



nes  fit

JANE – Deanononymizace transakcí

Vladimír Veselý
2019-09-09

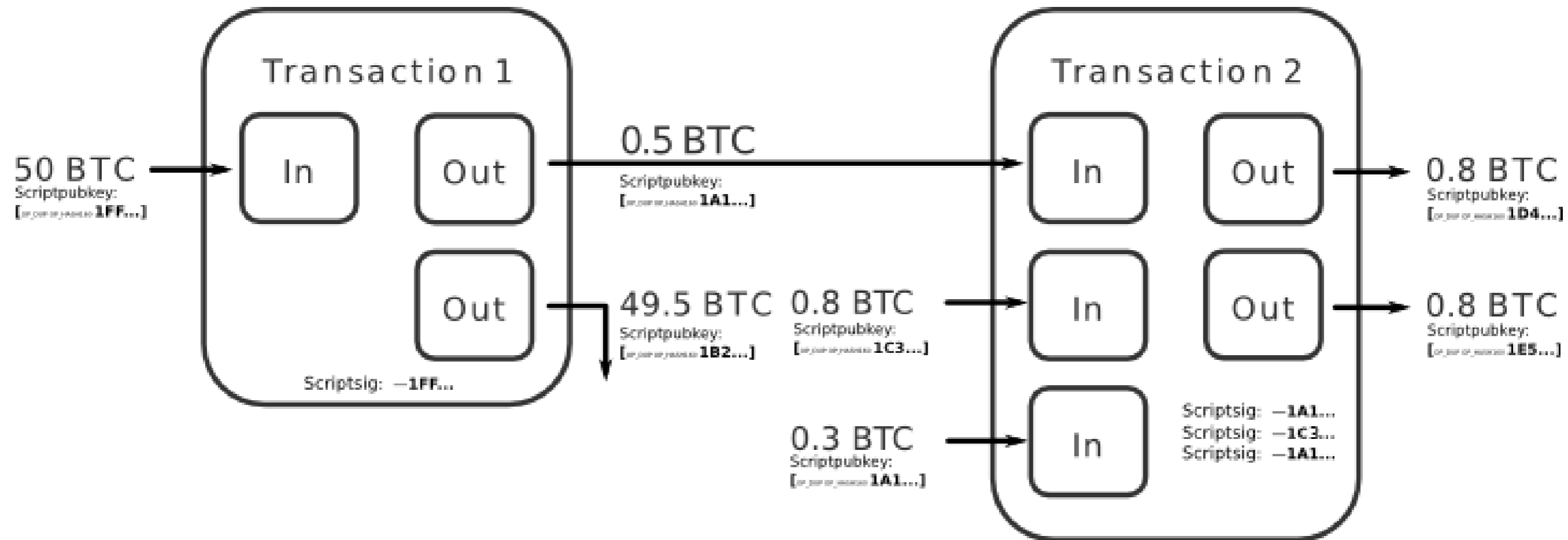


JANE



- *Tarzanova nejlepší kámoška*
- Platform as a Service
- Aktuální moduly
 - Kryptoalarm
 - Kryptoklienti
 - sMaSheD
 - MozArch
 - Lemmit
 - TOREATOR

Předmět

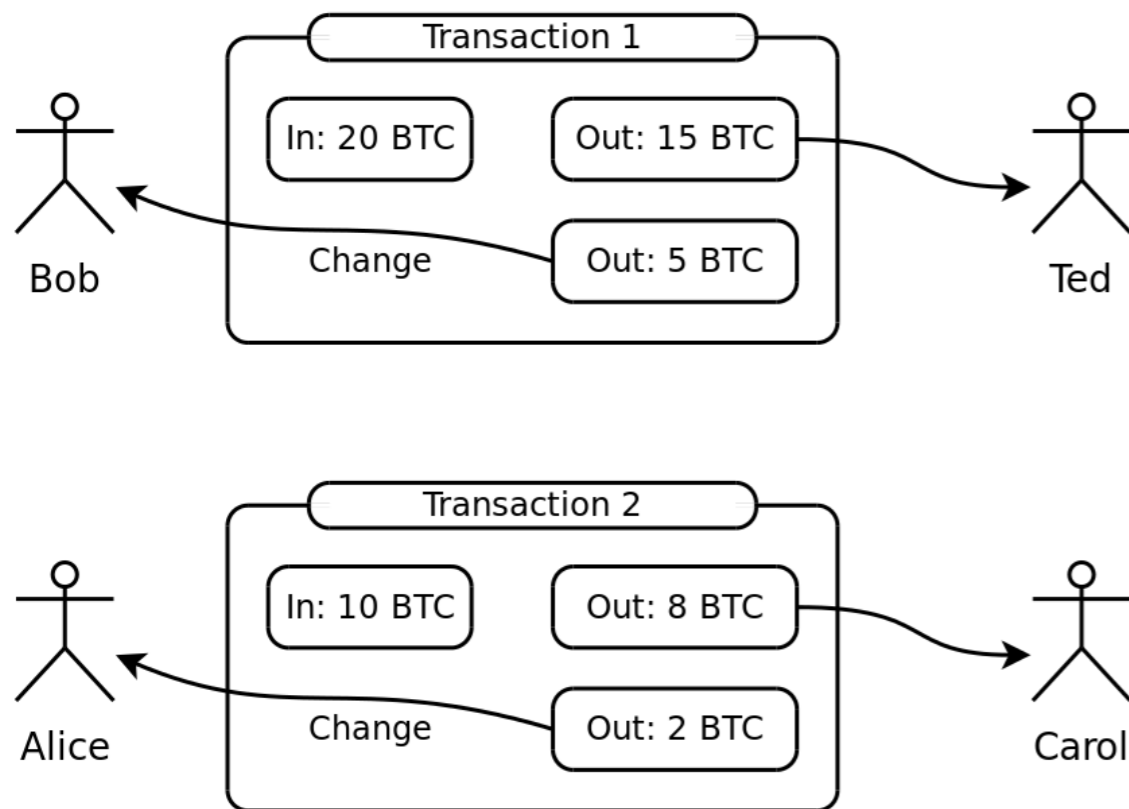


Metody obfuskuje

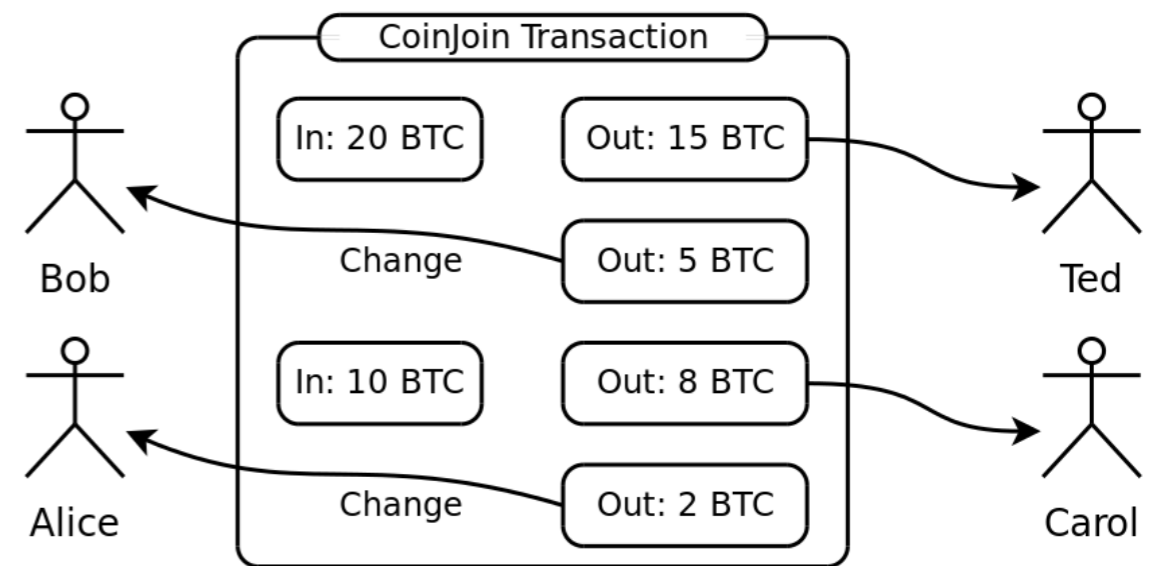


CoinJoining

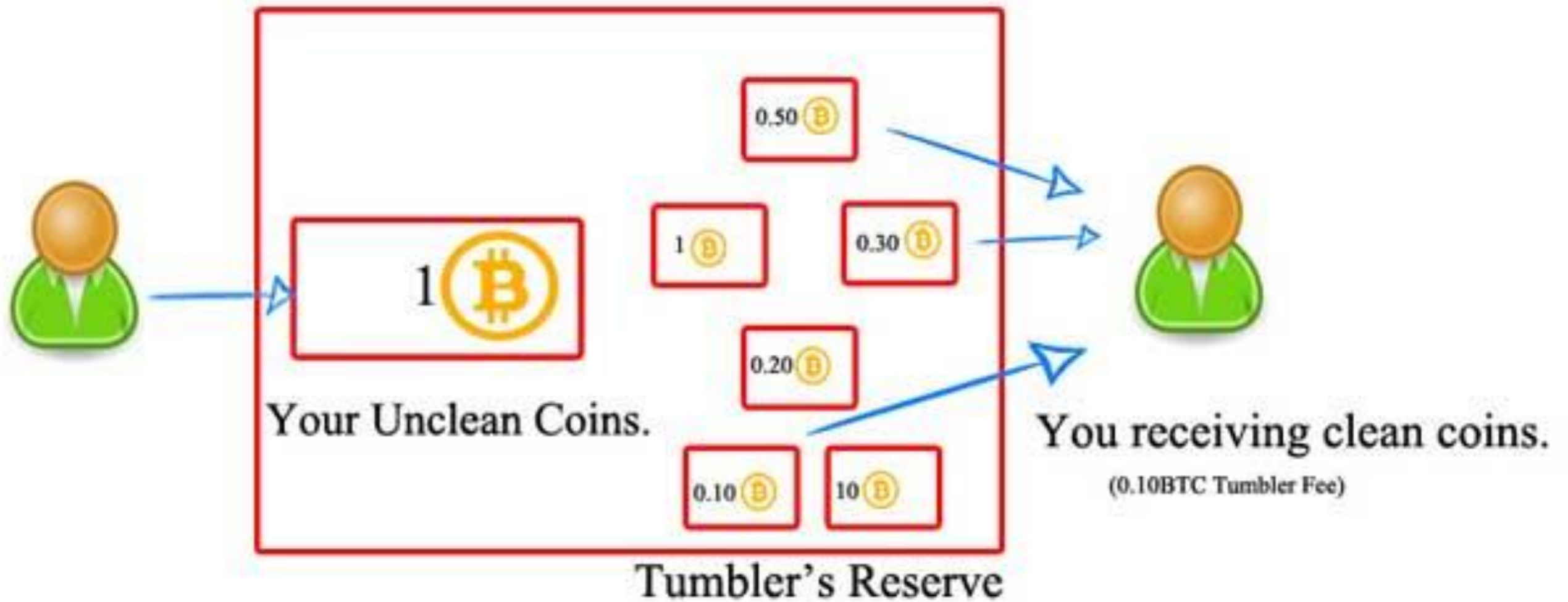
Without CoinJoin



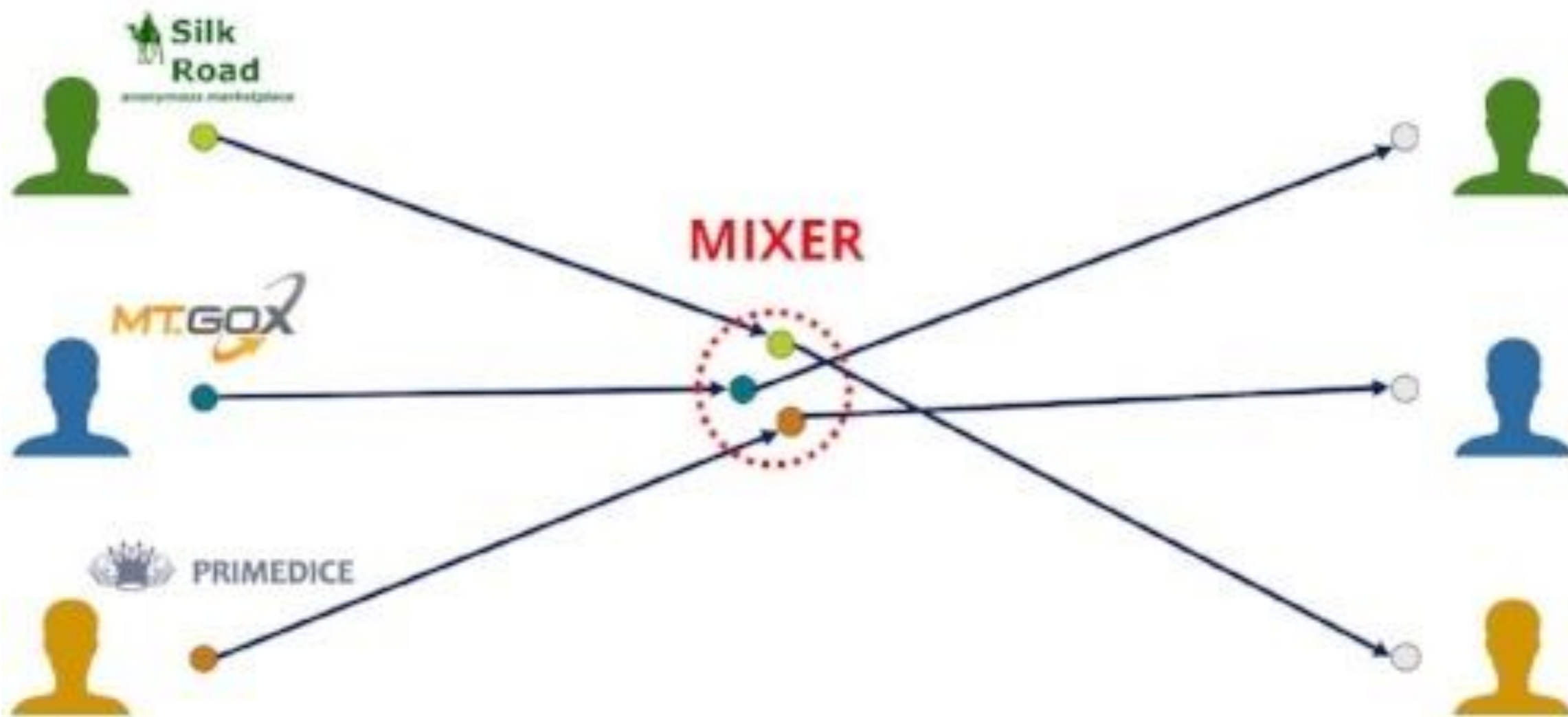
With CoinJoin



Mixing



Mixing



Ukázka

• <https://cryptomixer.io/>

CryptoMixer

Enter CryptoMixer code ?

1 Please enter bitcoin forward to address:

1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX 16h 4m

Add address

Remove delay

Service fee: **0.8160%** - **0.00%** (discount) ?



Time delay



Hide calculator

You send:

10 BTC

You receive (approximately) ?:

9.91790000 BTC after 16h 4m to 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX

Your personal fee 0.816%+0.0005 BTC for every incoming transaction

CONTINUE

Mix my bitcoins

CryptoMixer

2 Download the Letter of Guarantee before send us coins

3 Send your coins (min 0.001, max 632.6802 BTC) to:

17eQFz8mMAidr2jXSoYE1YYESB63pj666d

Add incoming address



Do you know: When you use CryptoMixer with the same code, you pay less service fee! Your CryptoMixer code is: **izwxo**. Save it! See [Fees](#) for details.

Které jsme analyzovali?

- Bitcoin Blender
- Bitcoin Laundry
- BextMixer.io
- PrivCoin
- Blender.io
- MixTum

- <https://www.thedarkweblinks.com/best-bitcoin-mixer-services/>

- <https://www.deepwebsiteslinks.com/bitcoin-tumbler-services/>

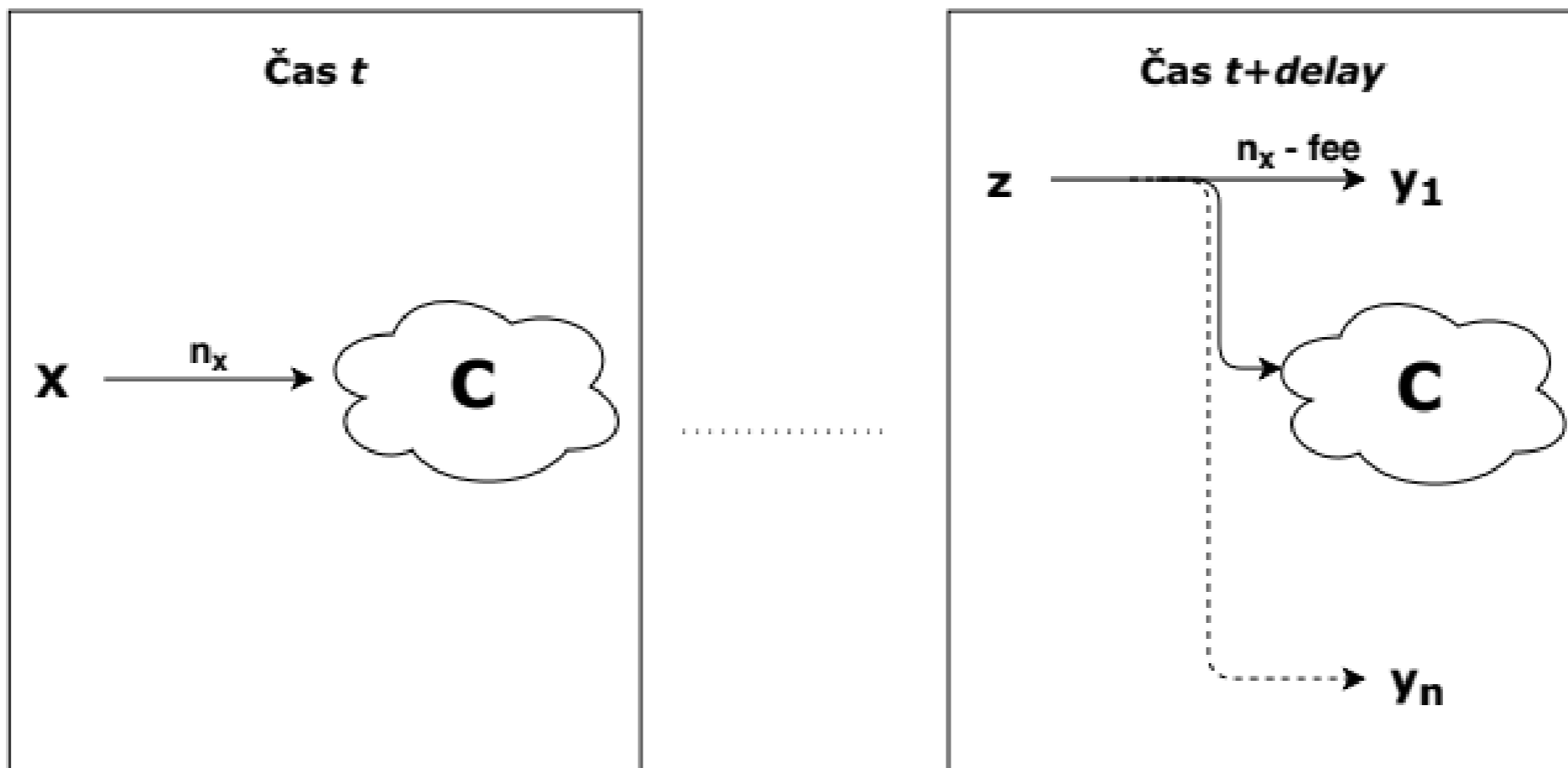
Top BTC Tumbling Service - Best Mixers Ranked May 2019

Find out which Bitcoin Mixers are the best. Our reviews come from real people and we do not share personal data of our users.

Top Bitcoin Tumbler Services 2019

1 - BitcoinMixer 213 Reviews 213 Likes	1 SmartMix Visit Website Tor Link	★★★★★ Minimum Fee: 0.5% Minimum Deposit: Above 0.001 BTC Minimum Confirmations Required: 2 Confirmation TOR ONLY: NO Max Time Delay: Random delay available No Logs Policy: Deleted after 7 days.
2 - CoinMixer 122 Reviews 122 Likes	2 Bitcoin Laundry Visit Website Tor Link	★★★★★ Transaction Fee: 0.0002/Address (No Service Fee) Minimum Deposit: 0.0005 BTC Minimum Confirmations Required: 1 TOR ONLY: No Max Time Delay: Yes, User Controlled No Logs Policy: Yes. (7 Day Retention)
3 - Helix Light 93 Reviews 91 likes	3 SmartMixer Visit Website Tor Link	★★★★★ Transaction Fee: 1% to 5% Minimum Deposit: N/A Minimum Confirmations Required: 3 TOR ONLY: No Max Time Delay: Yes, User Controlled No Logs Policy: 24 Hrs, Auto Delete
4 - BestMixer 62 Reviews 53 likes	4 Anonymix CryptoMixer Visit Website Tor Link	★★★★★ Transaction Fee: 0.3% Minimum Deposit: 0.002 BTC Minimum Confirmations Required: 1 TOR ONLY: No Max Time Delay: Yes, User Controlled No Logs Policy: Yes
	5 BMC Mixer Visit Website Tor Link	★★★★★ Minimum Fee (Not Including the fee/address): 1 to 4% Minimum Deposit: 0.0018 BTC Minimum Confirmations Required: No Define TOR ONLY: Yes Max Time Delay: User Required. No Logs Policy: YES.
	Blender Visit Website Tor Link	★★★★★ Minimum Fee (Not Including the fee/address): 0.5% to 2.5% Minimum Deposit: 0.0001 BTC Minimum Confirmations Required: 3 TOR ONLY: No Max Time Delay: 24 hours. No Logs Policy: YES.

Princip



Heuristika

- Určit cluster C , do něhož spadá adresa pro zaslání peněz.
- Procházet transakce clusteru C , jejichž čas t_2 je vyšší než čas vstupní transakce t_1 , dokud jejich čas nepřekročí $t + d_{max}$, kde d_{max} představuje maximální dobu zpoždění (72 hodin).
- Pro každou transakci proběhne kontrola, zda splňuje následující podmínky:
 - Obsahuje právě 1 vstupní a 2 výstupní adresy.
 - Druhá výstupní adresa spadá do clusteru C .
- Jestliže jsou podmínky splněny, přidá se do seznamu potenciálních
- Pro N od 1 do $addr_{max}$, kde $addr_{max}$ je nejvyšší počet možných výstupních adres:
 - Zkoušet kombinace pro N prvků ze seznamu potenciálních.
 - Pokud součet jejich prvních výstupních adres je v rozmezí $n_x - fee$, kde n_x je vstupní částka a fee spadá to intervalu mezi nejvyšším a nejnižším poplatkem služby, přidá se kombinace do seznamu možných řešení.

Naopak pro určení vstupní adresy na základě výstupní by se použil následující postup:

- Určit cluster C , do něhož spadá adresa pro drobné ve výstupní transakci.
- Procházet transakce clusteru C , jejichž čas t_2 je menší než čas vstupní transakce t_1 , počínaje časem $t - d_{max}$, kde d_{max} představuje maximální dobu zpoždění (72 hodin).
- Pro každou transakci určit adresu vedoucí do clusteru.
- Jestliže je hodnota výstupní adresy transakce vedoucí do clusteru v rozmezí $n_x + fee$, kde n_x je částka ve výstupní transakci a fee spadá to intervalu mezi nejvyšším a nejnižším poplatkem služby, přidá se transakce do seznamu možných řešení.



BestMixer.io Offers the Top Bitcoin Blender 2019 and Complete Anonymity



Cameron Bowen February 18, 2019 2 min read

The team behind BestMixer.io is proud to announce the launch of their top [bitcoin blender](#). This is a professional bitcoin mixer that allows you to perform any type of crypto transaction without any problem. The platform is designed to offer all the adaptability and support you need, all while making everything secure and very easy to use. This is designed to offer a very distinct, professional set of features for all kinds of customers.

Výsledek

Coin Demixer

Basic search

Advanced search

Search for matching input/output transaction

Input TX

TXID

Output TX 1

TXID

Output TX 2

TXID

Output TX 3

TXID

No. of outputs

3

Currency

Bitcoin (BTC)

Mixer

BestMixer.io

Cluster.
service

Tarzan

Min. fee (%)

0

Max. fee (%)

4

Min. address
fee

0

Max. address
fee

0.0004

Min. delay
(hrs)

0

Max. delay
(hrs)

72

Search

Výsledek

Coin Demixer

Basic search

Advanced search

Search finished

The results can be found below. The addresses in **red** correspond to the entry and leaving points, i.e. where the money was transferred to the cluster (in the input transaction) and where it was sent out back to the user's address (in output transactions).

Transaction(s) entered by user

Input transaction (671bacf7b79272cab3ade1d9d3162bd96a0151542e8f337698bd1e48e65d8652)

Inputs

bc1q58e3srpzfurpamsfz0ctd89pjghyawdkt5aapg (0.00160846 BTC)

Outputs

bc1q8l8dgzdn9x9lk7jdnsq4xeam9eeztpa3qvscgc (8.255E-5 BTC)

3KuhVxYpcCEoZezNPndTPxqnoDdsPiiM3Z (0.0015 BTC)

Possible matches (1)

Matches for 1 address (1)

Output transaction #0 (8621e1c1955941037f391658c9785ab98ff76b112b3327e099dac01d19b4eacc)

Inputs

37nK7cWnUqh5ougyybPMP6zq6ANF8vrc4Q (0.00153854 BTC)

Outputs

3JZVY58aSmYY6PiYM3Vb6P25nhGUhwa6QW (0.0014285 BTC)

3AzCEgWn8n8zcsvCod3ozdvYpZPYH5edT7 (6.578E-5 BTC)

Pokračování BestMixeru

BESTMIXER.IO

THIS SERVICE HAS BEEN SEIZED

by the Dutch Financial Criminal Investigation Service (FIOD) under the authority of the Dutch Prosecutor's Office

Dutch Law Enforcement have started an investigation on Bestmixer.io in June 2018. In this investigation we have collected information about transactions, letters of guarantee and support messages.

YOU ARE NOT ANONYMOUS

OPENBAAR MINISTERIE

EUROPOL **POLITIE** **POLICE LÉTZEBUERG** **FIOD Tax and Customs Administration**

Pokračování BestMixeru



EU Authorities Shut Down Bitcoin Transaction Mixer

Stan Higgins   

 May 22, 2019 at 18:00 UTC • Updated May 23, 2019 at 14:37 UTC

NEWS

Pokračování BestMixeru

[Europol](#) alleged that much of the money that passed through Bestmixer.io “had a criminal origin or destination,” contending that “in these cases, the mixer was probably used to conceal and launder criminal flows of money.” The agency said that the service, which launched in May 2018, mixed approximately 27,000 bitcoins.

“The Dutch FIOD has gathered information on all the interactions on this platform in the past year. This includes IP-addresses, transaction details, bitcoin addresses and chat messages,” the agency said. “This information will now be analysed by the FIOD in cooperation with Europol and intelligence packages will be shared with other countries.”



Otázky?

zašlete na veselyv@fit.vutbr.cz

Děkuji za pozornost...