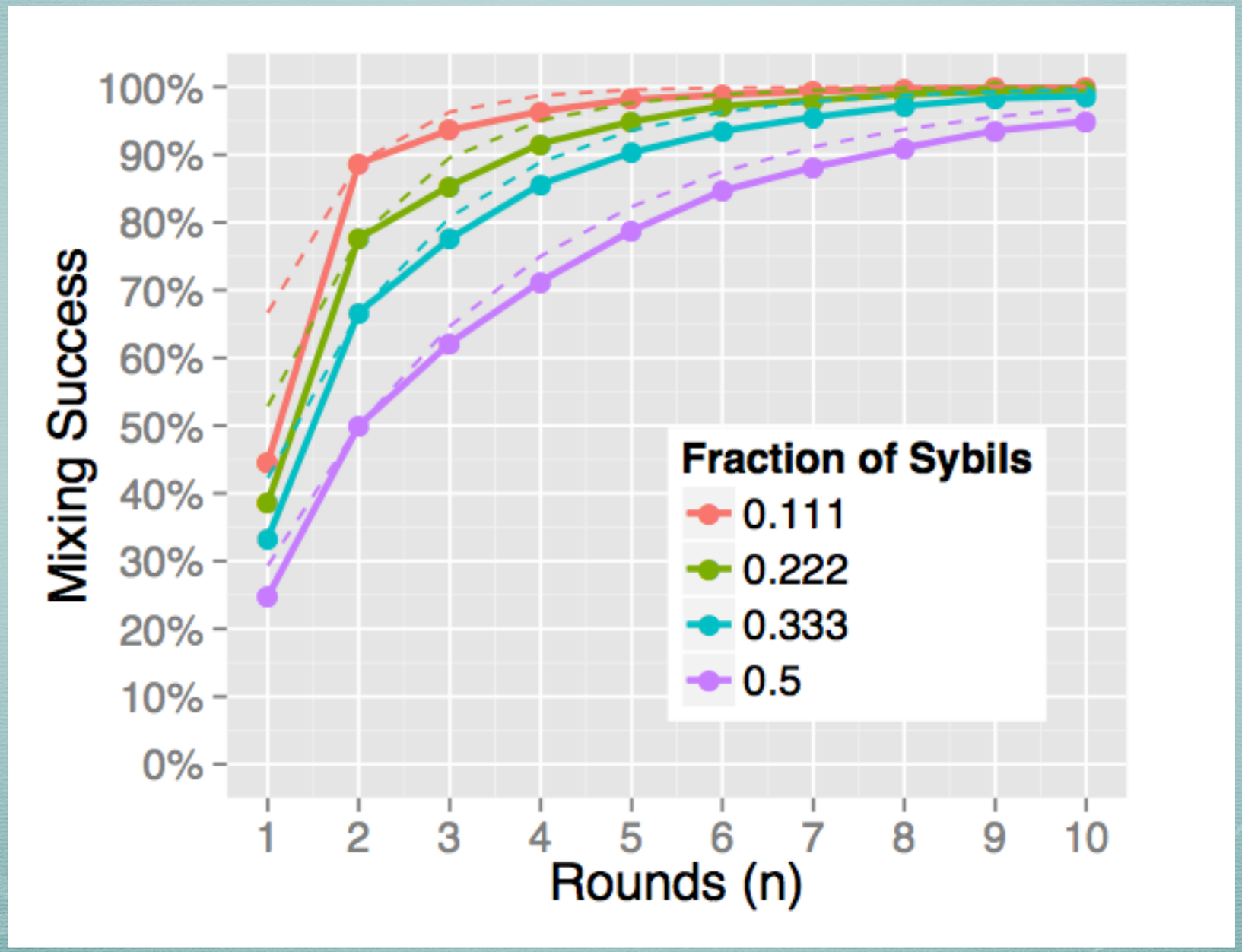
Cost of Bailing & Participating

- **All goes well:** Both parties pay τ
- **Responder bails:** Advertiser can reuse their ad
- **Advertiser bails:** Advertiser pays $\tau/2$, responder pays τ

Advantages of Xim

- Cost to advertising mitigates Sybils
- No evidence of pairing on the block chain
- No central authority
- Matchmaking and FairExchange define a complete protocol
- Compatible with Bitcoin and derivatives

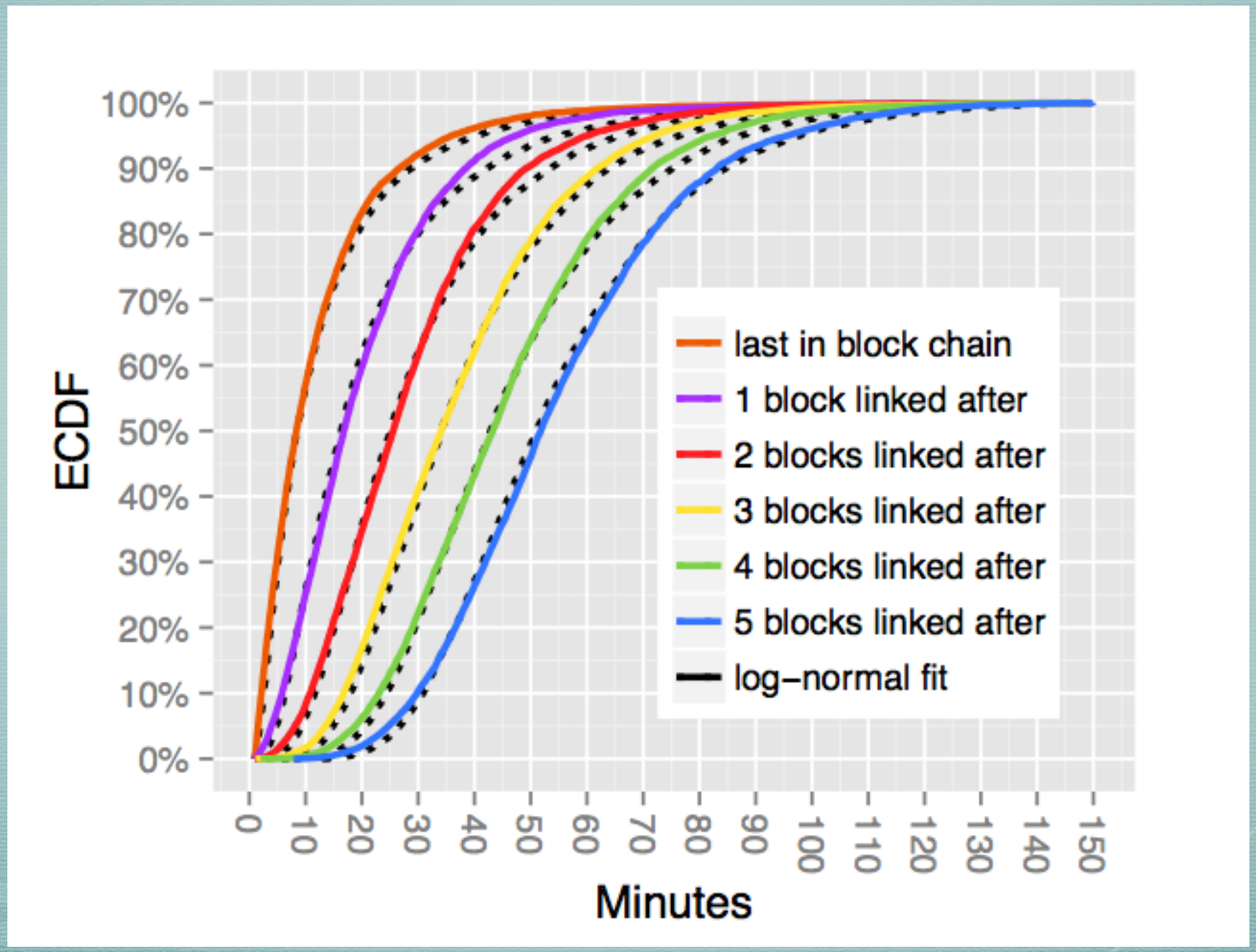
How successful is Xim?



Resistance to DoS

- Cost for honest participant is **linear**
- If 10% of the participants are Sybils, 10% additional cost

Parameter Settings



Xim Overview

- **Xim:** Public Matchmaking and FairExchange
- Resilient against Sybil and DoS Attacks
- Tunable parameters for better performance

References

- Coinjoin. http://bitcointalk.org/index.php?topic=279249.0, May 2014
- S. Barber, X. Boyen, E. Shi, and E. Uzun. Bitter to Better —How to Make Bitcoin a Better Currency. In Proc. Financial Crypto. & Data Security, pages 399-414, Feb 2012.
- S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. Voelker, and S. Savage. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In Proc. ACM IMC, pages 127-140, 2013.
- Icons from http://www.thenounproject.com

Barber et. al

- One side bails, other person gets their money back
- Both Alice and Bob commit money to each other's wallet
- When Bob claims his Bitcoin, he reveals a secret that enables Alice to claim her Bitcoin