COIN PARTY

Secure and Anonymous Decentralized Bitcoin Mixing

Jan Henrik Ziegeldorf, Roman Matzutt, Fred Grossmann, Martin Henze, Klaus Wehrle

Communication and Distributed Systems (COMSYS), RWTH Aachen, Germany

Bitcoin in a nutshell

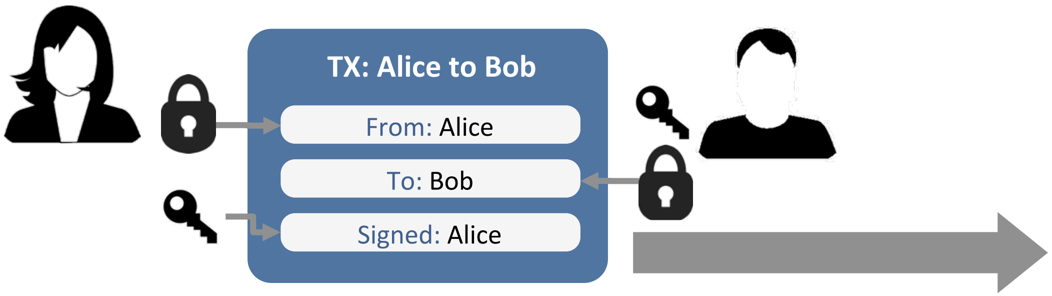
Bitcoin: A decentralized crypto-currency.

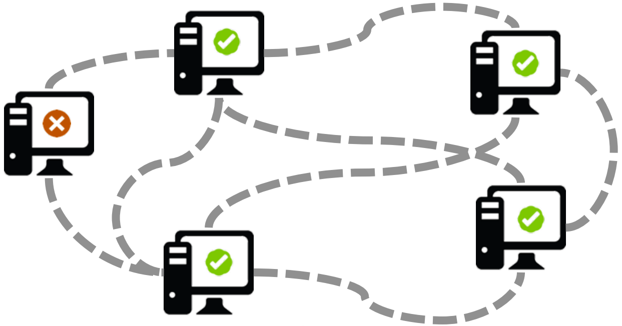
TRANSACTIONS

Signed transfers between Bitcoin addresses.

P2P WORKER POOL

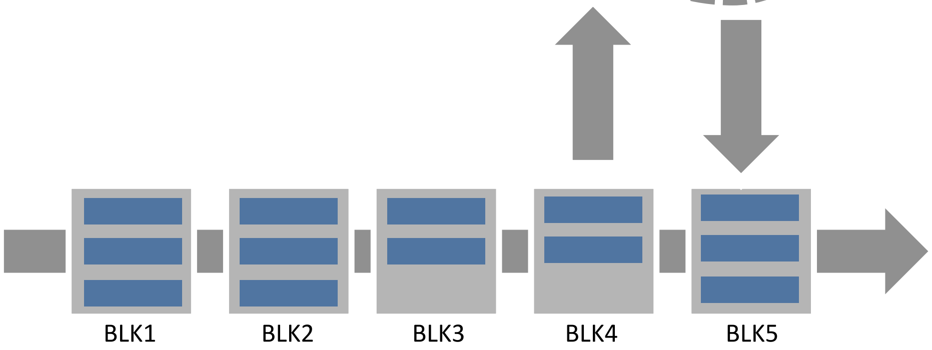
Proof of work to ensure correctness.



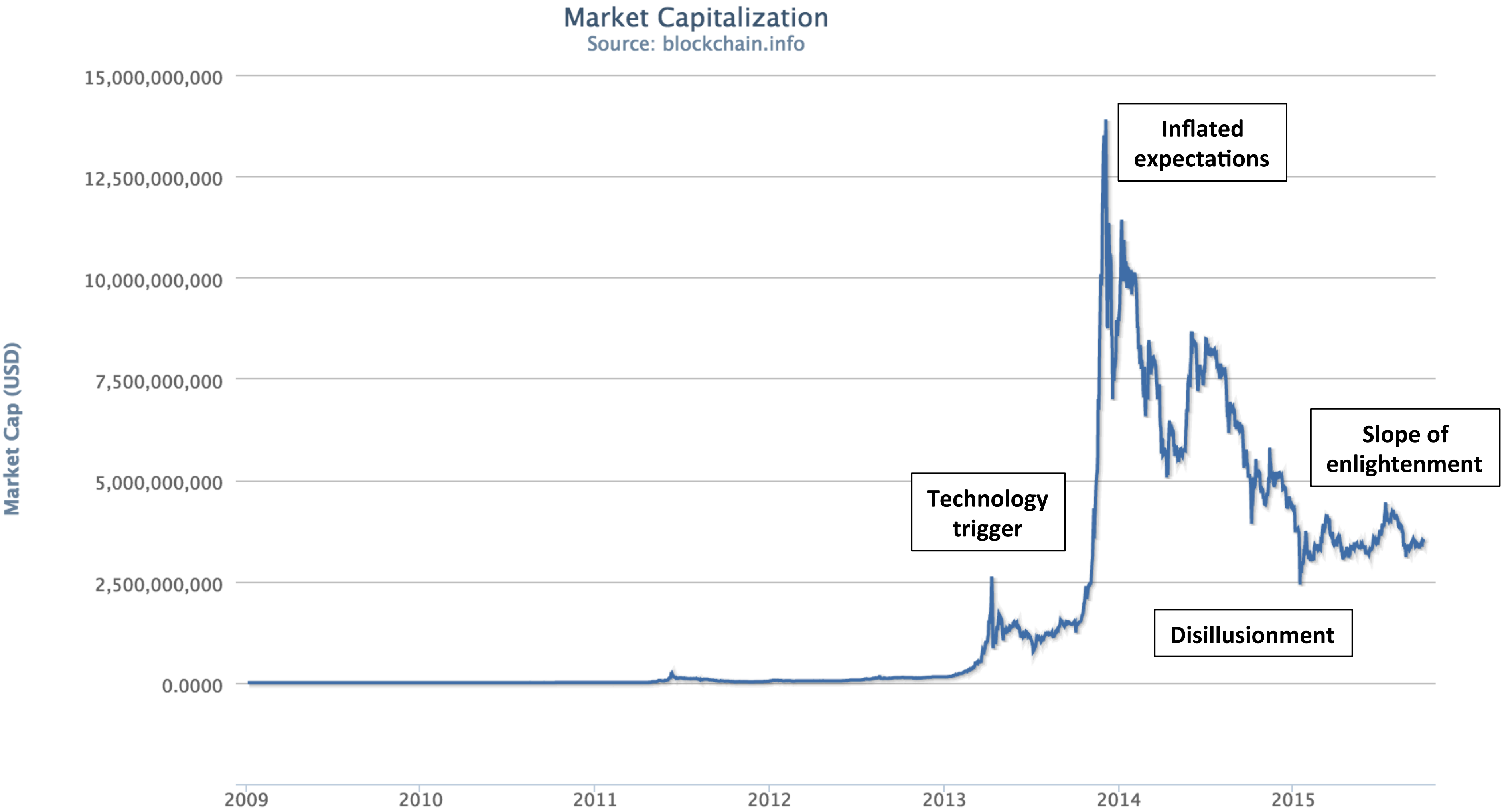


BLOCKCHAIN

A **shared public ledger** of all accepted transactions to keep balances.
Rules out, e.g., double spending.



The Bitcoin Hype Cycle



Market Capitalization

Source: blockchain.info

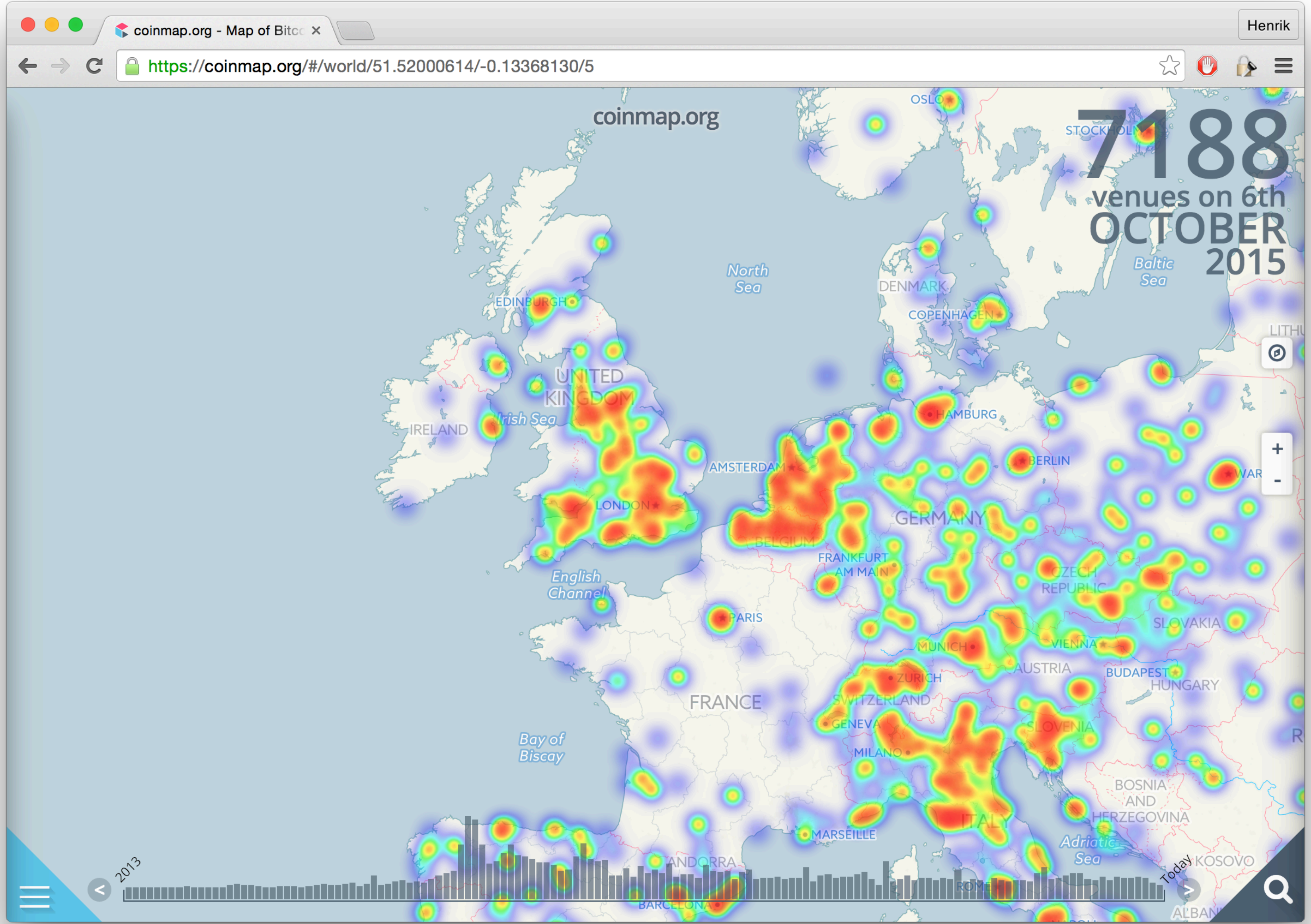
Inflated expectations

Technology trigger

Slope of enlightenment

Disillusionment

Is it used at all?



Pro's and Con's

Why is Bitcoin used?

- Investment (a really bad one)
- Fast (and simple)
- More secure (in a way)
- Cool & hip
- …

vs.

- Scams, crime, theft
- Volatility
- Low adoption
- …

Silk Road

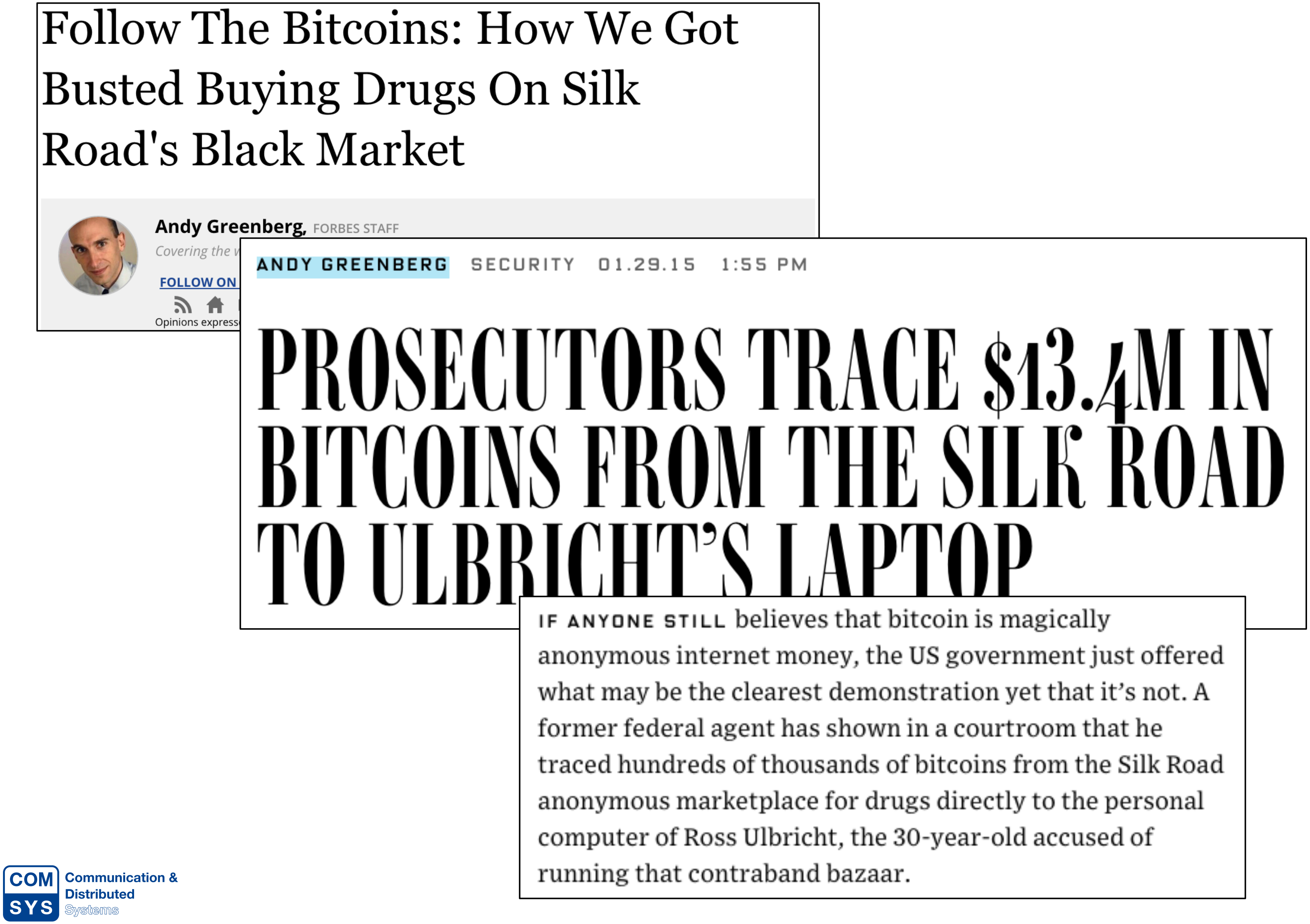
anonymous marketplace

Because it offers …

ANONYMITY / FINANCIAL PRIVACY

(No, it doesn't)

Downfall of Silkroad



Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market

Andy Greenberg, FORBES STAFF

Covering the w

FOLLOW ON

Opinions express

ANDY GREENBERG SECURITY 01.29.15 1:55 PM

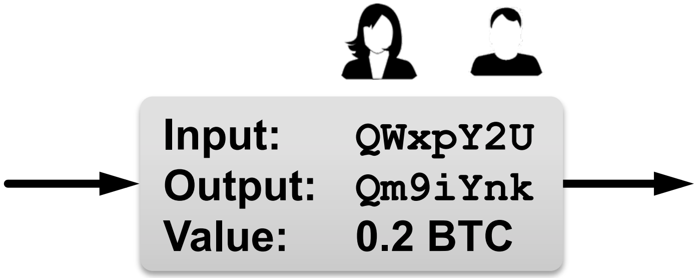
PROSECUTORS TRACE $13.4M IN BITCOINS FROM THE SILK ROAD TO ULBRICHT'S LAPTOP

IF ANYONE STILL believes that bitcoin is magically anonymous internet money, the US government just offered what may be the clearest demonstration yet that it's not. A former federal agent has shown in a courtroom that he traced hundreds of thousands of bitcoins from the Silk Road anonymous marketplace for drugs directly to the personal computer of Ross Ulbricht, the 30-year-old accused of running that contraband bazaar.

Financial Privacy in Bitcoin

PSEUDONYMITY

Virtually unlimited amount of addresses.



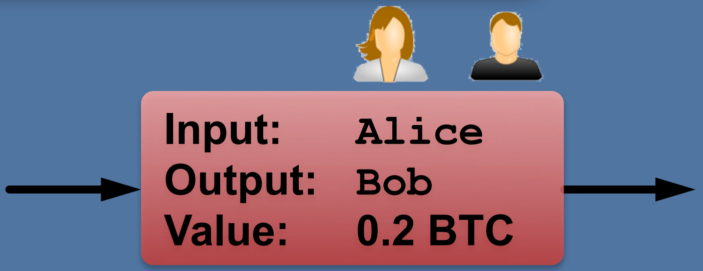
Input: QWxpY2U
Output: Qm9iYnk
Value: 0.2 BTC

Silk Road
anonymous market

How to re-establish Bitcoin's broken promise of financial privacy?

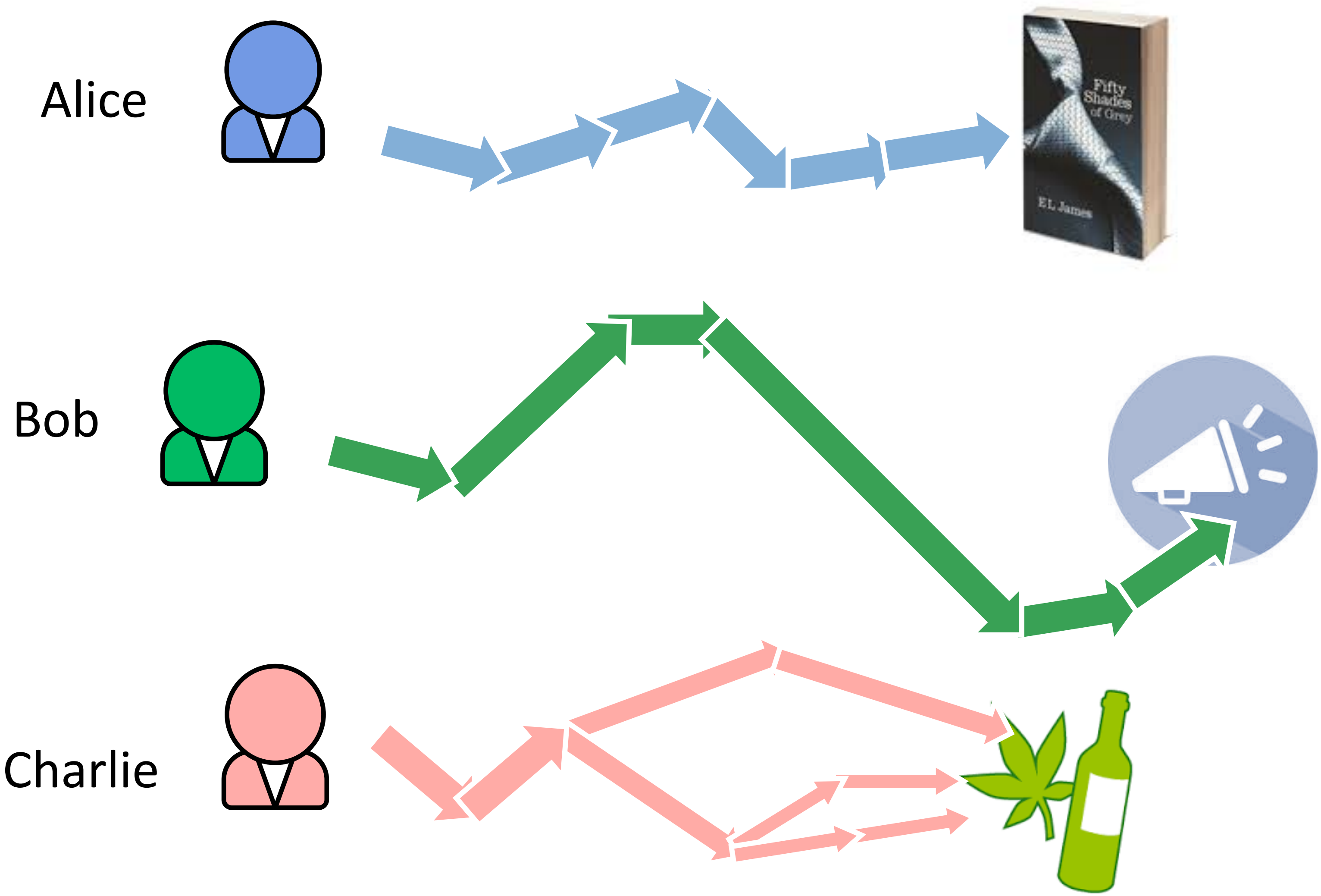
DE-ANONYMISATION

Blockchain taint analysis + side channels.

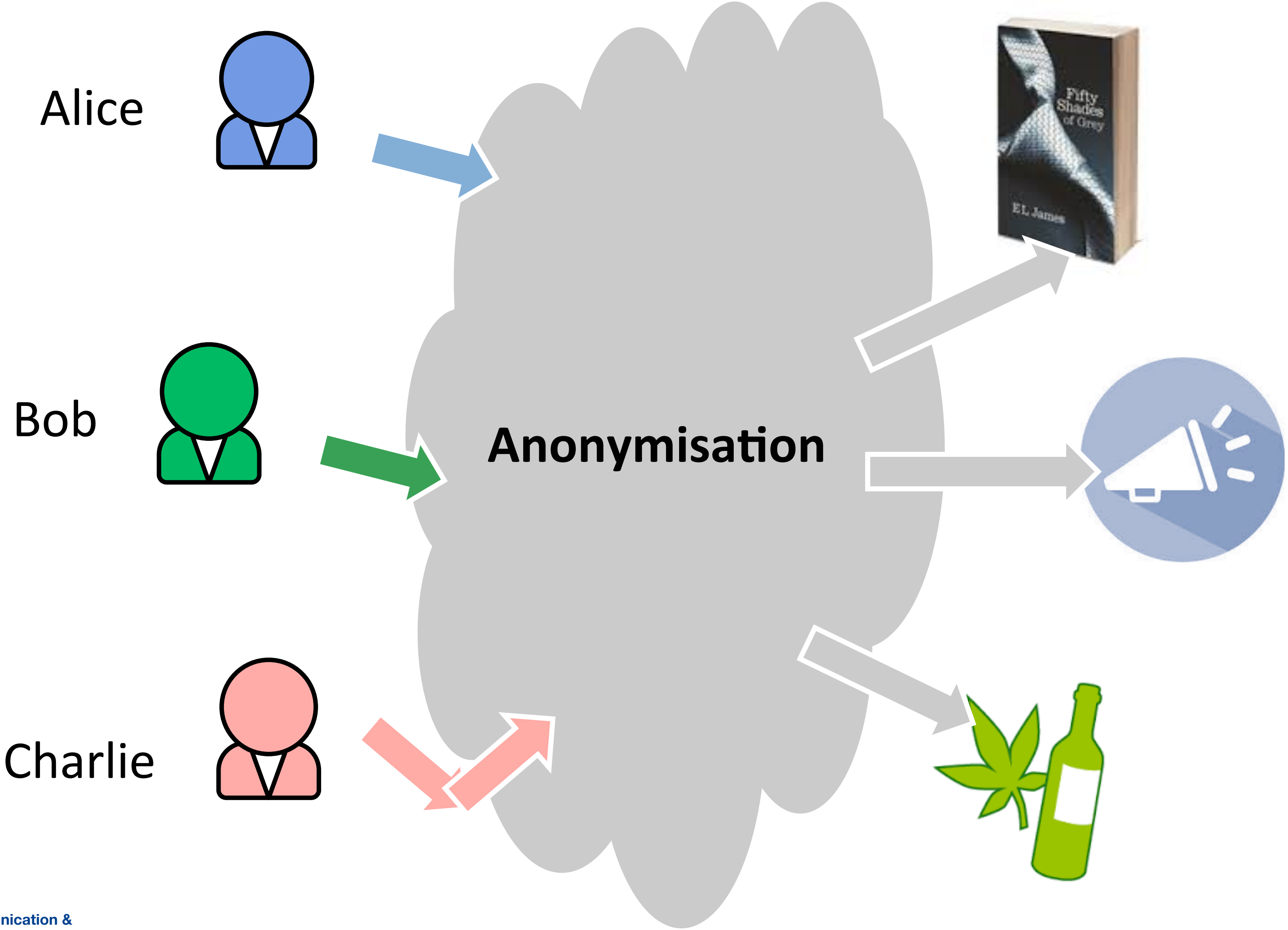


Input: Alice
Output: Bob
Value: 0.2 BTC

Bitcoin Mixing by Example



Bitcoin Mixing by Example



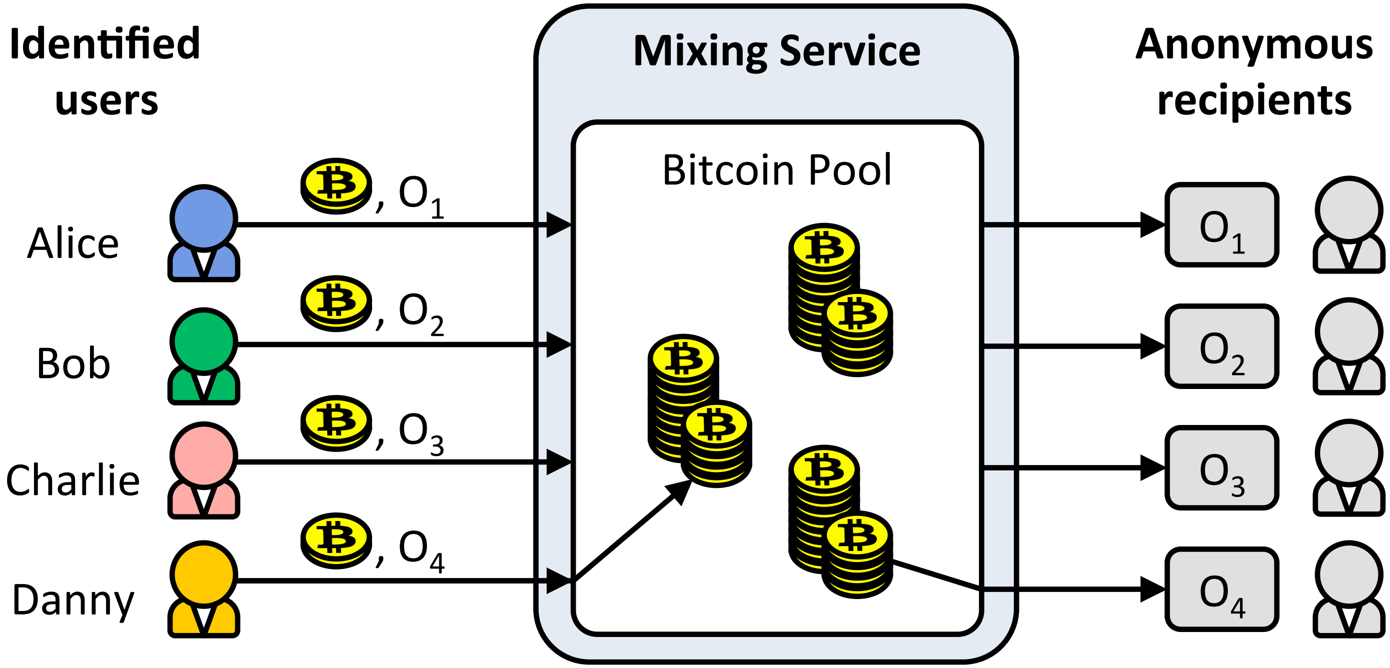
Alice

Bob

Charlie

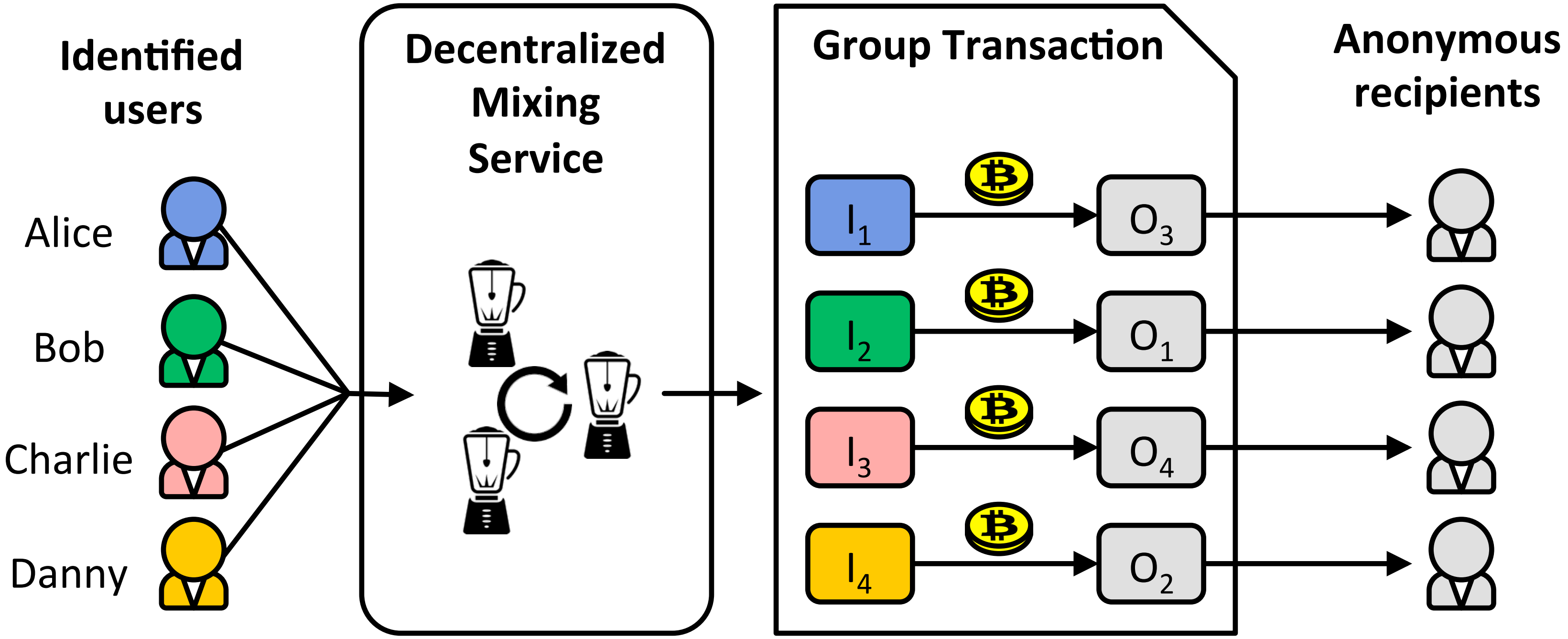
Anonymisation

1st Gen: Centralized mixing / eWallets / Improvements



- **Pros:** Easy to use, scalable, big anonymity sets
- **Cons:** TTP is single point of failure, involved mixing & Transaction fees
- **Improvements:** Mixcoin, BlindCoin

2nd Gen: Decentralized Mixing (CoinJoin, CoinShuffle, …)



- E.g. CoinJoin, CoinShuffle (implemented in NXTcoin?), XIM
- **Pros:** Secure, anonymity against insiders, no TTP, no SPoF
- **Cons:** Small anonymity sets, no deniability, (scalability)

Desiderata

Requirements for an ideal mixing service

SECURITY

No theft, double spending or loss of funds.
No DoS.

ANONYMITY

Anonymous against in- and outsiders.
Big anonymity sets.
Unbiased randomness.

DENIABILITY

Means of plausible deniability.
No cryptographic evidence.

[

MISUSE PREVENTION

Prevent money-laundering, …

]

SCALABILITY

Large numbers of users.
Low impact on Bitcoin network.

COST EFFICIENCY

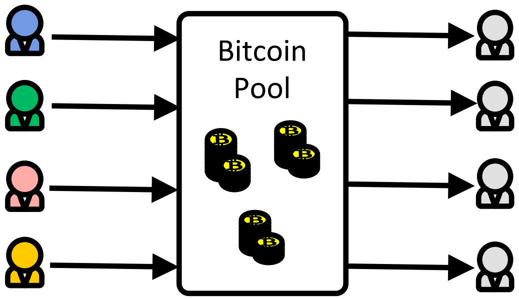
No mixing fees.
Minimal transaction fees.

APPLICABILITY & USABILITY

Compatible with Bitcoin network.
No additional software.

This presentation

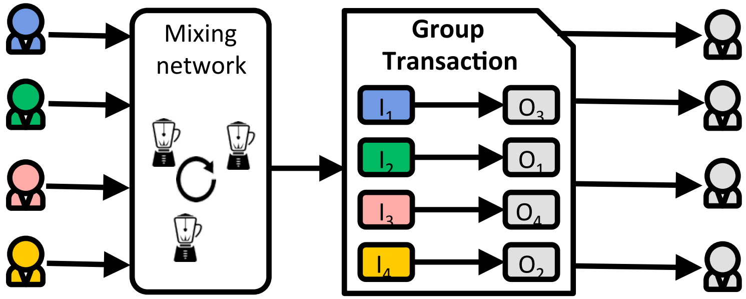
Centralized mixing



🟥 Security | 🟥🟩 Anonymity | 🟩 Deniability

🟩 Scalability | 🟧 Costs | 🟩 Usability

Decentralized mixing



🟩 Security | 🟩🟥 Anonymity | 🟥 Deniability

🟧 Scalability | 🟩 Costs | 🟧 Usability

COIN
PARTY

OUR APPROACH

- Threshold ECDSA
- Single instead of group transactions
- Separate input and mixing peers

🟩 Security

🟩 Anonymity

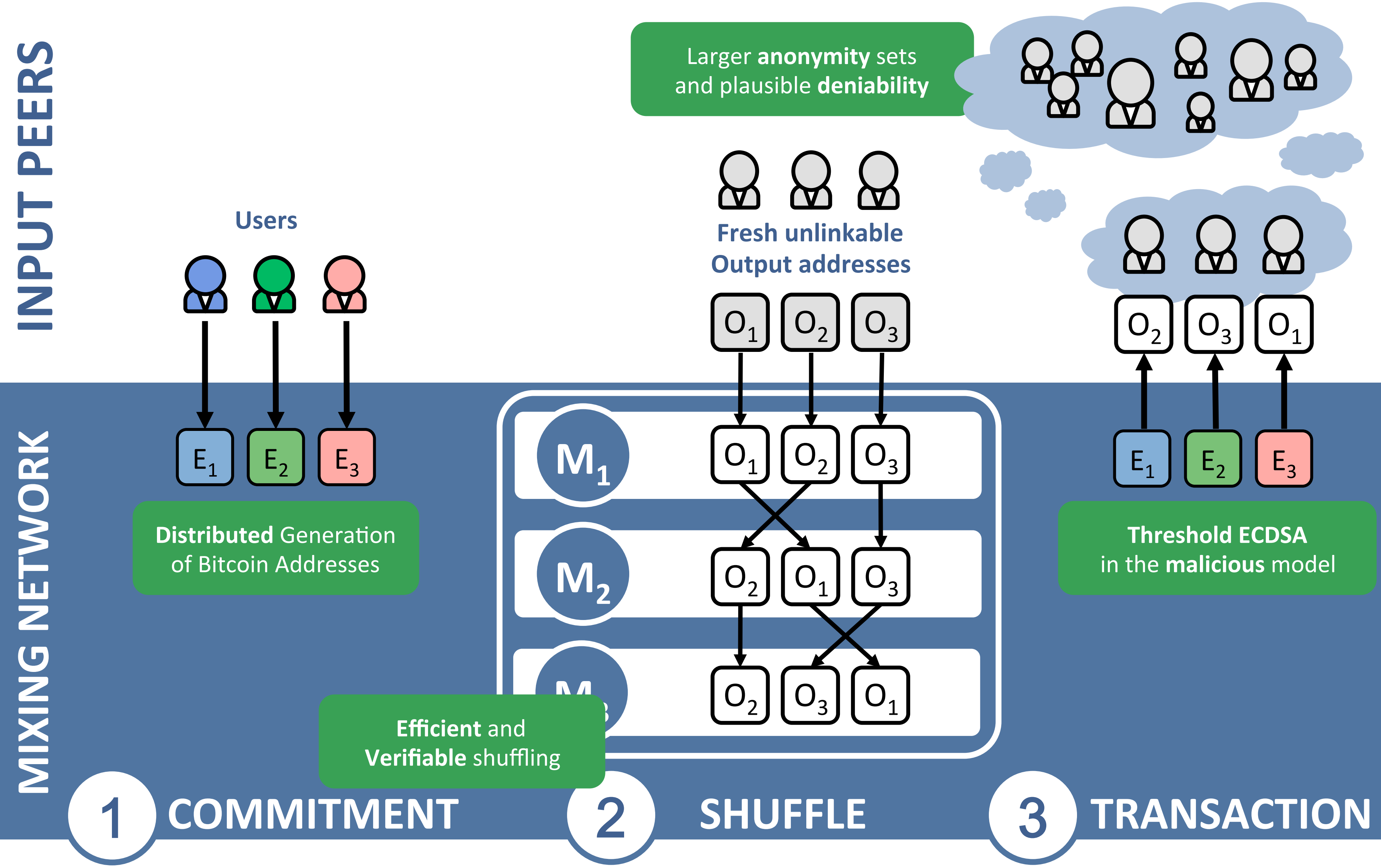
🟧🟩 **Deniability**

🟩 Scalability

🟩 Costs

🟩 Usability

CoinParty Protocol Overview



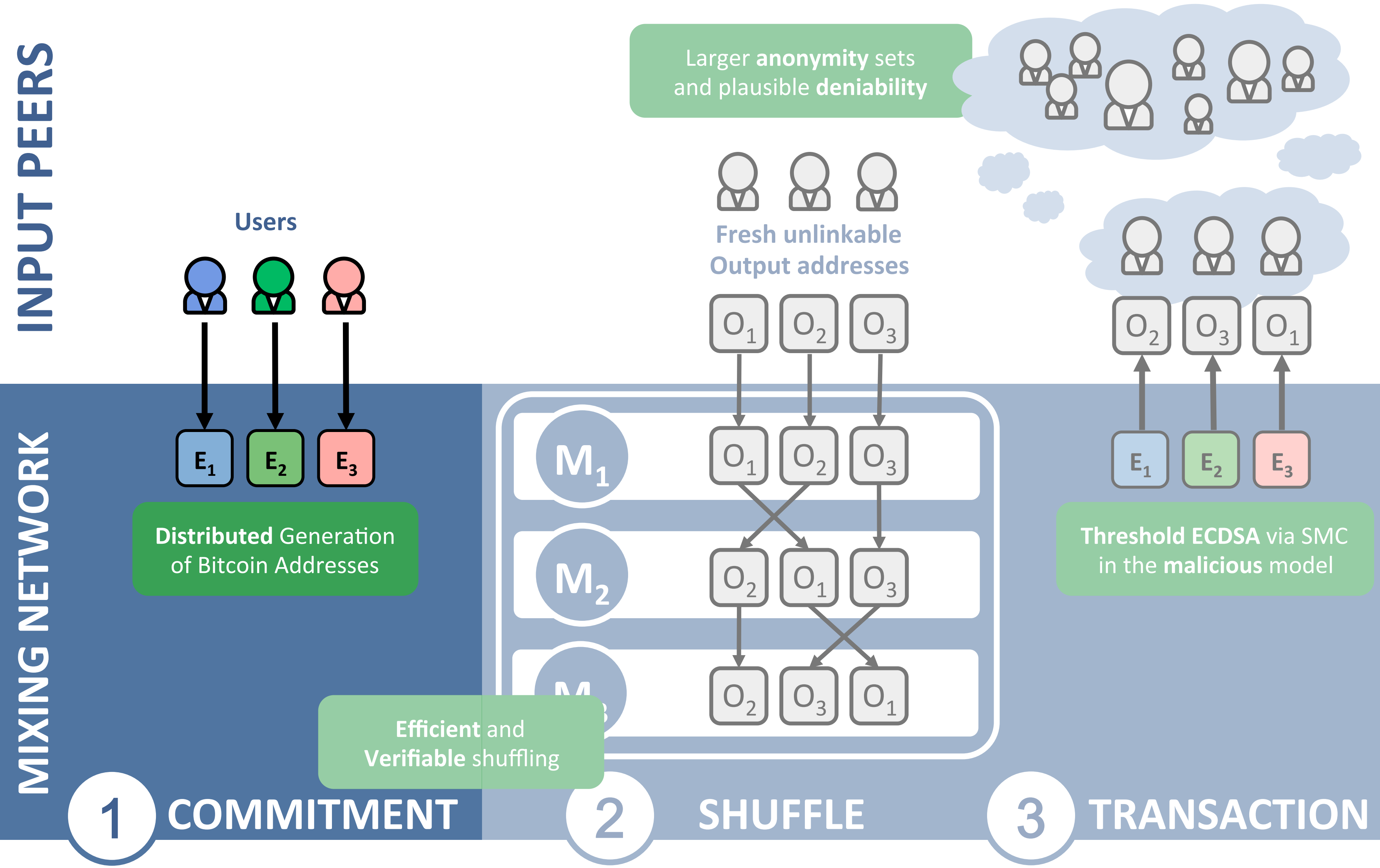
Larger **anonymity** sets and plausible **deniability**

Distributed Generation of Bitcoin Addresses

Efficient and **Verifiable** shuffling

Threshold ECDSA in the **malicious** model

CoinParty Protocol Overview



Larger **anonymity** sets and plausible **deniability**

Distributed Generation of Bitcoin Addresses

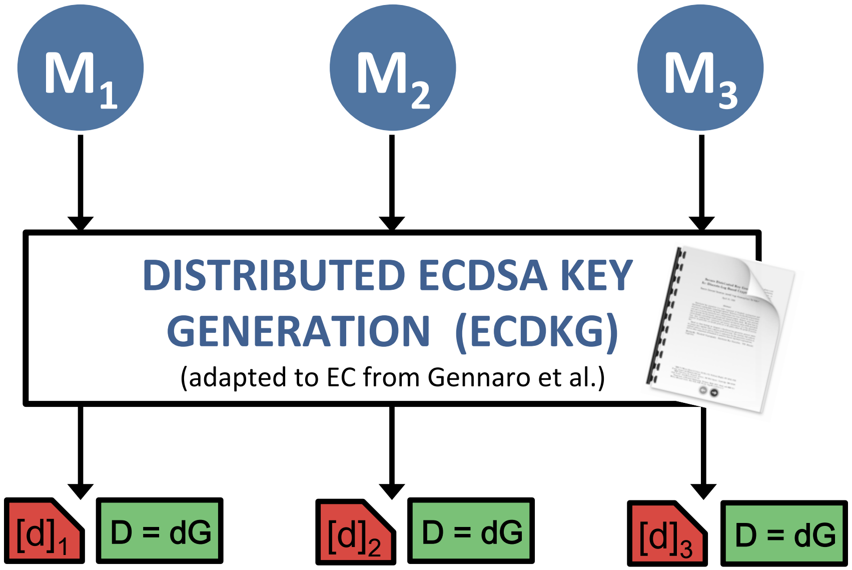
Efficient and **Verifiable** shuffling

Threshold ECDSA via SMC in the **malicious** model

Commitment Phase

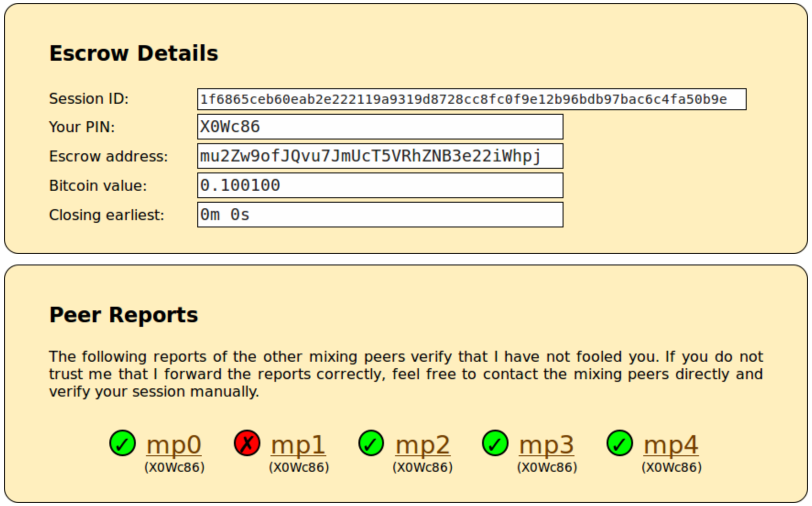
Goal 1: Shared control addresses

- Gennaro et al. adapted to EC
  - Shared private key d = Recombine($[d]_1$,$[d]_2$,$[d]_3$)
  - Full public key D = dG
- *Indistinguishable* from normal Bitcoin address
- Precompute ~ 80 % of overhead


M_1
M_2
M_3
DISTRIBUTED ECDSA KEY GENERATION (ECDKG)
(adapted to EC from Gennaro et al.)
$[d]_1$
D = dG
$[d]_2$
D = dG
$[d]_3$
D = dG

Goal 2: Receive commitments

- Mixing peers provide web interface
- User checks mixing parameters
- User commits funds in standard transaction



Escrow Details

Session ID:	1f6865ceb60eab2e222119a9319d8728cc8fc0f9e12b96bdb97bac6c4fa50b9e
Your PIN:	X0Wc86
Escrow address:	mu2Zw9ofJQvu7JmUcT5VRhZNB3e22iWhpj
Bitcoin value:	0.100100
Closing earliest:	0m 0s

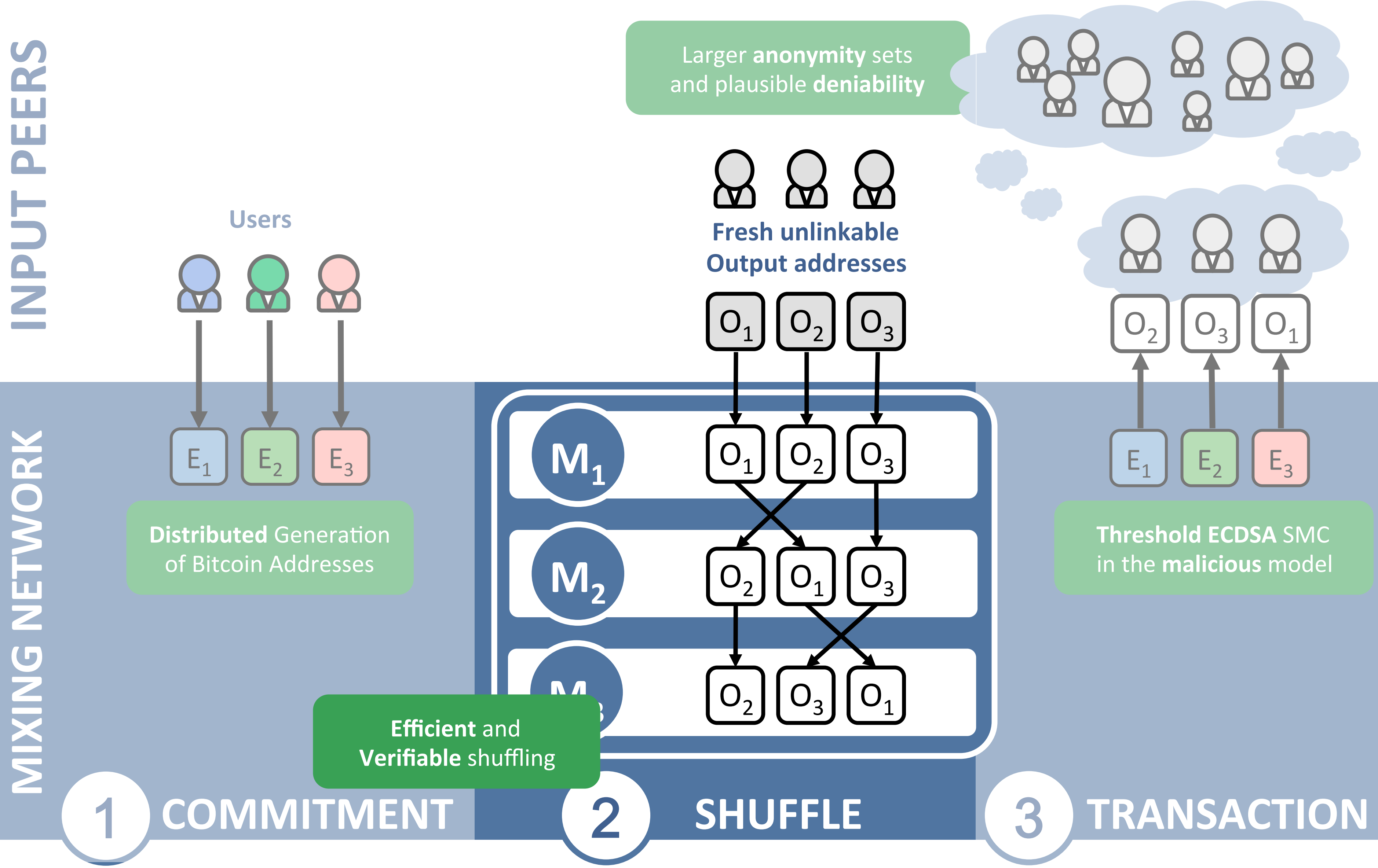
Peer Reports

The following reports of the other mixing peers verify that I have not fooled you. If you do not trust me that I forward the reports correctly, feel free to contact the mixing peers directly and verify your session manually.

✓ mp0 (X0Wc86) ✗ mp1 (X0Wc86) ✓ mp2 (X0Wc86) ✓ mp3 (X0Wc86) ✓ mp4 (X0Wc86)

Gennaro, Rosario, et al. "Secure distributed key generation for discrete-log based cryptosystems." EUROCRYPT'99. Springer, 1999.

CoinParty Protocol Overview



Larger **anonymity** sets and plausible **deniability**

Fresh unlinkable Output addresses

Distributed Generation of Bitcoin Addresses

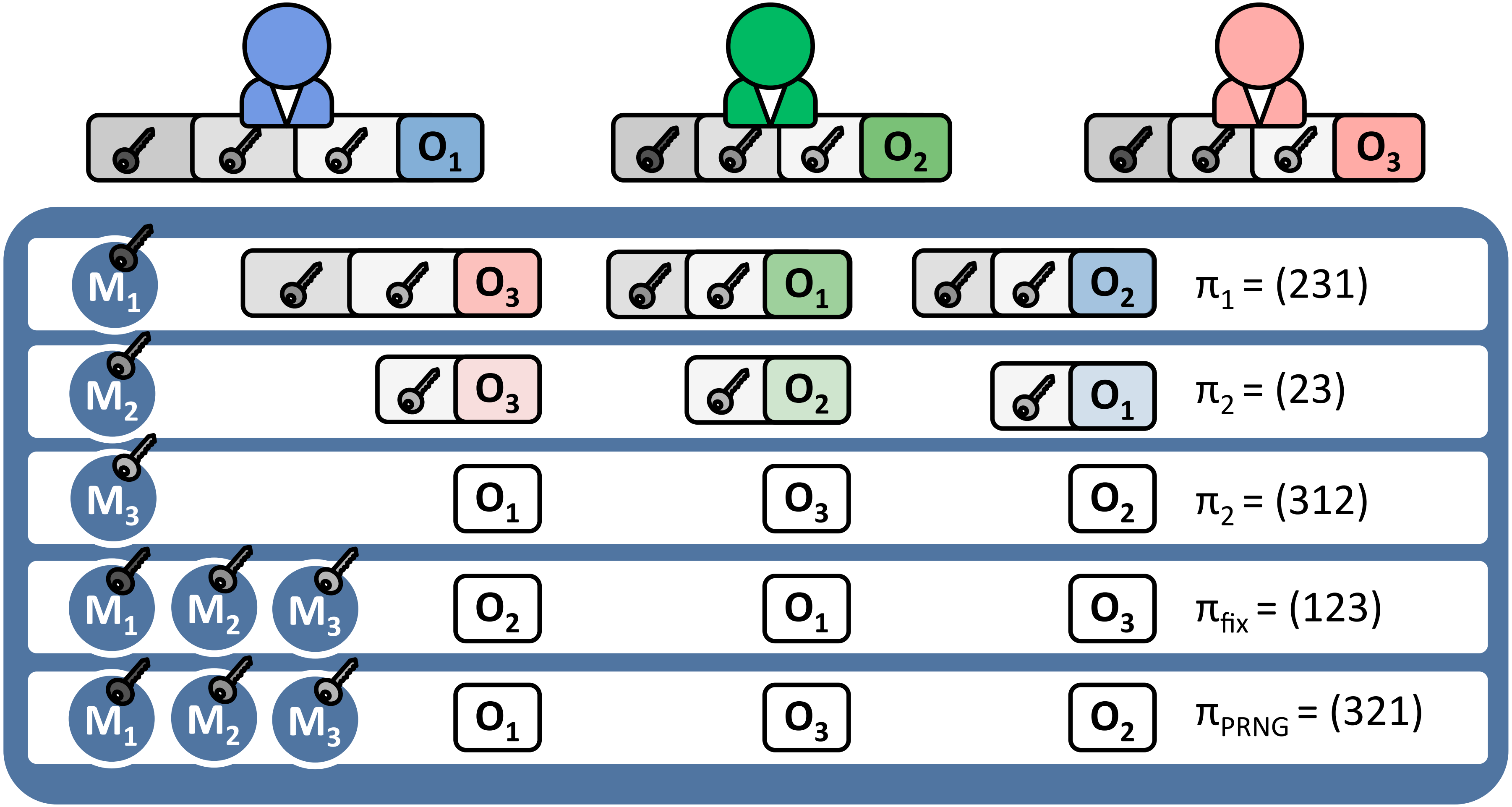
Efficient and **Verifiable** shuffling

Threshold ECDSA SMC in the **malicious** model

Shuffle Phase

Goal: Unlink users from supplied addresses. Shuffle addresses.

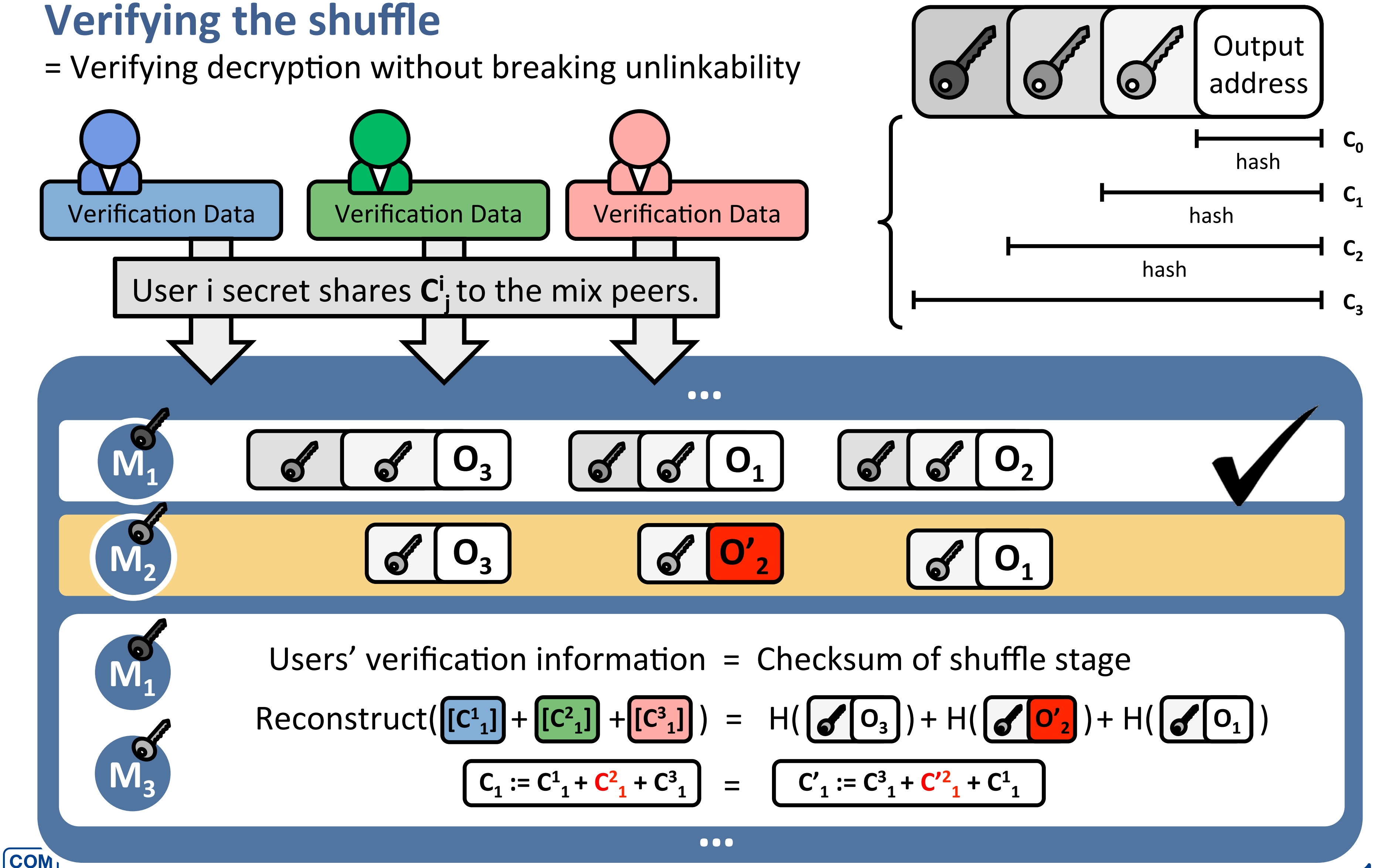
Solution: Verifiable shuffle



Shuffle Phase (cont'd)

Verifying the shuffle

= Verifying decryption without breaking unlinkability



User i secret shares C^i_j to the mix peers.

Users' verification information = Checksum of shuffle stage

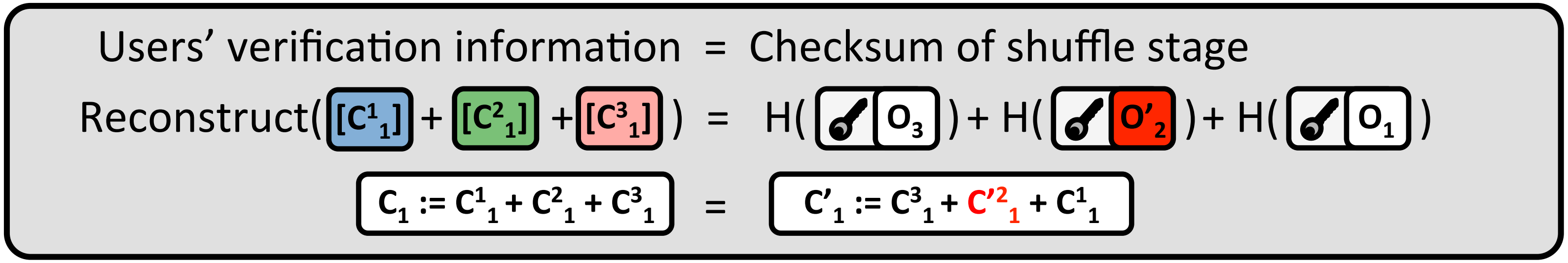
$$\text{Reconstruct}([C^1_1] + [C^2_1] + [C^3_1]) = H(O_3) + H(O'_2) + H(O_1)$$

$$C_1 := C^1_1 + C^2_1 + C^3_1 = C'_1 := C^3_1 + C'^2_1 + C^1_1$$

Shuffling Phase (cont’d)

Handling malicious behavior

Case 1: Mix M_2 did not decrypt correctly



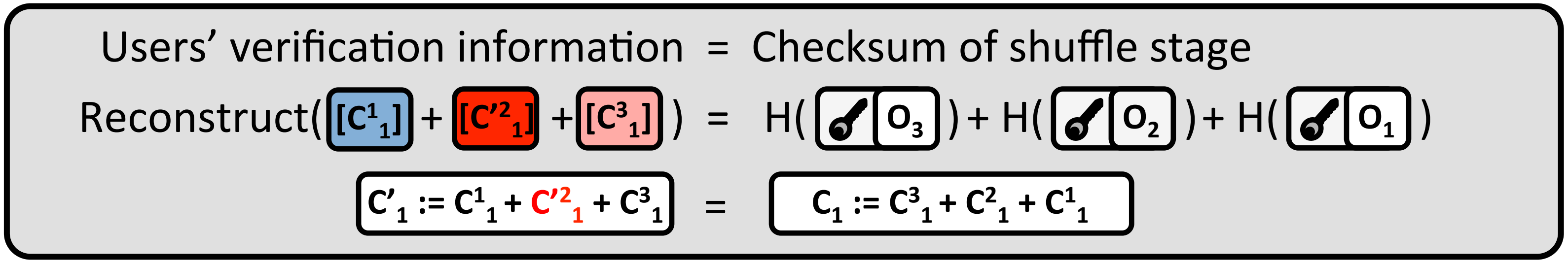
Users’ verification information = Checksum of shuffle stage

Reconstruct($[C^1_1]$ + $[C^2_1]$ + $[C^3_1]$) = H(🔑 O_3) + H(🔑 O'_2) + H(🔑 O_1)

$C_1 := C^1_1 + C^2_1 + C^3_1$ = $C'_1 := C^3_1 + C'^2_1 + C^1_1$

- Reconstruct M_2’s private key and check decryption
- Skip and punish dishonest mix M_2

Case 2: Users supplied inconsistent verification information



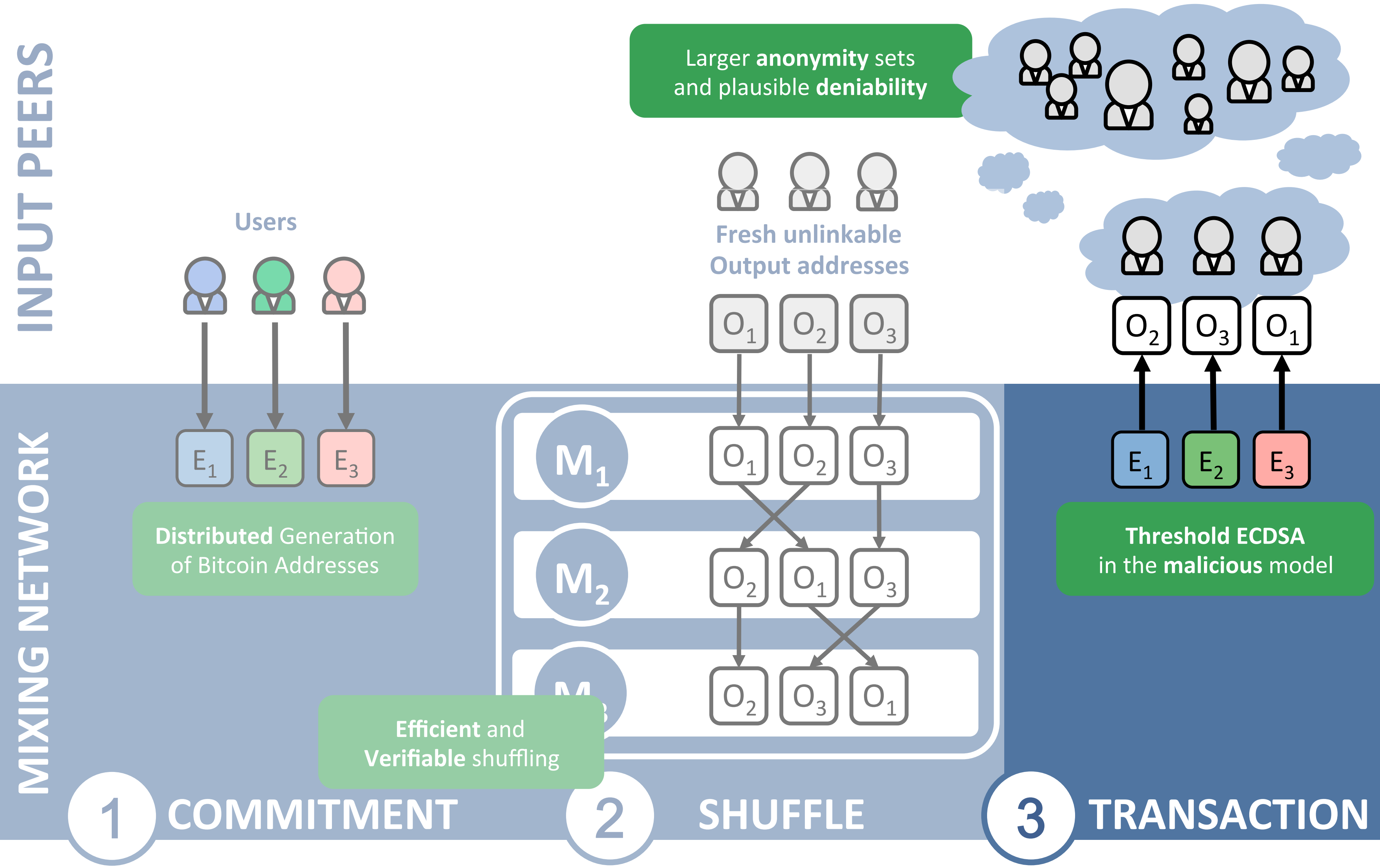
Users’ verification information = Checksum of shuffle stage

Reconstruct($[C^1_1]$ + $[C'^2_1]$ + $[C^3_1]$) = H(🔑 O_3) + H(🔑 O_2) + H(🔑 O_1)

$C'_1 := C^1_1 + C'^2_1 + C^3_1$ = $C_1 := C^3_1 + C^2_1 + C^1_1$

- Reconstruct all checksums C^j_1 on shuffle stage
- Identify and punish all misbehaving users *j*
- Need to abort shuffle

CoinParty Protocol Overview



Larger **anonymity** sets
and plausible **deniability**

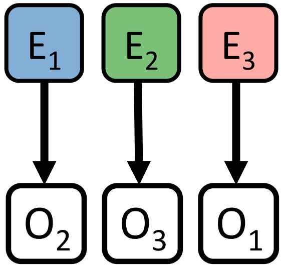
Distributed Generation
of Bitcoin Addresses

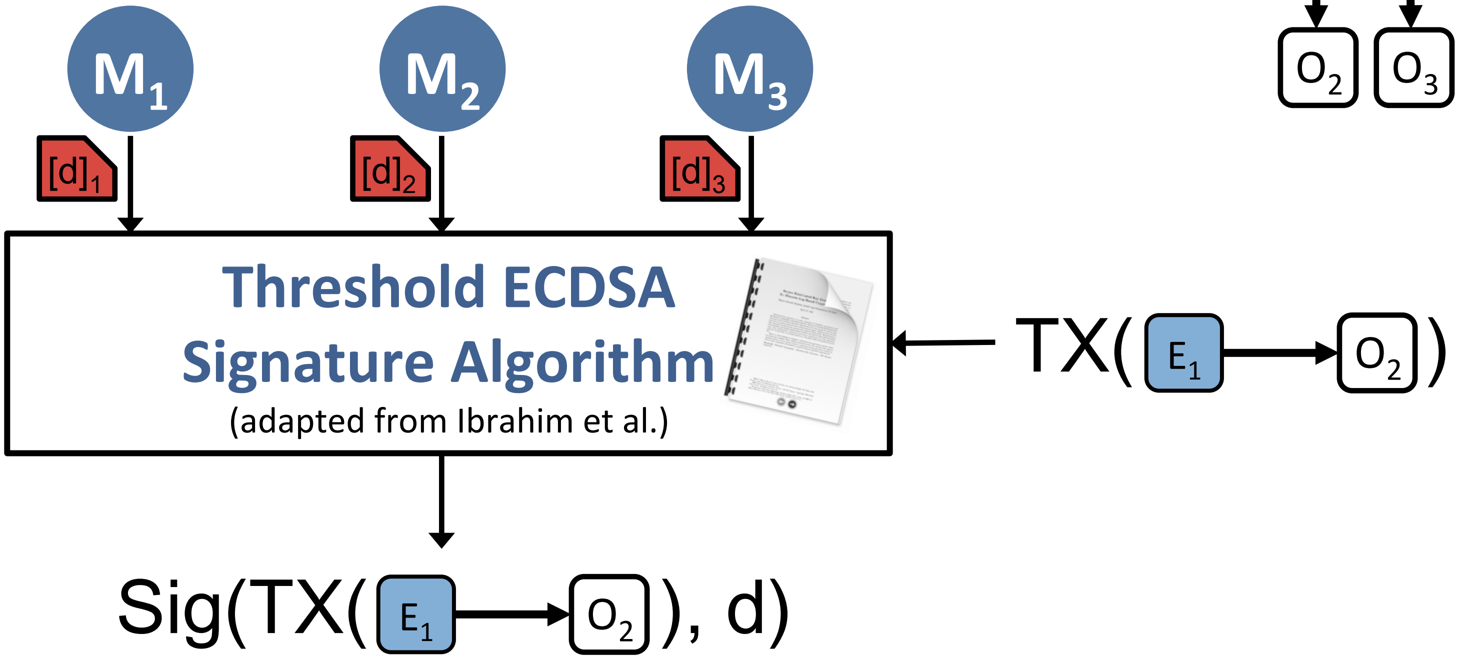
Efficient and
Verifiable shuffling

Threshold ECDSA
in the **malicious** model

Transaction Phase

GOAL: Sign transaction from a shared Bitcoin address





Threshold ECDSA Signature Algorithm

(adapted from Ibrahim et al.)

$TX(E_1 \rightarrow O_2)$

$Sig(TX(E_1 \rightarrow O_2), d)$

- Precompute ~ 75 % of overhead
- Threshold transactions are **indistinguishable** from normal Bitcoin transactions

Ibrahim, Maged H., et al. "A robust threshold elliptic curve digital signature providing a new verifiable secret sharing scheme." Circuits and Systems, IEEE, 2003.

Reminder

Requirements for an ideal mixing service

SECURITY
No theft, double spending or loss of funds.
No DoS.

ANONYMITY
Anonymous against in- and outsiders.
Big anonymity sets.
Unbiased randomness.

DENIABILITY
Means of plausible deniability.
No cryptographic evidence.

[**MISUSE PREVENTION**
Prevent money-laundering, …]

SCALABILITY
Large numbers of users.
Low impact on Bitcoin network.

COST EFFICIENCY
No mixing fees.
Minimal transaction fees.

APPLICABILITY & USABILITY
Compatible with Bitcoin network.
No additional software.

Discussion: Security

Proof Sketch

- Use secure primitives: Secret sharing, ECDKG, TECDSA
  - Security of Commitment and Transaction phase follows directly
- Shuffle stage
  - Malicious behavior is detected
  - Skip malicious mixes ☺
  - Malicious users can DoS ☹
  - But we can punish them effectively 😐

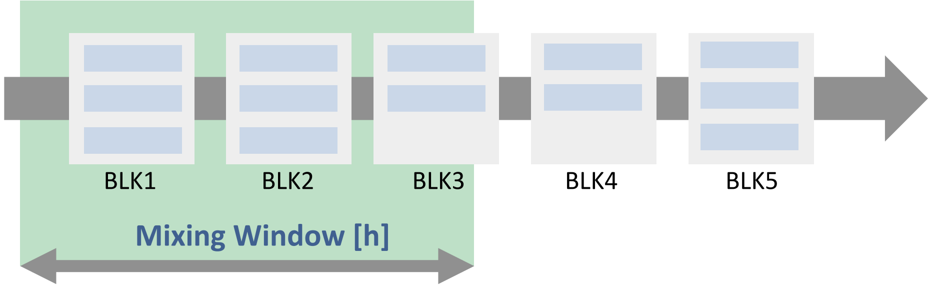
Security Thresholds

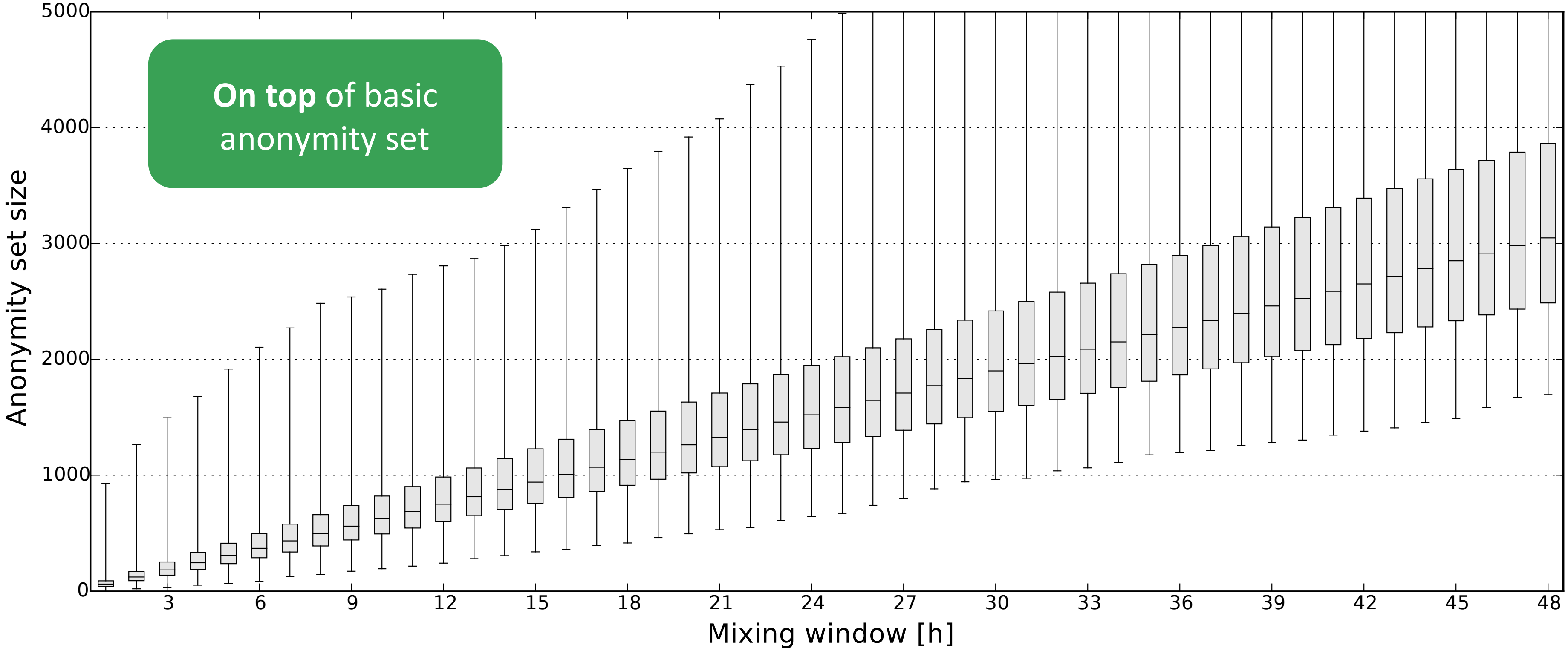
- Secret Sharing, ECDKG, TECDSA are essentially MPC problems
  - Need *guaranteed output*
  - Don’t have *broadcast channel*
- ***m/3 malicious mixes*** is theoretic upper bound
- Any number of malicious users

Discussion: Anonymity

Anonymity against

- **Mixing peers:** # of users
- **Other users:** # of users - # of sybils
- **Passive observers:** Analyze blockchain





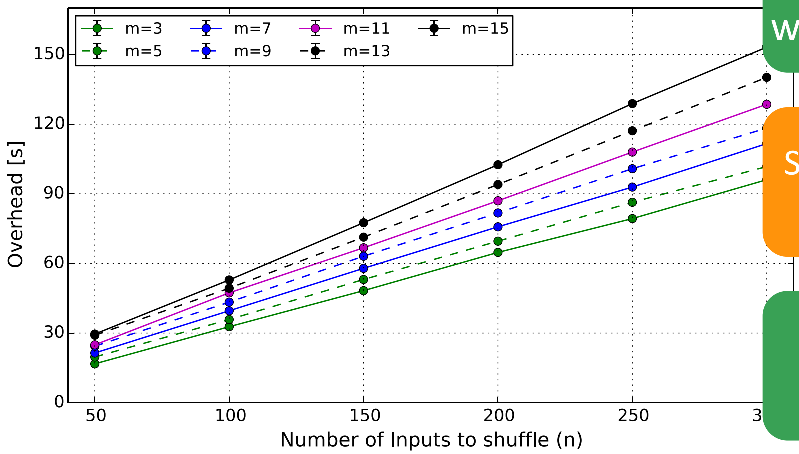
On top of basic anonymity set

Discussion: Scalability

MIXING OVERHEAD in CLOUD SETTING

Hosts
Azure Cloud A1 Instances
1 virtual core, 1.75 GB RAM

Network
US and EU Locations
50 - 100 ms intracontinental
150 -200 ms intercontinental



< 3 minutes
with 15 Mixing Peers

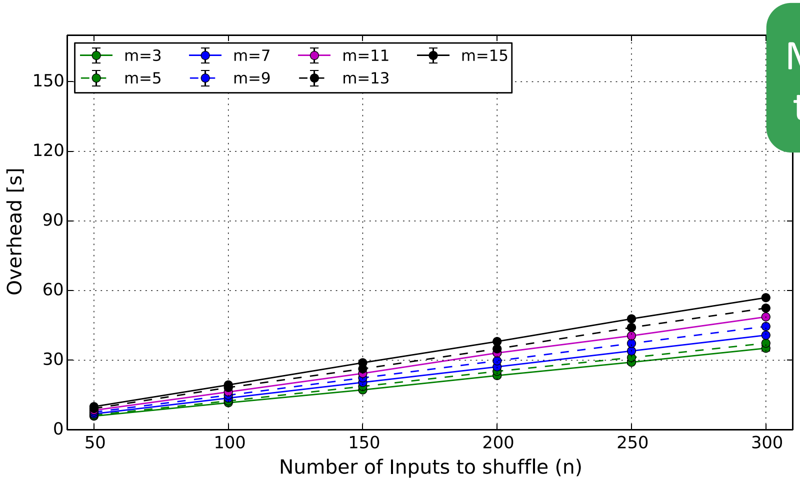
Scales with number of **inputs** and **MPs**

Approx. **75 %** can be precomputed

MIXING OVERHEAD in LAN SETTING

Host
16 CPUs / 32 Threads
32 GB RAM

Network
Gigabit LAN



Most overhead due to **communication**

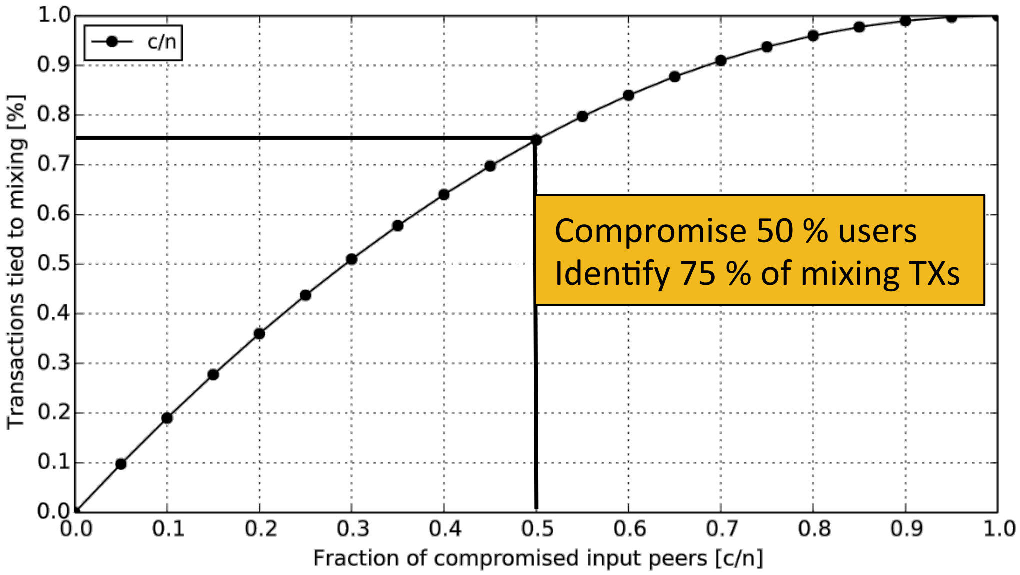
Discussion: Deniability

Deniability against …

- **Passive observers:** Full – Mixing TXs are indistinguishable from normal TXs
- **Mixing peers:** None – MPs can identify their own mixing transactions
- **Other users:** Reduced – Sybil attacks threaten deniability

Malicious users

$$p = 1 - (1 - c / n)^2$$



Compromise 50 % users
Identify 75 % of mixing TXs

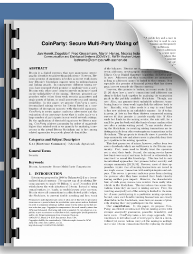
Conclusion

OUR APPROACH

Mixing in single transactions using Threshold ECDSA.
Refined shuffling for deniability.

COIN PARTY

Security	Against 1/3 malicious adversary
Privacy	Orders of magnitude more anon.
Deniability	With some restrictions
Scalability	100s – 1000s of users
Costs	No mixing fees. No TX fees.
Applicability	Fully standard Bitcoin TXs



CoinParty: Secure Multi-Party Mixing of

Jan Henrik Ziegeldorf, Fred Grossmann, Martin Henze, Nicolas Inda
Communication and Distributed Systems (COMSYS), RWTH Aachen Univer
lastname@comsys.rwth-aachen.de

ABSTRACT

Categories and Subject Descriptors

General Terms

Keywords

1. INTRODUCTION

FUTURE WORK

Applications

PREVENTING MISUSE

Deniability