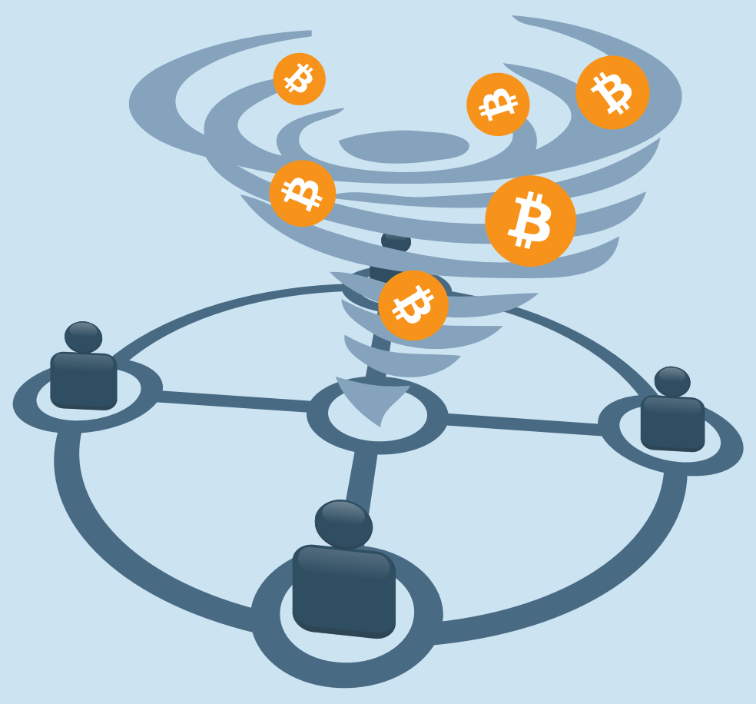
ValueShuffle: Mixing Confidential Transactions

Tim Ruffing
Saarland University
@real_or_random

Pedro Moreno-Sanchez
Purdue University
@pedrorechez

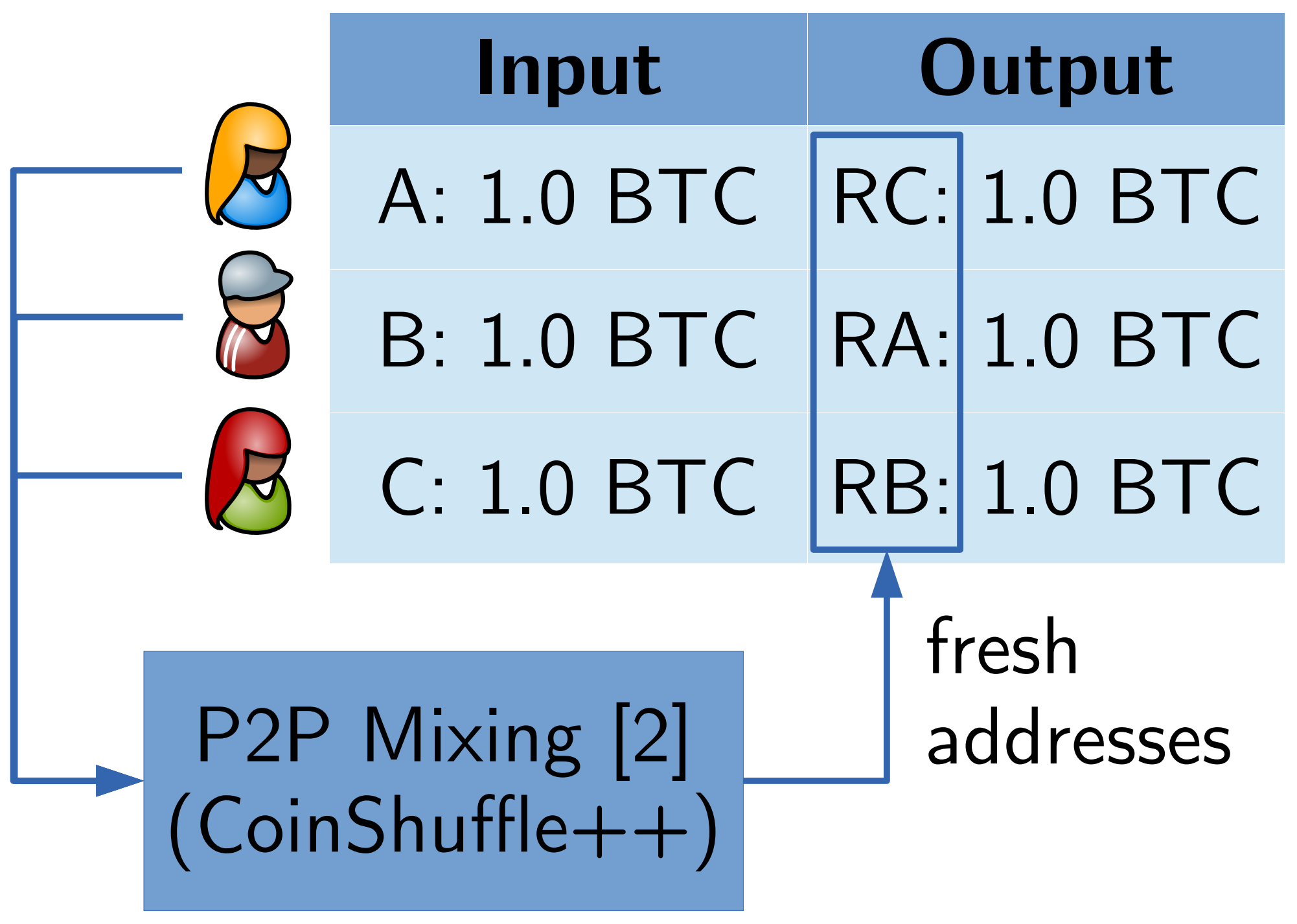


Problem: Privacy Issues in Bitcoin

Input	Output
A: 1.0 BTC	RA: 0.1 BTC
	A′: 0.9 BTC
Alice	

- Sender and receiver linkable
- Leakage through change address
- Amounts disclosed

CoinJoin [1]



Input	Output
A: 1.0 BTC	RC: 1.0 BTC
B: 1.0 BTC	RA: 1.0 BTC
C: 1.0 BTC	RB: 1.0 BTC

Pros:
✓ Sender and receiver unlinkable

Cons:
✗ Amounts disclosed
✗ Only fixed amounts to ensure unlinkability

Confidential Transactions [3]

$$\mathrm{Com}(x_1, r_1) \oplus \mathrm{Com}(x_2, r_2) = \mathrm{Com}(x_1+x_2, r_1+r_2)$$

Input	Output
A: Com(1.0, $r_{\mathrm{in},1}$)	RA: Com(0.1, $r_{\mathrm{out},1}$)
	A′: Com(0.9, $r_{\mathrm{out},2}$)

$$\mathrm{Com}(1.0, r_{\mathrm{in},1}) \overset{?}{=} \begin{matrix}\mathrm{Com}(0.1, r_{\mathrm{out},1}) \\ \oplus \\ \mathrm{Com}(0.9, r_{\mathrm{out},2})\end{matrix}$$

Pros:
✓ Hidden amount

Cons:
✗ Linkability
✗ User creating the transaction learns amounts

Challenge: Combining CoinJoin and CT

How to ensure

$$\sum_i r_{\mathrm{in},i} = \sum_i r_{\mathrm{out},i}$$

without revealing $r_{\mathrm{in,i}}$ and $r_{\mathrm{out,i}}$ to other peers?

Our Solution: ValueShuffle [4]

Input	Output
A: Com(5.4, r_{in},A)	C′: Com(0.1, $r_{\mathrm{out,C'}}$)
B: Com(1.2, r_{in},B)	B′: Com(0.7, $r_{\mathrm{out,B'}}$)
C: Com(0.3, r_{in},C)	RA: Com(0.4, $r_{\mathrm{out,RA}}$)
	RC: Com(0.2, $r_{\mathrm{out,RC}}$)
	A′: Com(5.0, $r_{\mathrm{out,A'}}$)
	RB: Com(0.5, $r_{\mathrm{out,RB}}$)
	F: Com(0.0, $-\,r_{\Delta}$)

Also possible without adding this output

$$r_\Delta = \sum_i r_{\mathrm{in},i} - \Big(\sum_i r_{\mathrm{out},i} + \sum_i r_{\mathrm{out},i}\Big) = \sum_i \big(r_{\mathrm{in},i} - (r_{\mathrm{out},i} + r_{\mathrm{out},i})\big)$$

We need to compute a sum such that individual summands are not revealed.

ValueShuffle = CoinShuffle++ + Secure Sum Protocol (DC-net)

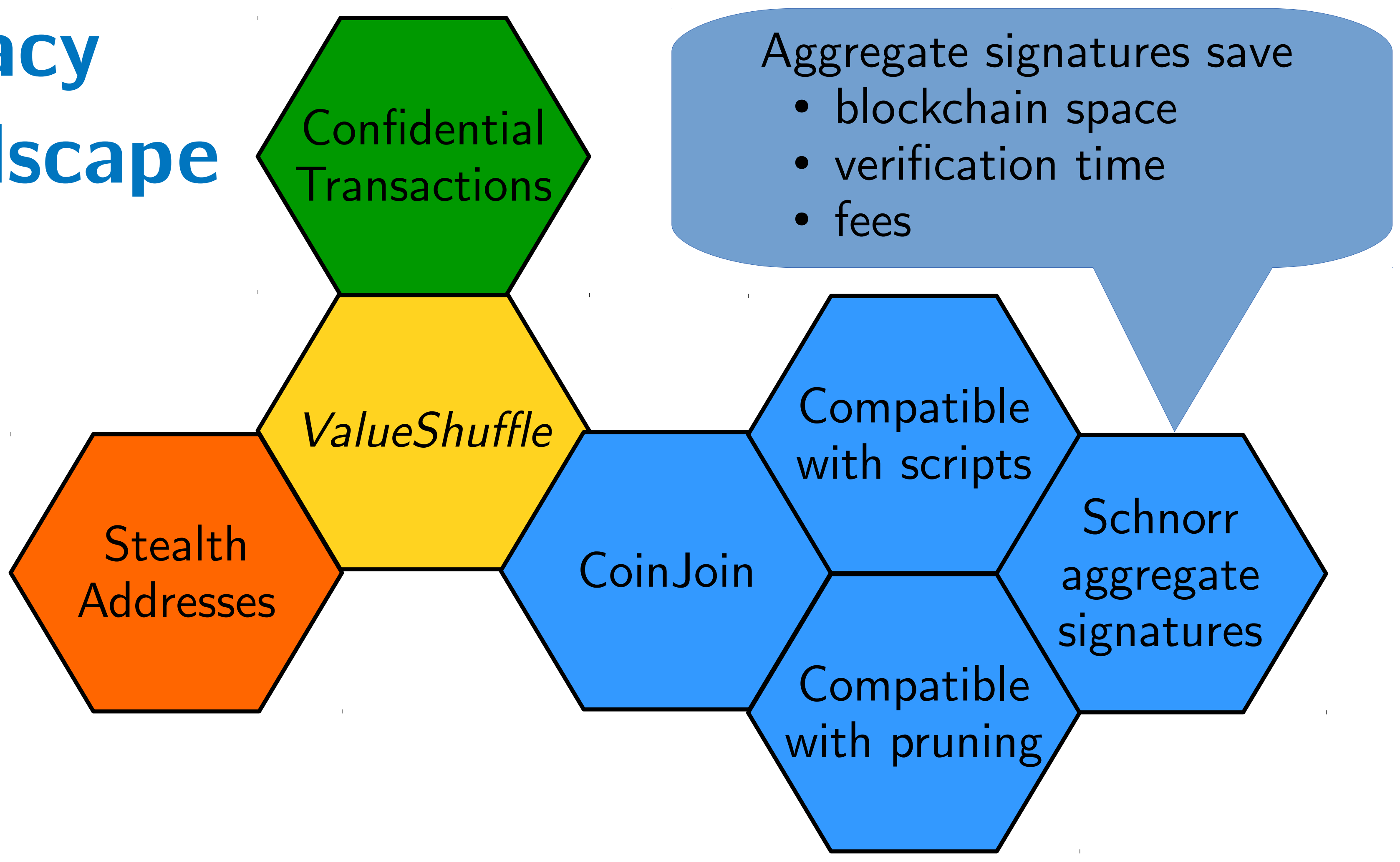
Main Technical Challenge

If a malicious peer sends garbage in the secure sum protocol, how can we identify and exclude him to ensure termination of ValueShuffle without hurting privacy?

Benefits

- Sender Anonymity
- Termination in the presence of disruptive peers
- Mixing with different amounts
- No leakage through change addresses
- Mixing and actual spending in just one transaction
- Efficiency: Just $4+2f$ communication rounds for f actively disrupting peers (uses central bulletin board)

Privacy Landscape



Aggregate signatures save
- blockchain space
- verification time
- fees

References

[1] Gregory Maxwell. *CoinJoin: Bitcoin Privacy for the Real World*. Post on Bitcoin Forum (2013). https://bitcointalk.org/index.php?topic=279249

[2] Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate. *P2P Mixing and Unlinkable Bitcoin Transactions*. NDSS'17

[3] Gregory Maxwell. *Confidential Transactions*. Technical Report (2015). https://people.xiph.org/~greg/confidential_values.txt

[4] Tim Ruffing, Pedro Moreno-Sanchez. *Mixing Confidential Transactions: Comprehensive Transaction Privacy for Bitcoin*. BITCOIN'17

[5] Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate. *CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin*. ESORICS'14

UNIVERSITÄT DES SAARLANDES

PURDUE UNIVERSITY