CoinShuffle anonymity in the Block chain

Jan-Willem Selij

July 2, 2015

Outline

Bitcoin 101

- A decentralized digital crypto-currency
- Transactions
- Blocks
- Block chain

Transaction: Example

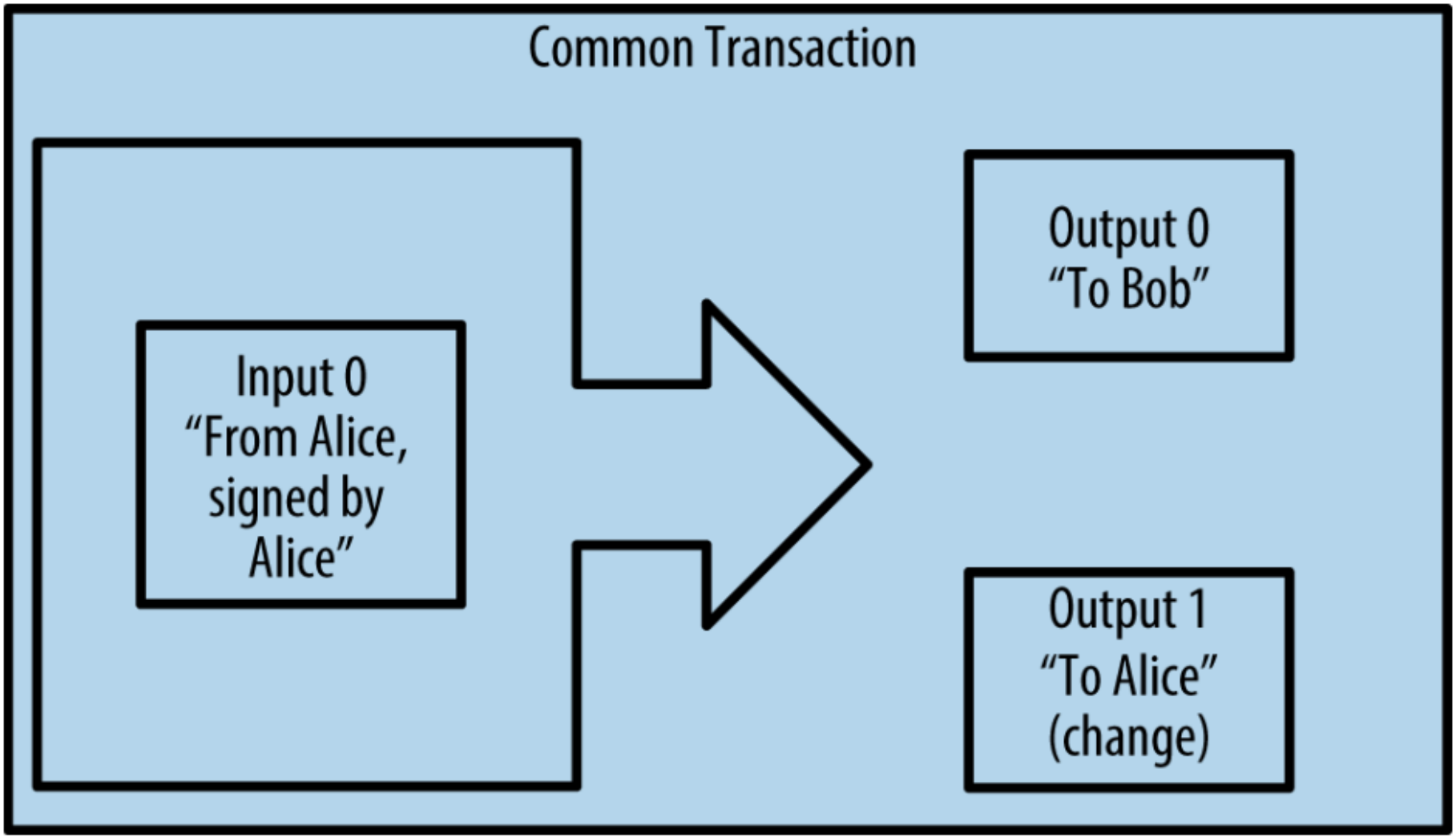


Figure: Bitcoin Transaction [2]

Block chain

- Public ledger
- Consists of every transaction ever
- Addresses may look cryptic but are pseudonymous.
- Transactions can be traced back to their very first origin: a mining reward

Importance of interchangeable Bitcoins

- *Taint* shows Bitcoin addresses used in the past leading to a transaction. Possibly indicating source.
- Effectively the likeliness of a "connection" between a transaction and address
- Bitcoins can be discriminated this way
- Prone to attackers that monitor address belonging to people
- Various organizations or individuals like to stay anonymous
- What we want: *unlink* input and output address

Mixing Service

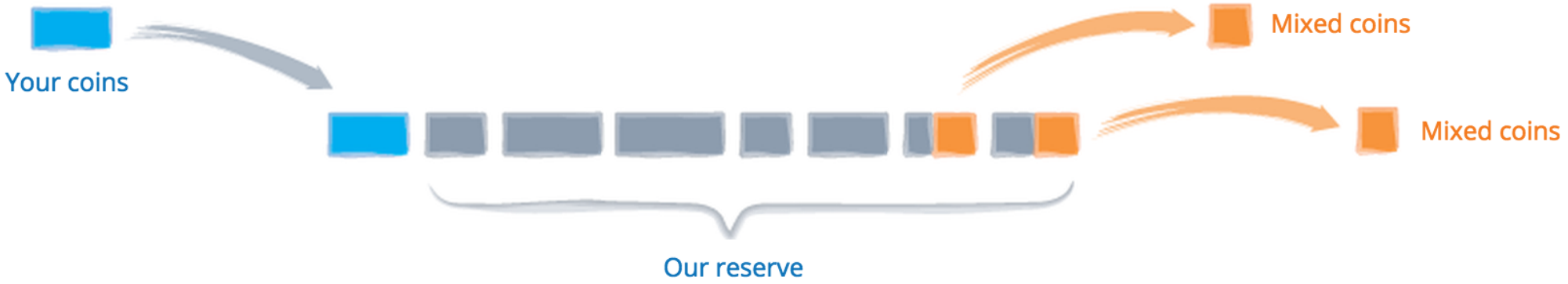


Figure: Mixer Example Service [3]

Related Work

- BitIodine / CoinSeer [9] [10]
- Mixed results with mixers [7]
- Zerocoin / Zerocash [5] [4]
- MixCoin / CoinJoin [6] [8]

CoinShuffle

- Does not require a central server to store funds on
- Participants do not learn each other's addresses
- Single transaction fee

Research Questions

- Can a CoinShuffle-transaction as such be detected in the block chain?

Sub questions

- In which situations is it possible to detect the transaction, and what information can be derived from this?
- If this is the case, what can be done to improve the anonymity?

Outline

CoinShuffle: Transaction Verification

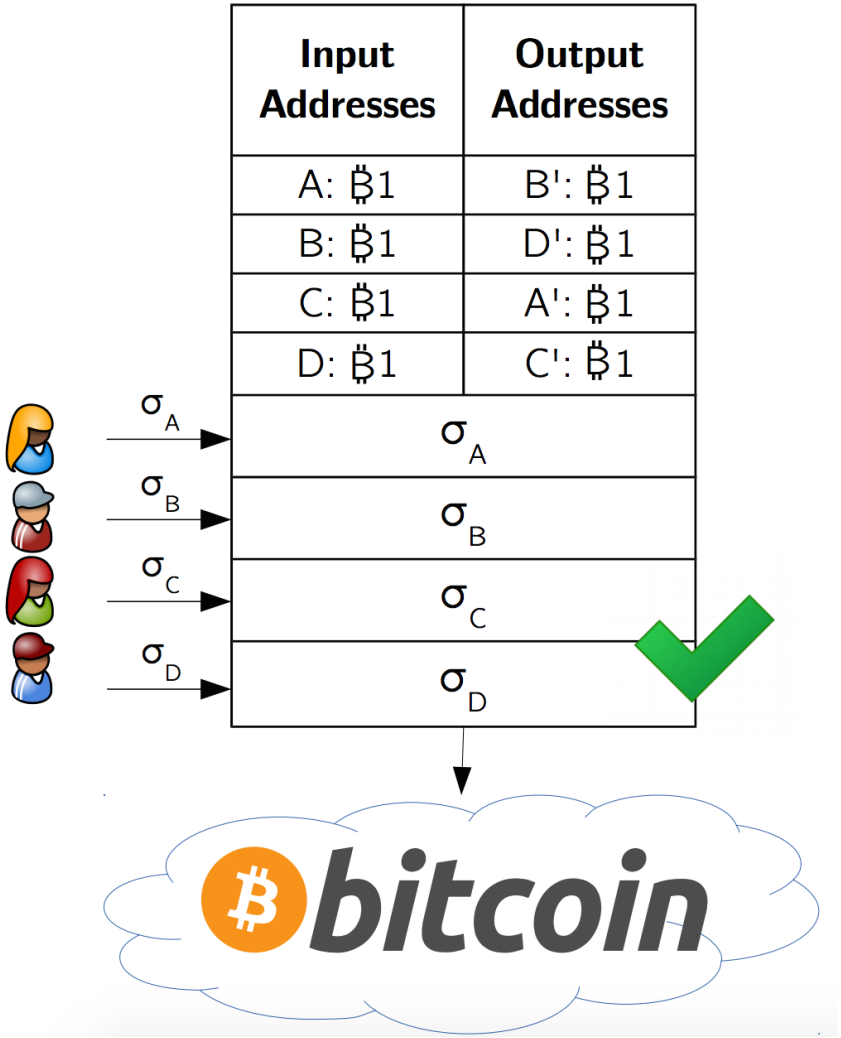


Figure: Transaction Verification [1]

Outline

CoinShuffle Test Setup

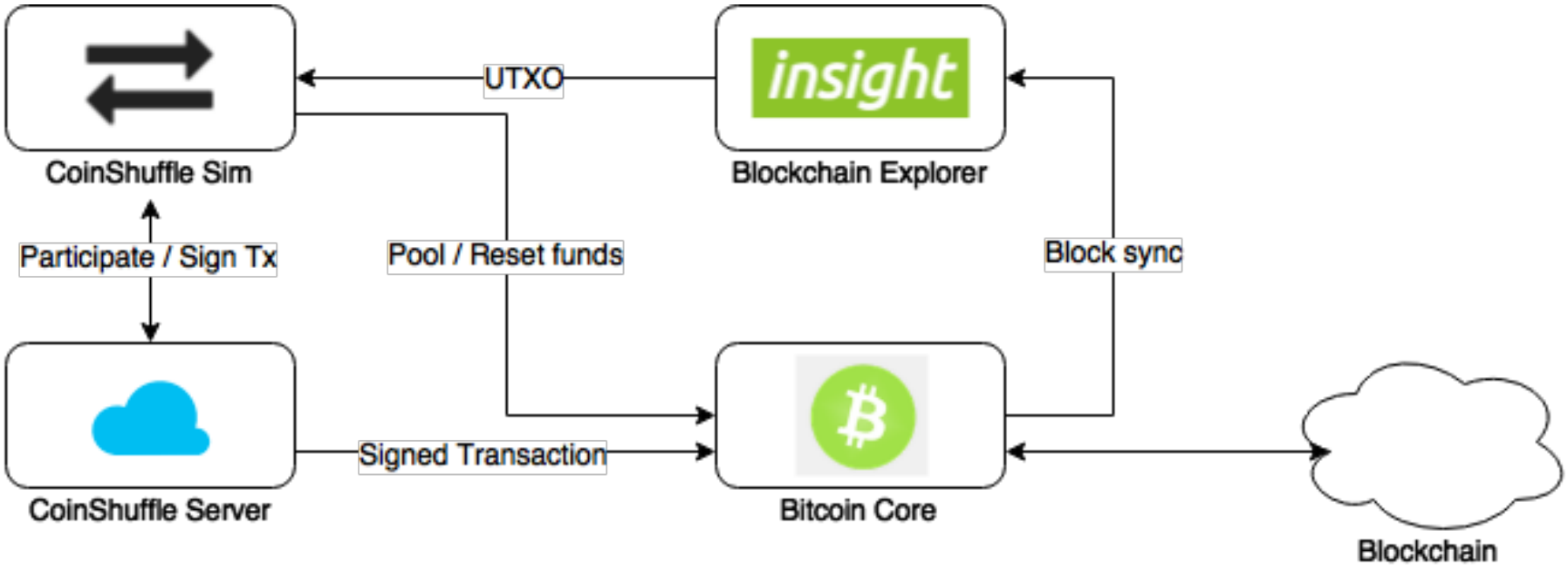


Figure: CoinShuffle Test setup

CoinShuffle Transaction

From (amount)	To (amount)
Generation: 0.00004768 + 0.0001 total fees	mjkyzZJZMWKUahJqVCgAEfphjwiH21JEHD: 0.00014768
mtUhedGBQ2txSYbH5ZTktdyyi8816m2UM3: 1.6 mu75neruhq29tDS8SZhNg5jkK7ZQpt8phi: 1.1 n4gKvUQFSY58oFJxY2zcKQpS45B7WPLmHt: 2.1 mpHvfkpNc9cTL6oytRCuCRKwjb4giBVreo: 1.23 mzRjMNjesdB6HyjpYkVYy81FnvSoTvjcJ9: 1.4 mvbVJ5he6hs4dsUcc1MnWkPMGttgV8ppNY: 1.5 mp3ubgiJaAUAAddb54QArDuBKgeX829RNN: 1.7 mqotCTdWDGocKk3q4PgG4NjJdFp3Z4q5rp: 1.3 mx71vJ2Jn7tSLetwpf4T4veqU9qDbziuUj: 1 morMCuQ6sMVPS8enxCRnTidaebhPz1Nftv: 1.45	n1Te8fxTxyZtWi7Y8QeCCHEHLjPFpriZPn: 1 muQk3uAak7d3FLKSVL7yoGDzV1YtQg2oqS: 1 msDtXzyP8eAGWSMbyTT35yByodUNf1Zpg4: 1 mfhaGJVjYGTBw81HtoLQMws9gCn5sknrWz: 1 mh2nsd6qeZqCimtcDjX5TihGSHPA7s8AwW: 1 mvZXkjFD556r5fNUuwFFsPXjKwSe8JVBGd: 1 mwZPzLSjRxHbhWGDiXvoF8BgyEJZXjooki: 1 mzHXgphR655SMgio8oPDkQNJuLq7W1KnZH: 1 mqjCTNuKUcJYBzCQ8hHMiPPmK2dmV1vWjH: 1 mjSAtRMtMnMAsz81t4Ra8nmbktEkn95iLK: 1 mx88pbGvfSVwGJUiax7jwjobmrdT48VZ7n: 0.5999 mgqPTUzfKPbS4HzZCbGadphRhN3KtATPmY: 0.1 mxL1tLNf9EtJakoDkVThveTjQa3Kr3TNHH: 1.1 n2RTBztTGww6skrTBAsxMj51WWfeu4MDR7: 0.23 mvHyGRLooD4BovvEKZD6SsaWk5f3B4TWQA: 0.4 mwhYwJKYMakvfDMA6MxKSypiEtDwBs2Bq3: 0.5 mh6PBAsgxbyXbnppZ23wT4zCWWSLouVMHV: 0.7 muZ383LAK4FuGQosYyuGFTMfDcP5XeZGNv: 0.3 mwLb53ztz8b4VRLs1T8eRt11bjZzc6N6H2: 0 mqDYLYzUSBjKvw2brqEpS3GHsMDrtc7kuX: 0.45

1 2 3 4

Figure: CoinShuffle Transaction

Analysis

- Script checks transactions on recognition points
- Positive results on test network
- Working on scanning the live Bitcoin network

CoinShuffle transaction detection

```
[TX id: 478adb1678d38e0fe5ce406bef60a61a391b9c3555c321e79c1e41bccb4b8700] Possible CoinShuffle transaction
[TX id: 478adb1678d38e0fe5ce406bef60a61a391b9c3555c321e79c1e41bccb4b8700] Ins: 10 Outs: 20
[TX id: 478adb1678d38e0fe5ce406bef60a61a391b9c3555c321e79c1e41bccb4b8700] 10 occurrences of 100000000 BTC (1 BTC)
[TX id: 29041698fb9fa23b6b24ecb8337710d5e17d9fa845fb816d1d9c6011203d33f9] Possible CoinShuffle transaction
[TX id: 29041698fb9fa23b6b24ecb8337710d5e17d9fa845fb816d1d9c6011203d33f9] Ins: 5 Outs: 10
[TX id: 29041698fb9fa23b6b24ecb8337710d5e17d9fa845fb816d1d9c6011203d33f9] 5 occurrences of 100000000 BTC (1 BTC)
```

Figure: CoinShuffle Transaction Detection

Improvements

- Splitting over multiple hours/days not really possible
- Multiple addresses per participant increases detection complexity from outside

Summary

- CoinShuffle-transactions are visible in the Block chain
- Amount visible, change addresses can be linked to input
- Protocol can be improved by applying Mixer's techniques

- Future Work
  - Traverse Bitcoin livenet in search for transactions.
  - Make detection harder (protocol modifications)
  - CoinShuffle wallet

References I

Coinshuffle: Practical decentralized coin mixing for bitcoin, 2014.
http://esorics2014.pwr.wroc.pl/resources/abstracts/paper236.pdf.

Andreas M. Antonopoulos.
Mastering Bitcoin.
O'Reilly Media, 2014.

Bitmixer.
Bitmixer - how it works?, 2015.
https://bitmixer.io/how.html.

References II

Christina Garman Matthew Green Ian Miers Eran Tromer Eli Ben-Sasson, Alessandro Chiesa and Madars Virza.
http://zerocash-project.org/media/pdf/zerocash-oakland2014.pdf, 2014.
http://zerocash-project.org/media/pdf/zerocash-oakland2014.pdf,.

Matthew Green Ian Miers, Christina Garman and Aviel D. Rubin.
Zerocoin: Anonymous distributed e-cash from bitcoin, 2013.
http://isi.jhu.edu/~mgreen/ZerocoinOakland.pdf,.

Andrew Miller Jeremy Clark3 Joshua A. Kroll Joseph Bonneau, Arvind Narayanan and Edward W. Felten.
Mixcoin: Anonymity for bitcoin with accountable mixes, 2014.

References III

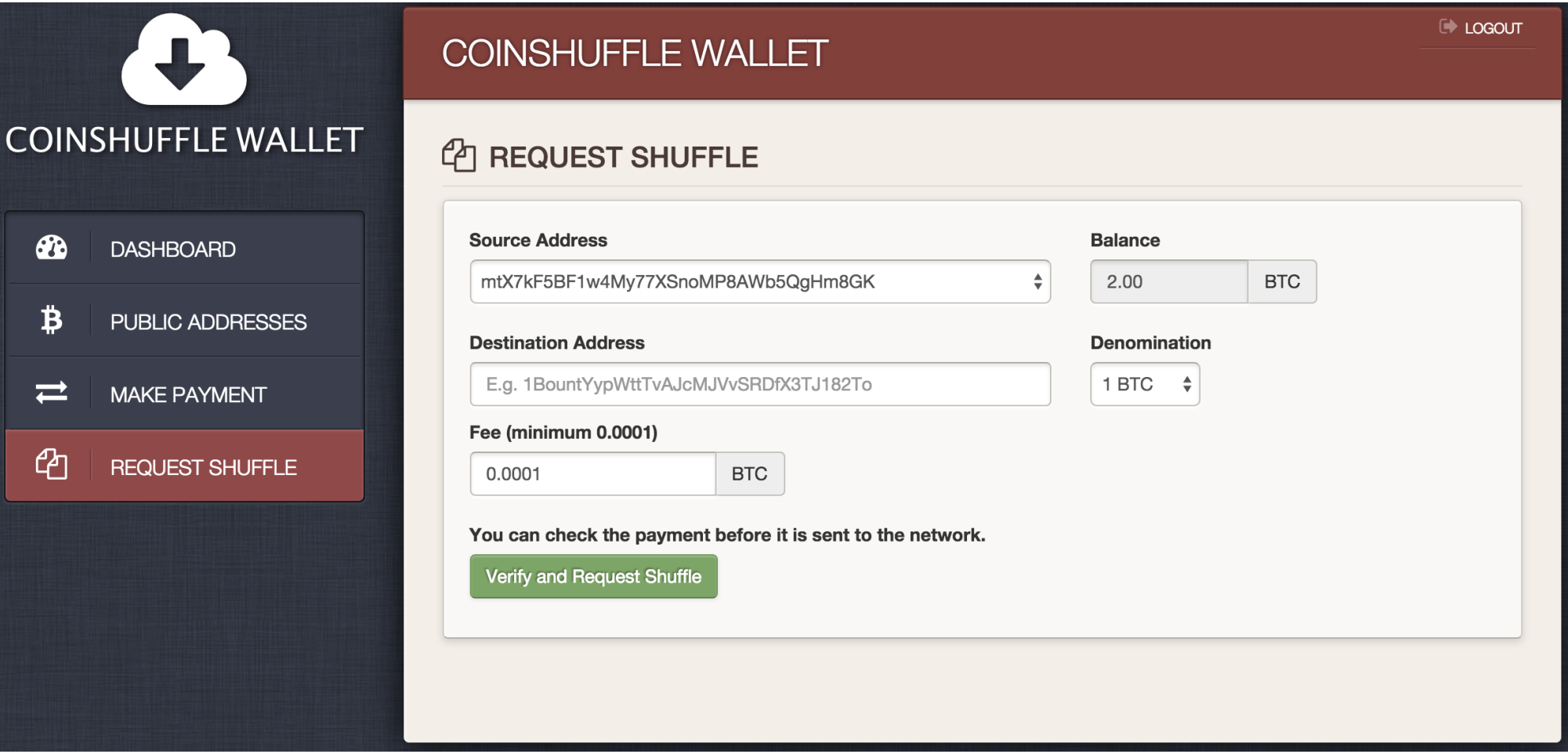
Rainer Bhme Malte Mser and Dominic Breuker.
An inquiry into money laundering tools in the bitcoin ecosystem, 2013.
https://maltemoeser.de/paper/money-laundering.pdf.

G. Maxwell.
Coinjoin: Bitcoin privacy for the real world, 2013.
https://bitcointalk.org/index.php?topic=279249.0.

Federico Maggi Michele Spagnuolo and Stefano Zanero.
Bitiodine: Extracting intelligence from the bitcoin network, 2014.
https://ifca.ai/fc14/papers/fc14_submission_11.pdf,.

Diana Koshy Philip Koshy and Patrick McDaniel.
An analysis of anonymity in bitcoin using p2p network traffic, 2014.
http://fc14.ifca.ai/papers/fc14_submission_71.pdf,.

CoinShuffle Wallet



Block chain

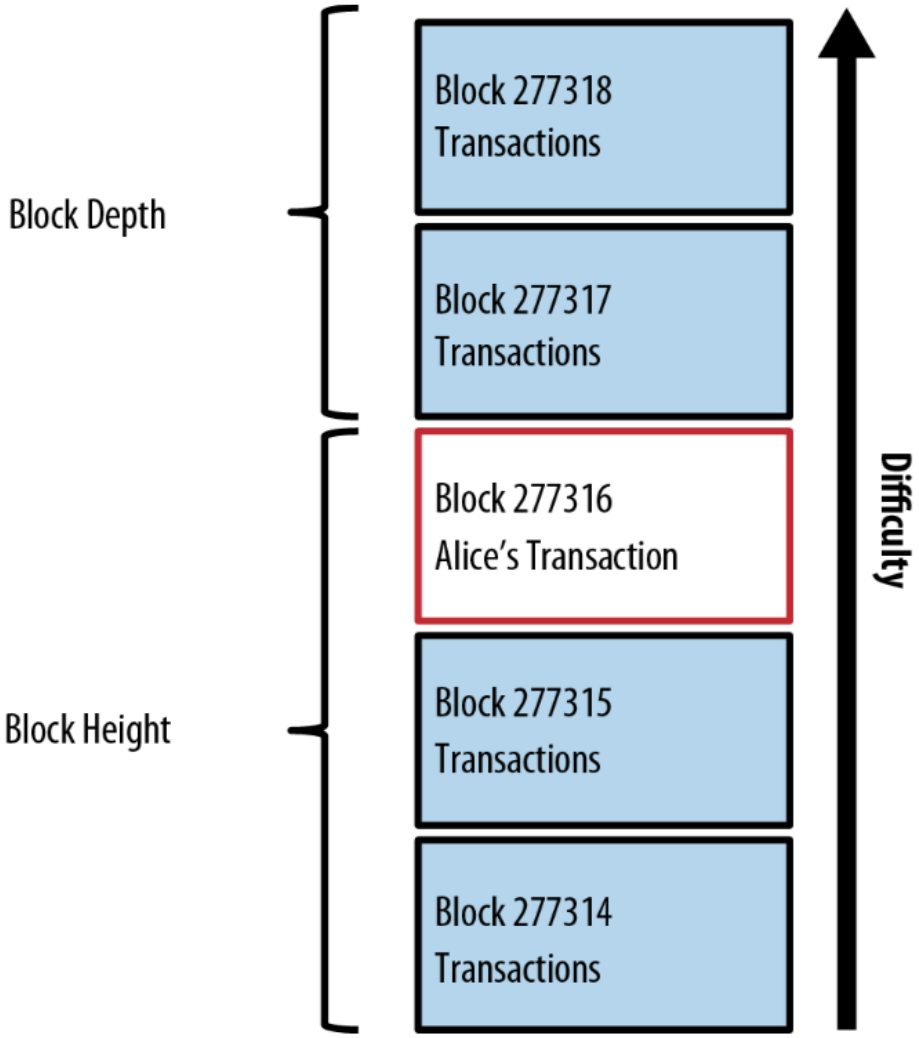


Figure: Bitcoin Block chain [2]

Mixing Service

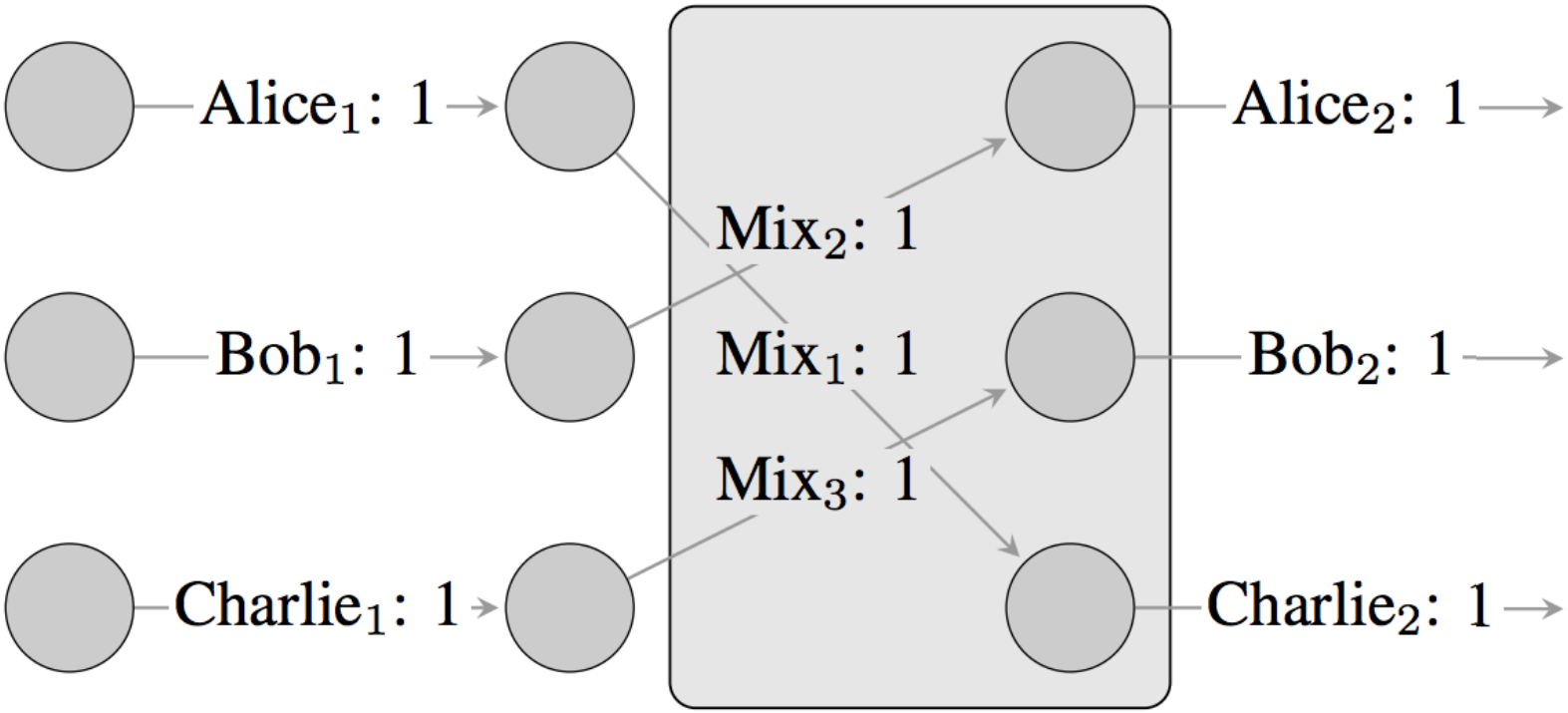


Figure: Hypothetical Mixing Service [7]

CoinShuffle: Announcement

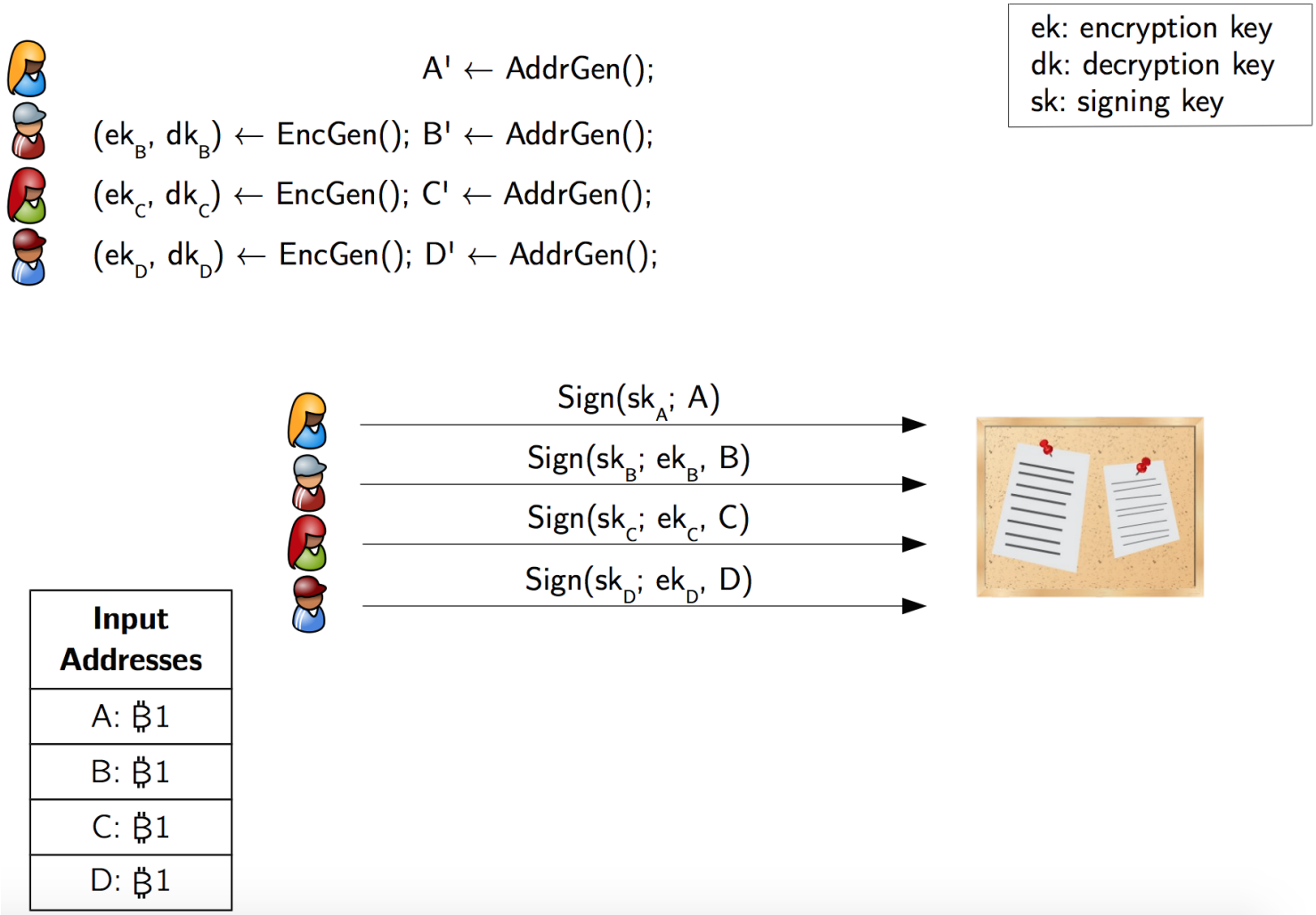


Figure: Announcement [1]

CoinShuffle: Shuffling

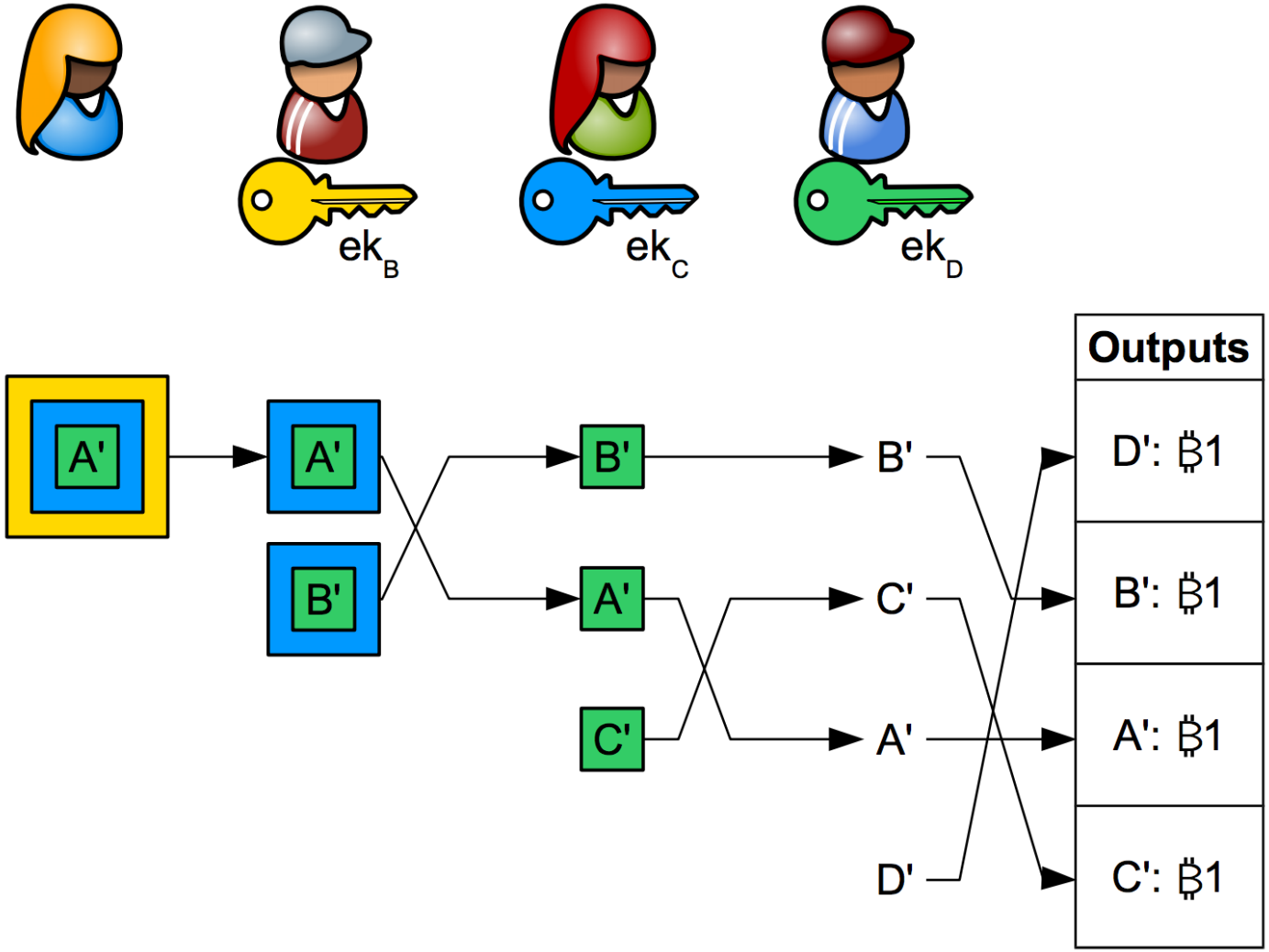


Figure: Shuffling [1]

CoinShuffle transaction detection

```
Possible CoinShuffle transaction
Ins:  10 Outs:  20
10 occurrences of 100000000 BTC (1 BTC)
```