



BITCOIN - ANONYMOUS



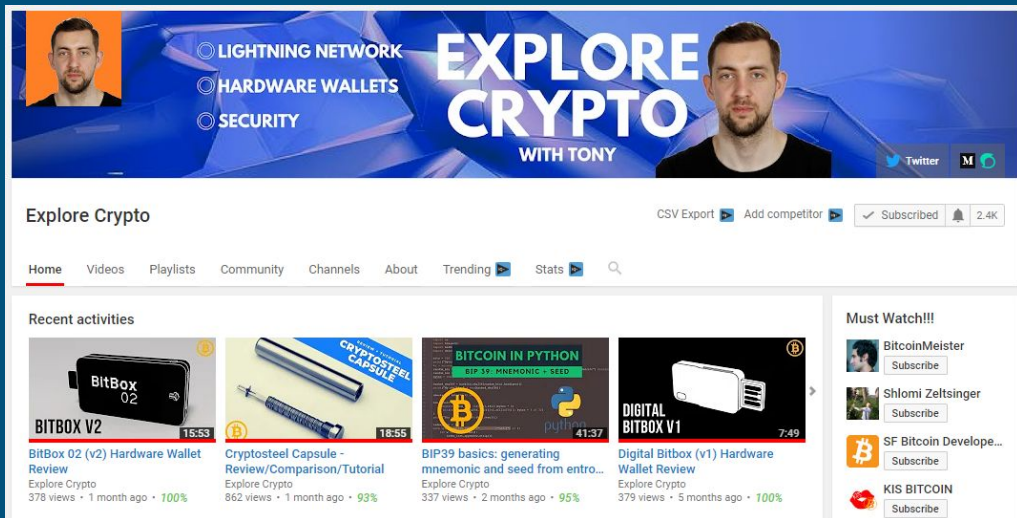
OR NOT?





SAMOURAI WALLET
a bitcoin wallet for the streets.

About me



Non programmers
watching me code



Other programmers
watching me code



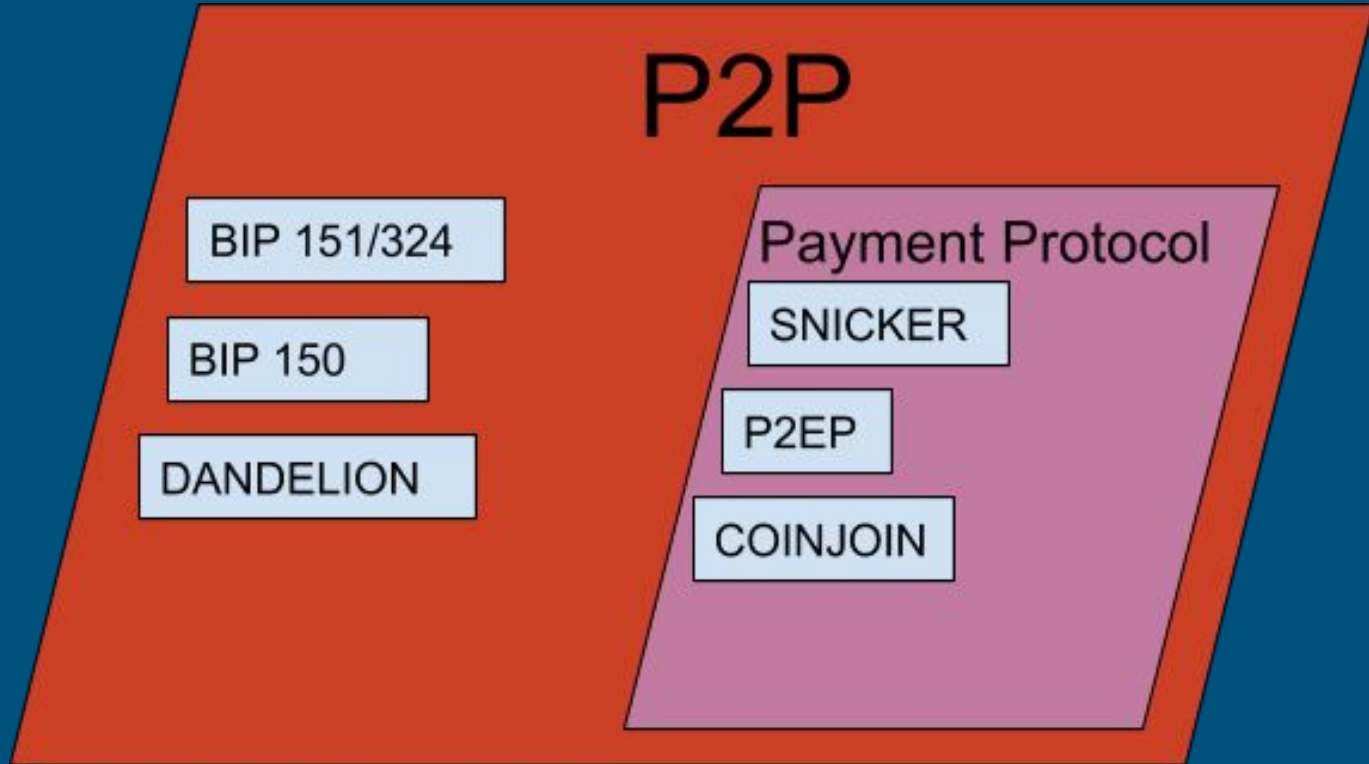
Censorship Resistance / Privacy / Anonymity

CENSORSHIP
RESISTANCE

PRIVACY

ANONYMITY

Protocols



“Bad actors”

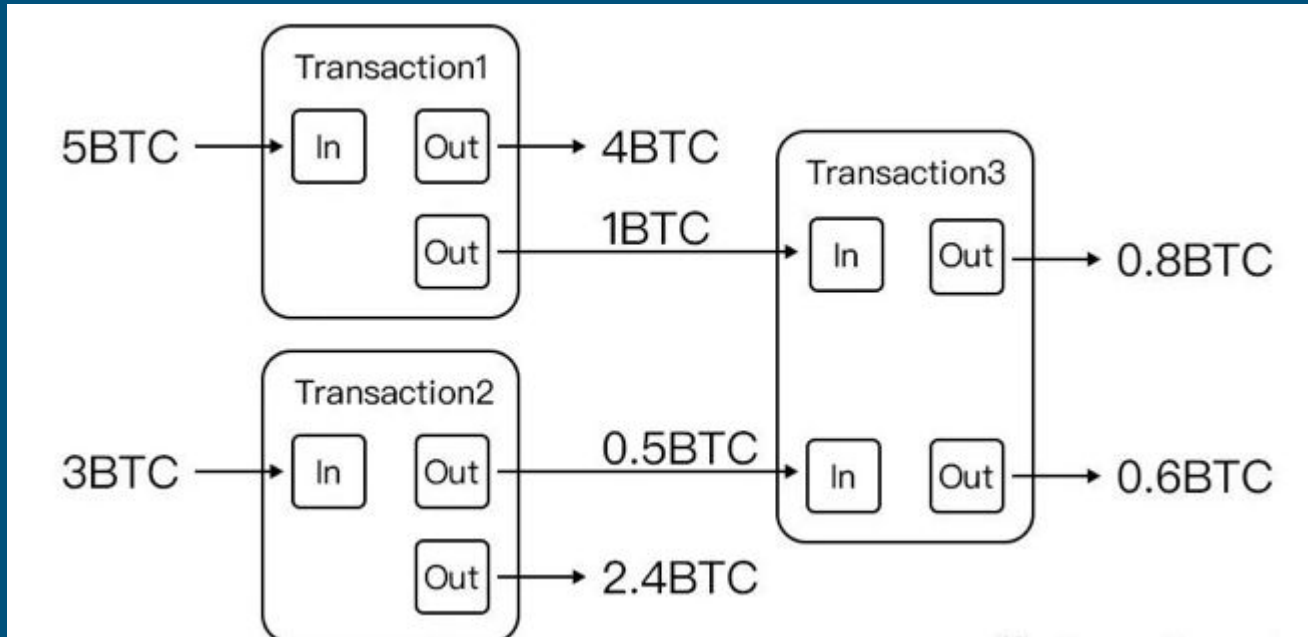


Bottle Pay
@bottlepay

To maintain our integrity as service providers, and to protect the interests of our users, we have taken the painful decision to shut Bottle Pay down rather than become subject to the new [#5AMLD](#) regulations. Please withdraw funds within the next 2 weeks.



UTXO Model vs Account Model



Blockchain Analytics

OS Projects:

- KYCP (Know Your Coin Privacy)
- OXT.me
- walletexplorer

Analytic Companies:

- chainalysis
- blockchain intelligence group
- coinfirm

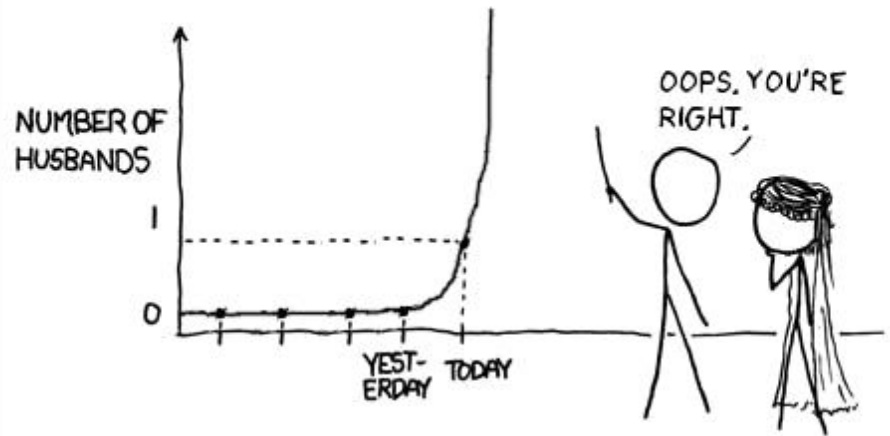
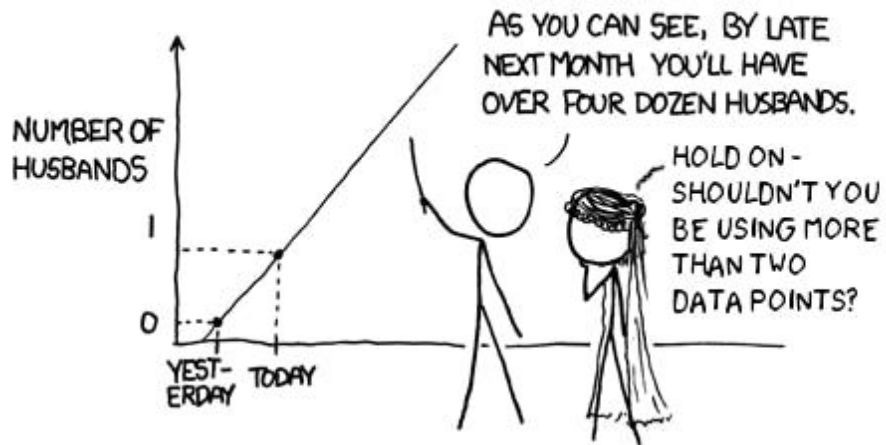


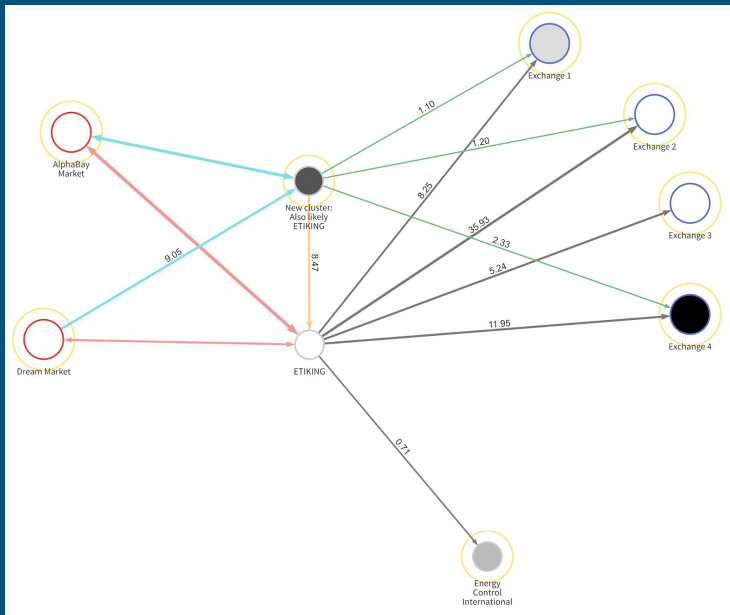
Blockchain Analytics

ASSUME
PROBABLY

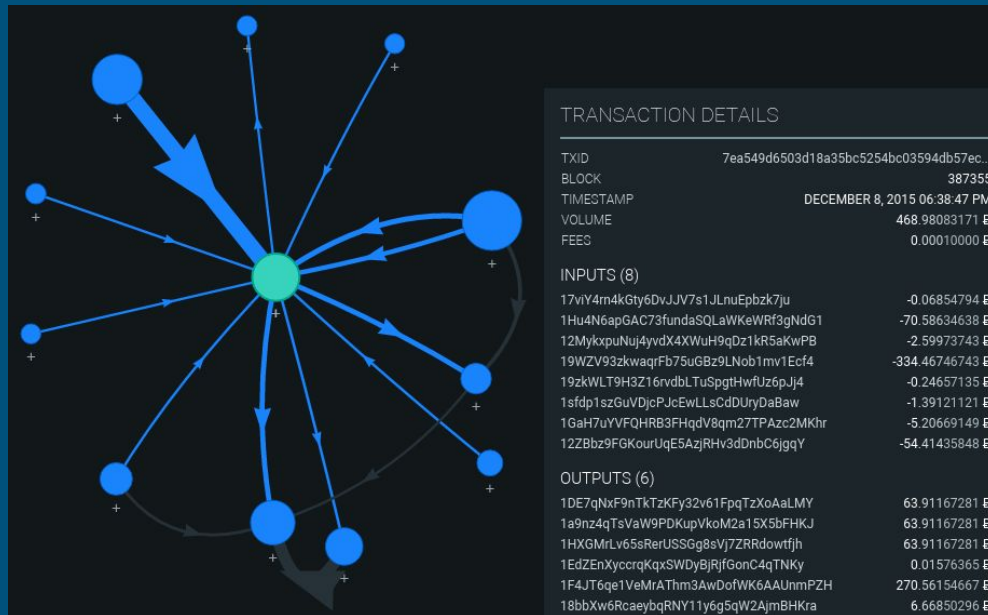
Blockchain Analytics

MY HOBBY: EXTRAPOLATING





Chainalysis Tool

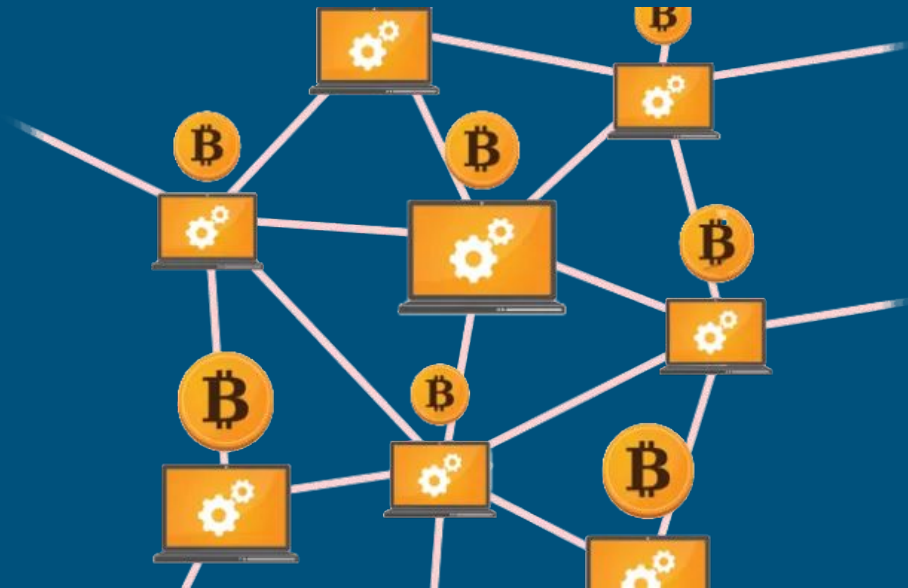


OXT.me

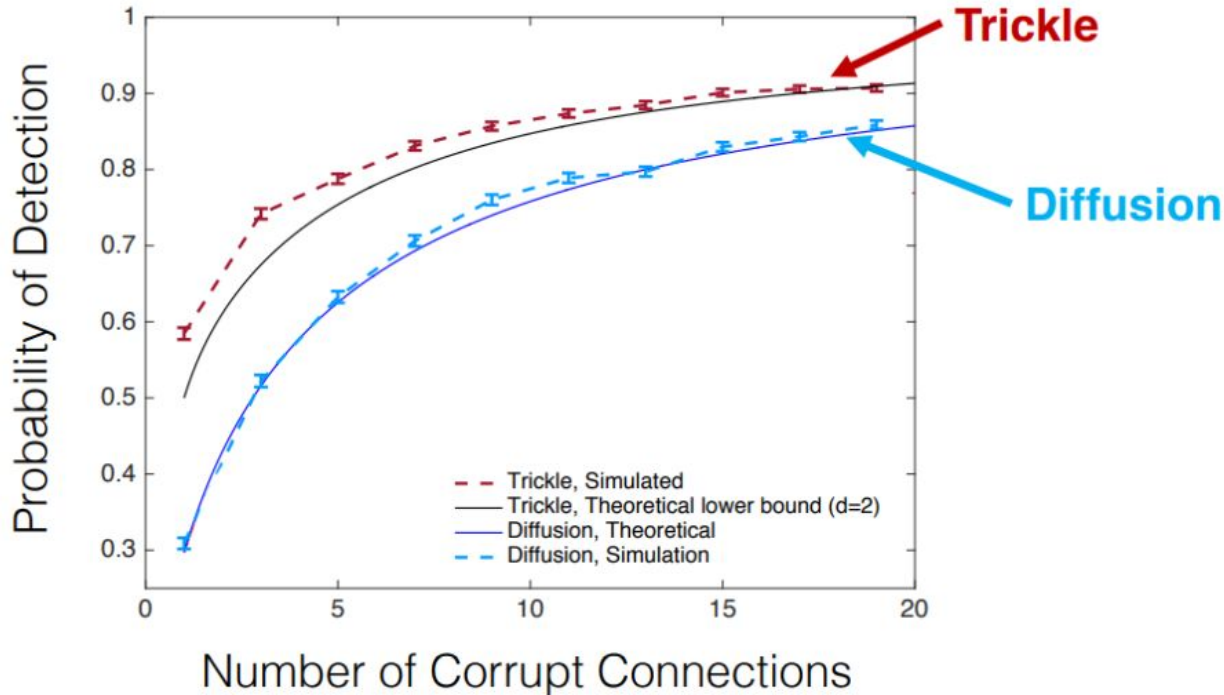
P2P Layer

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshi@gmx.com
www.bitcoin.org

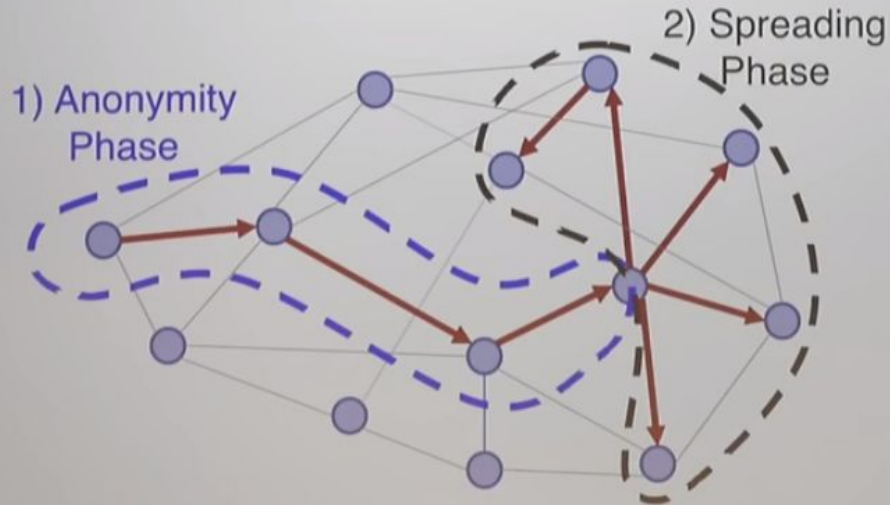


P2P - Dandelion



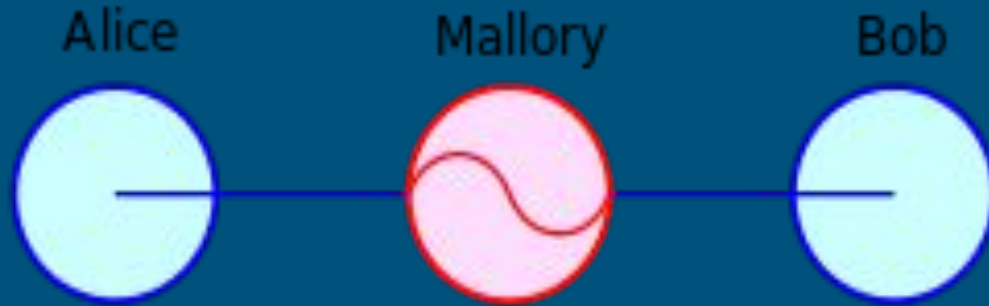
P2P - Dandelion

Spreading Protocol: Dandelion



P2P - MITM attack defences

“With the current unencrypted message transport, BGP hijacking, block delay attacks and message tampering are inexpensive and can be executed covertly (undetectable MITM)”



P2P - MITM attack defences

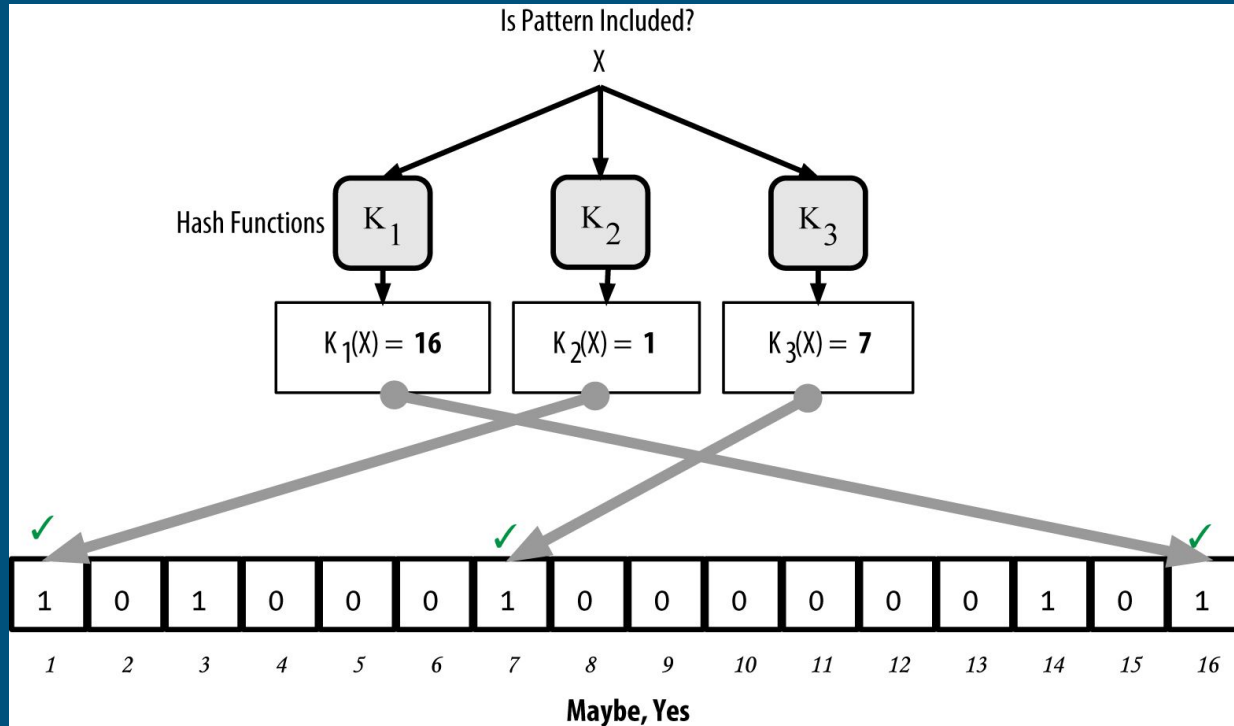
BIP 324 - Version 2 Peer-to-Peer Message Transport Protocol

BIP 150 - Peer Authentication

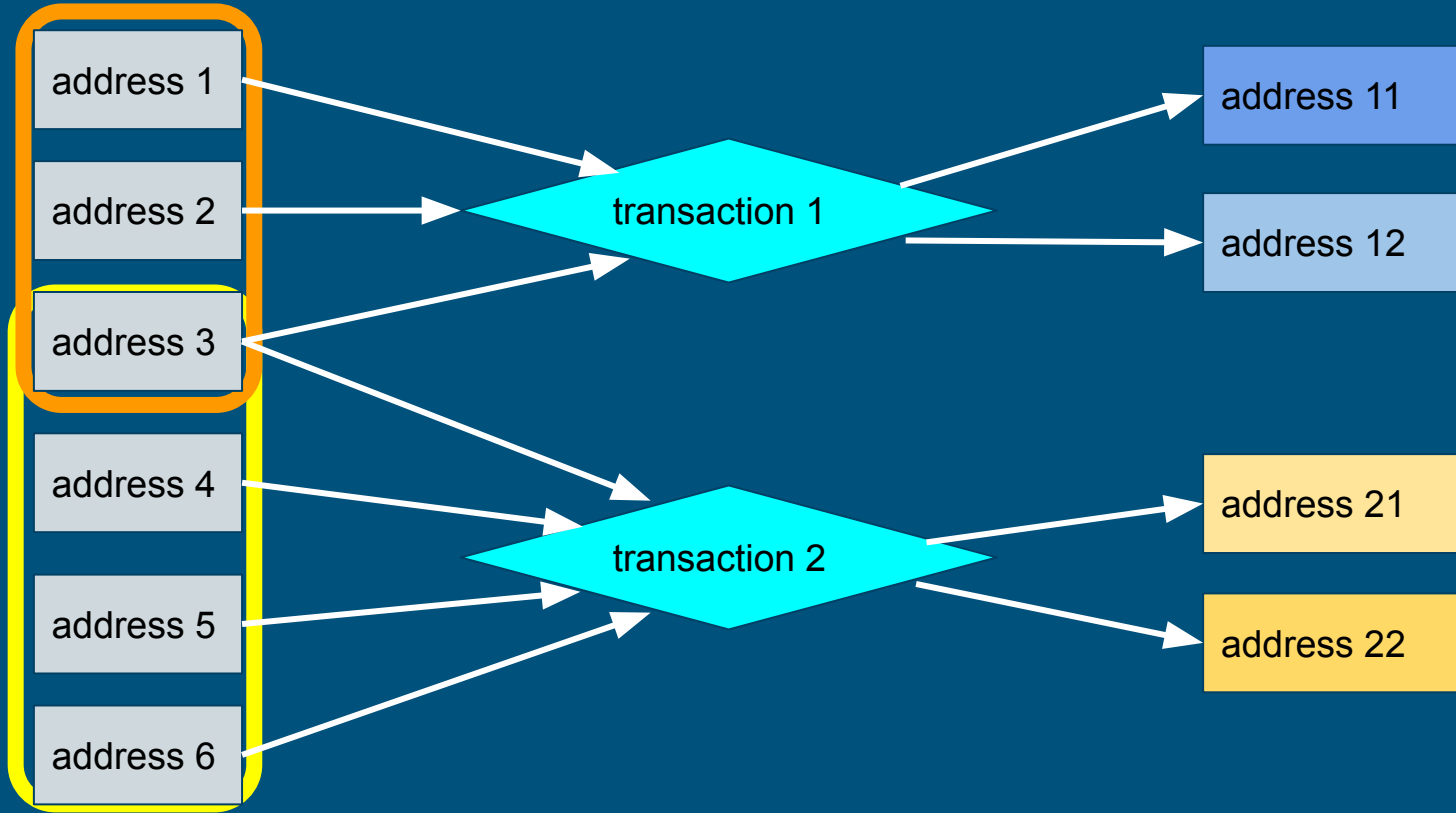
BIP 324 is really just a building block in strengthening Bitcoin's P2P layer against malicious MITM attacks. It may become a critical step in development work to determine whether MITM attacks pose a real threat to Bitcoin or it may be determined that they do not. But it's hard to gather that data without tools like the ones suggested by BIP 324.

BIP 324 is focused on providing tools to mitigate passive MITM attacks, while co-implementation with BIP 150 offers some potential tools for active MITM attacks.

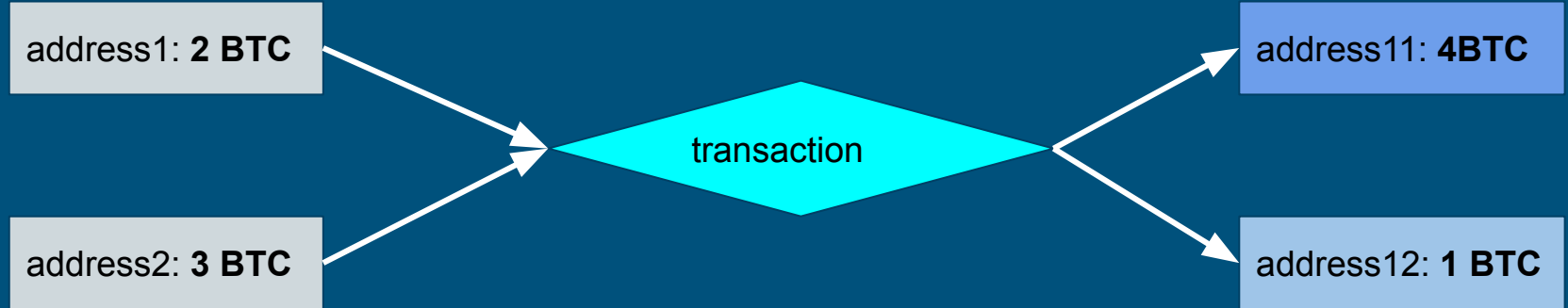
P2P - SPV



Blockchain Analytics - Co-Input Clustering



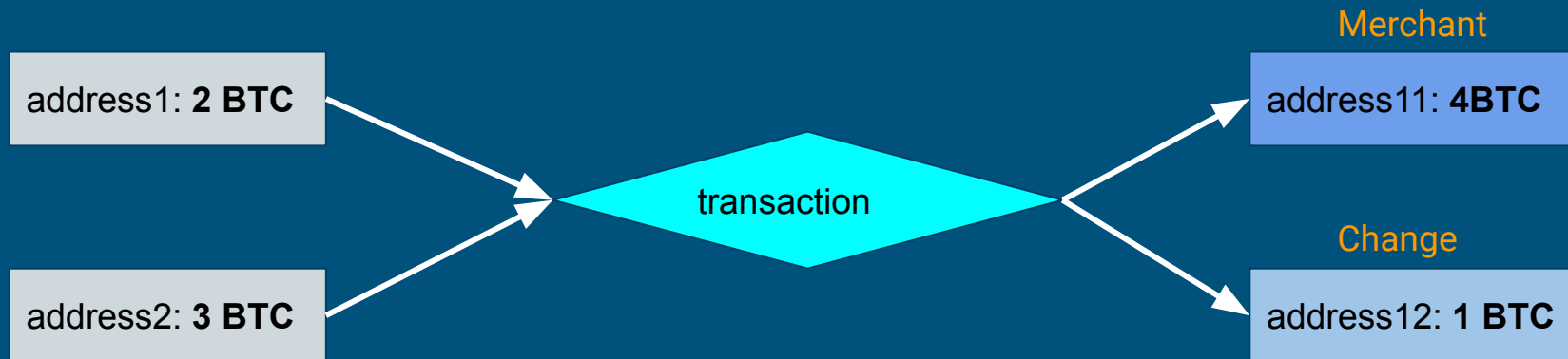
Blockchain Analytics



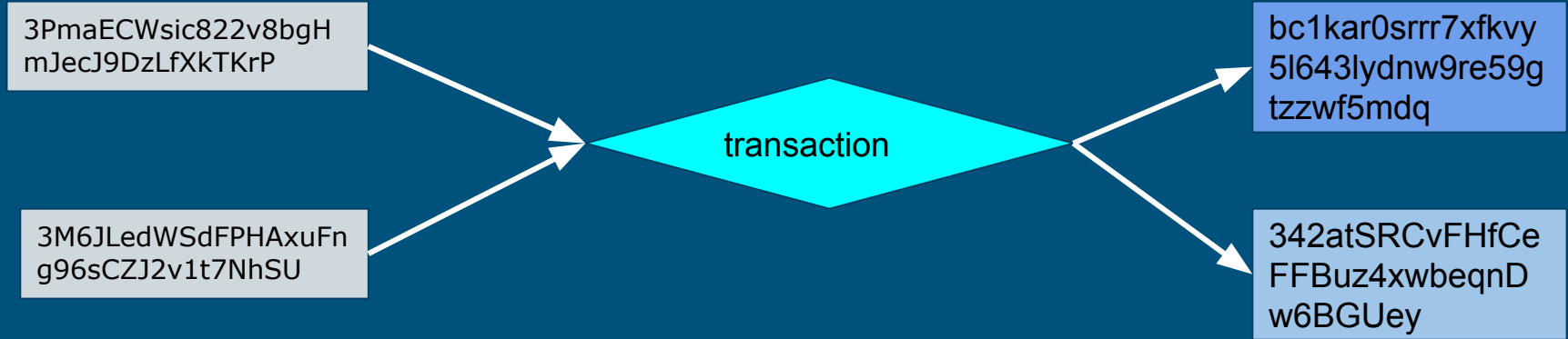
User (addresses 1 and 2) is sending bitcoin to a P2P merchant in two inputs (2 and 3 BTC).

Which output is a merchant related, which output is a change?

Blockchain Analytics

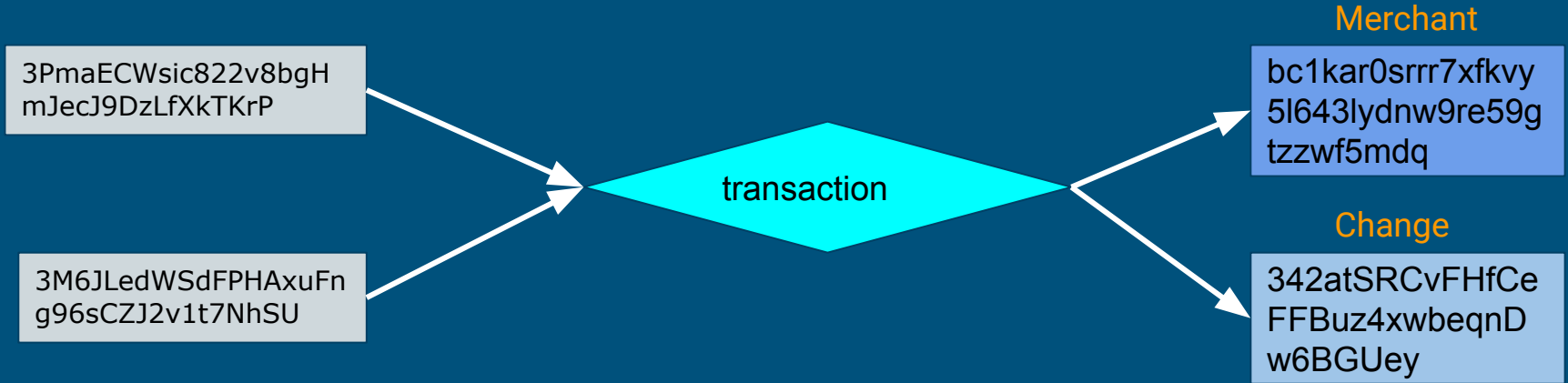


Blockchain Analytics

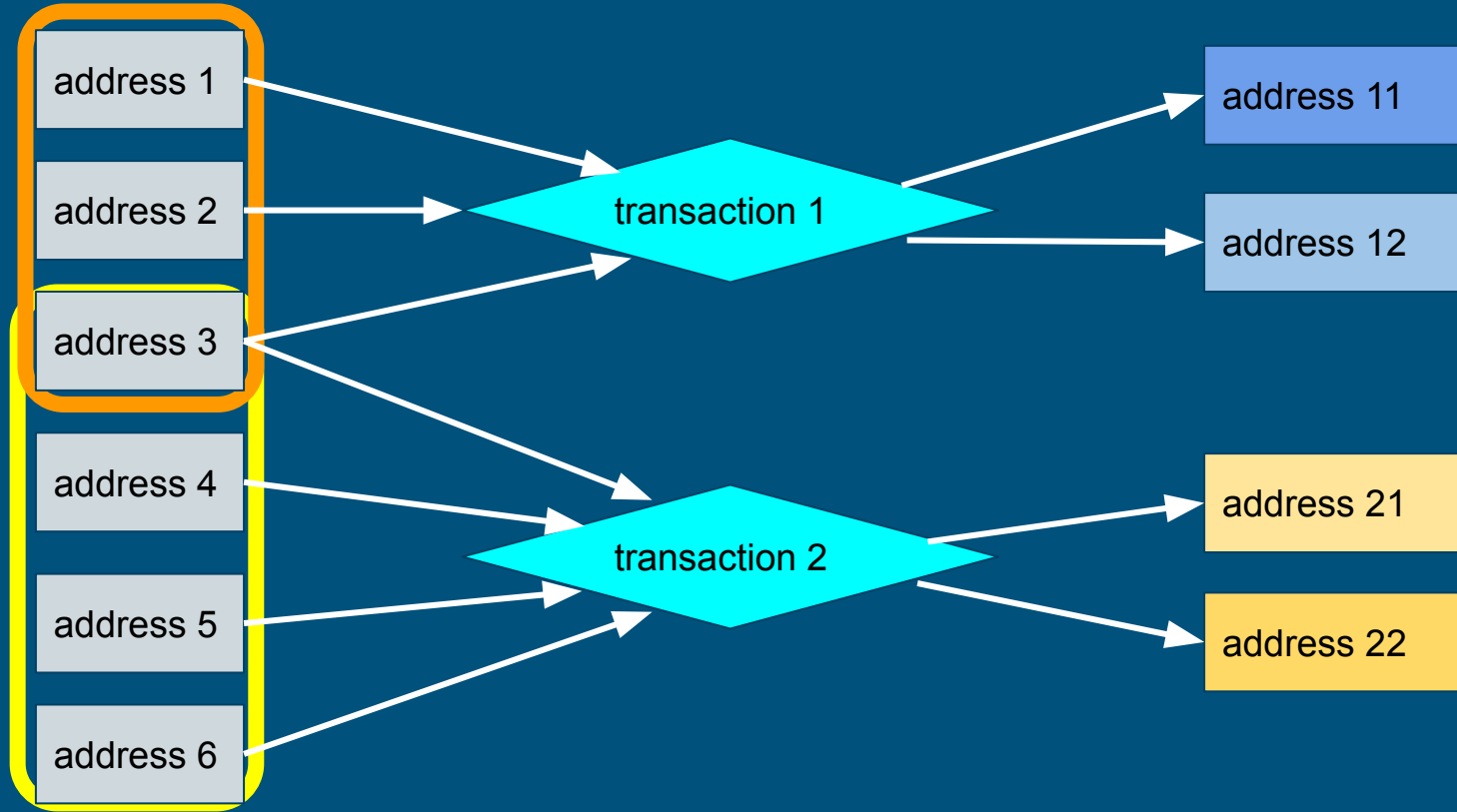


User is sending bitcoin to a P2P merchant in two inputs - P2SH format.
Which output is a merchant related, which output is a change?

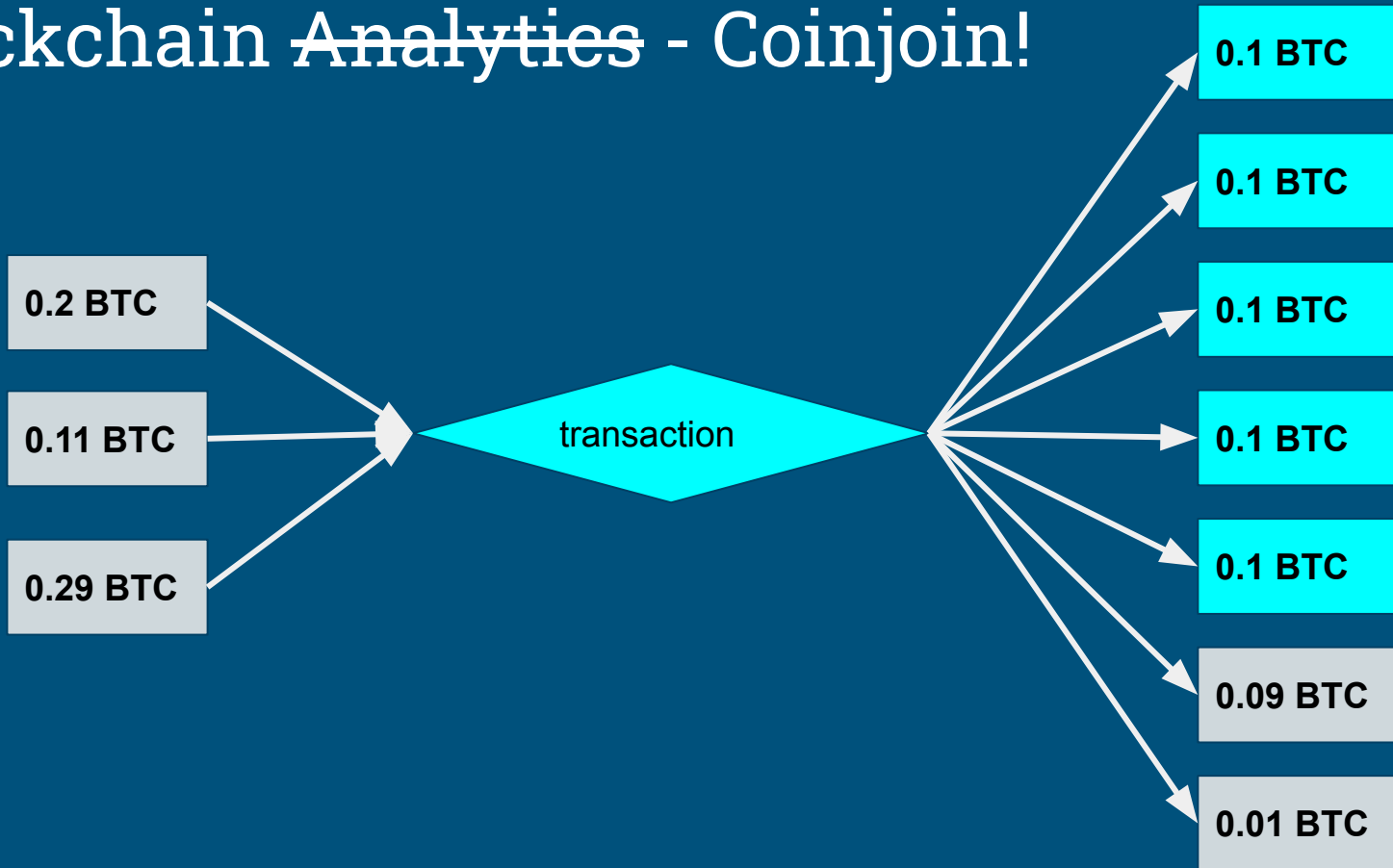
Blockchain Analytics



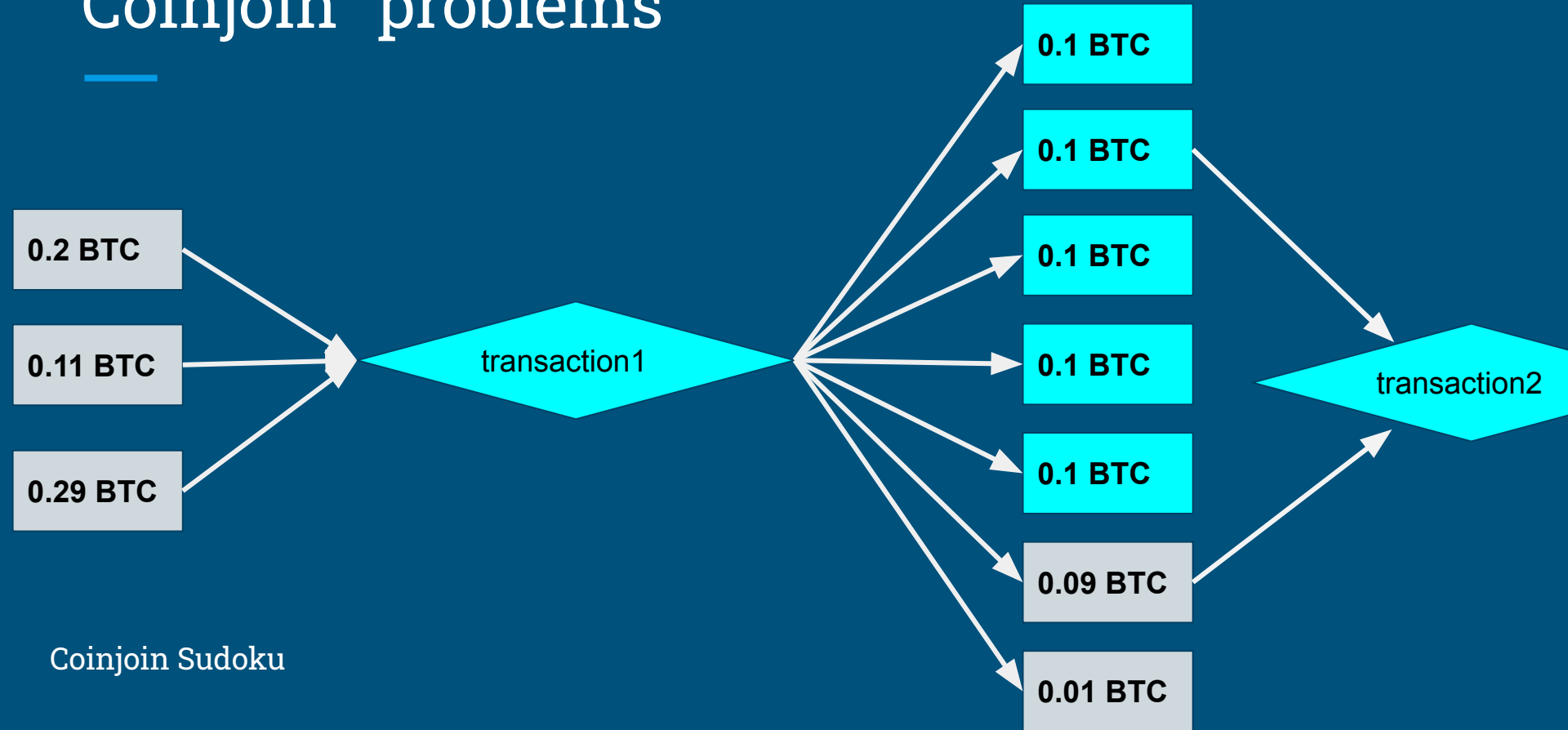
Blockchain Analytics - Co-Input Clustering



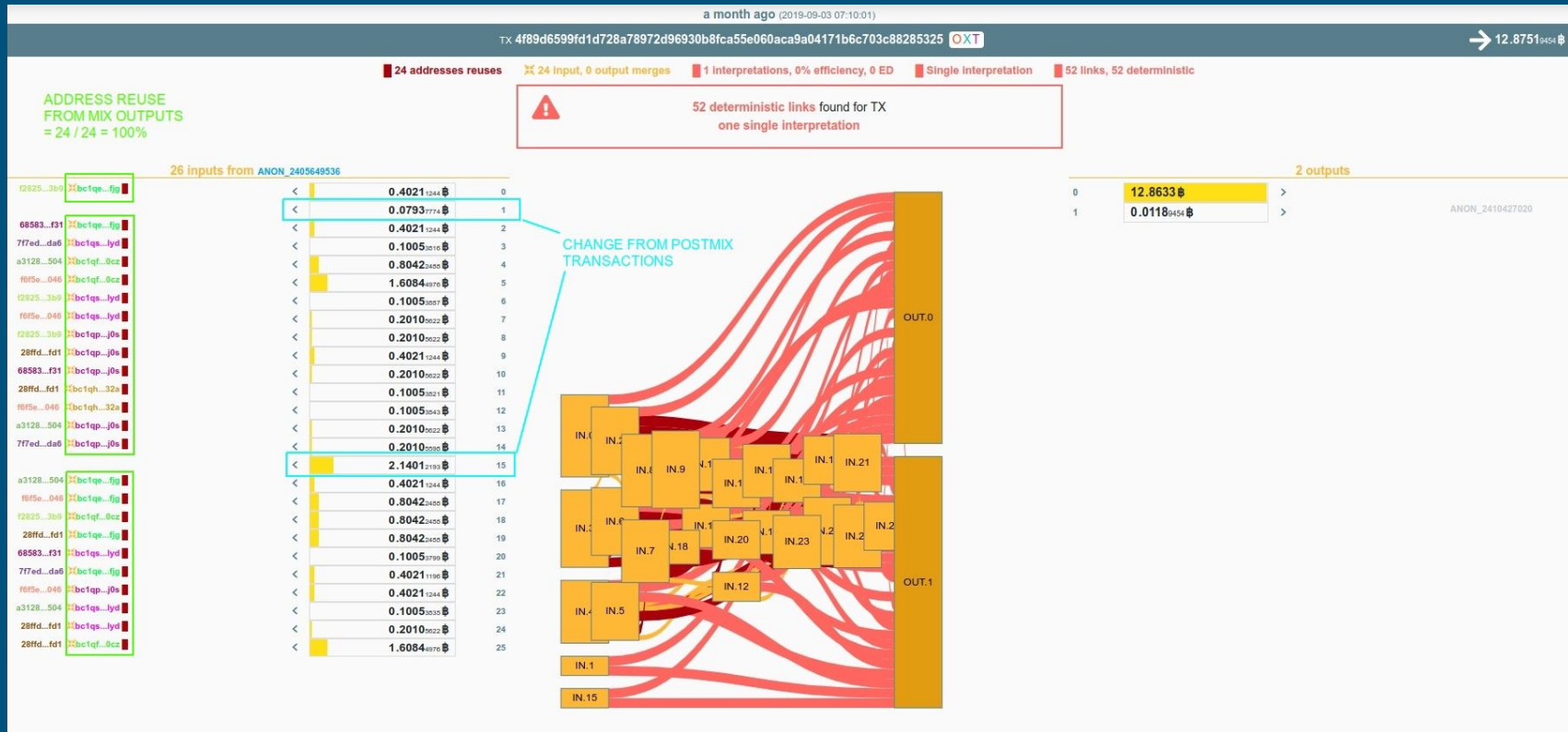
Blockchain ~~Analytics~~ - Coinjoin!



Coinjoin “problems”



Coinjoin “problems”



Coinjoin “problems”



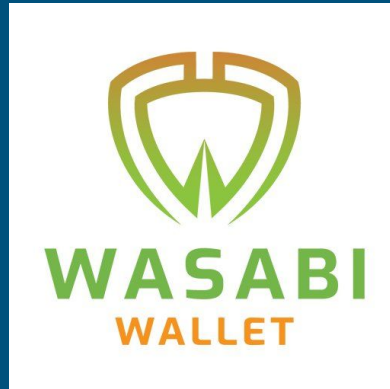
Coinjoin “apps”

JoinMarket

Samourai Wallet



Wasabi Wallet

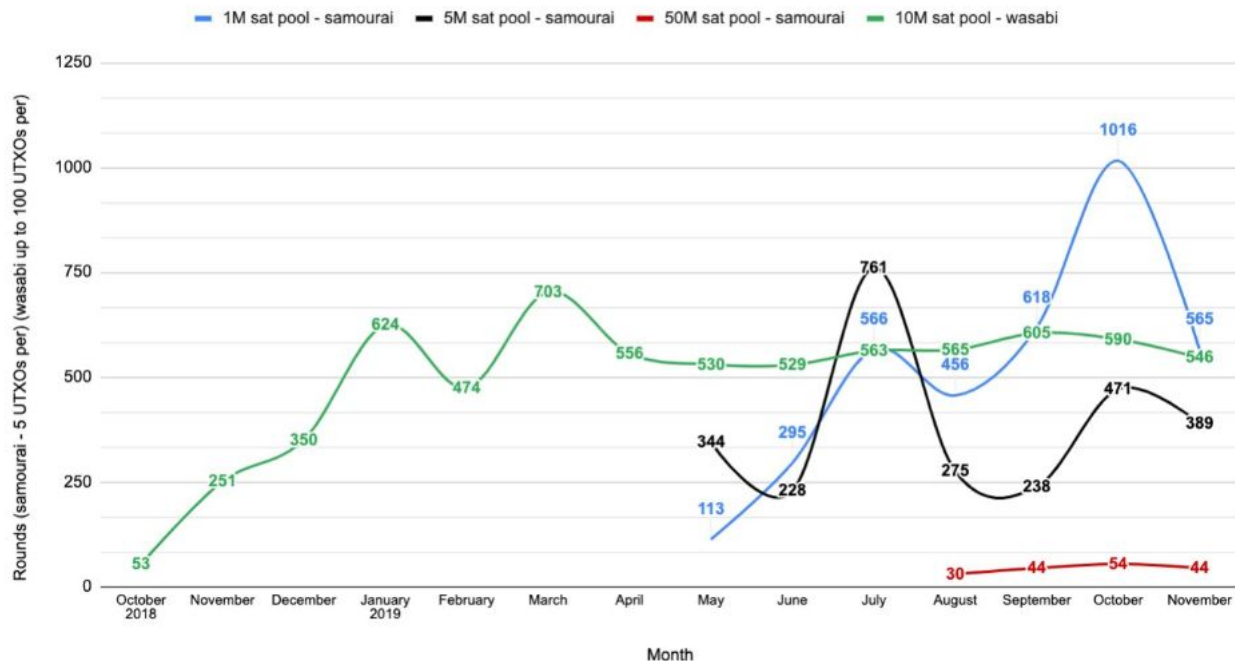


ZeroLink Protocol

Coinjoin “apps”

Coinjoin Usage* - Samurai Whirlpool & Wasabi Wallet

*numbers can be inflated at negligible cost by the respective teams



2019.9

Wasabi transaction count:	600
Samurai transaction count:	898
Wasabi total volume:	26200 BTC
Samurai total volume:	200 BTC
Wasabi total mixed volume:	17485 BTC
Samurai total mixed volume:	200 BTC
Wasabi anonset weighted volume mix score:	419303
Samurai anonset weighted volume mix score:	1000

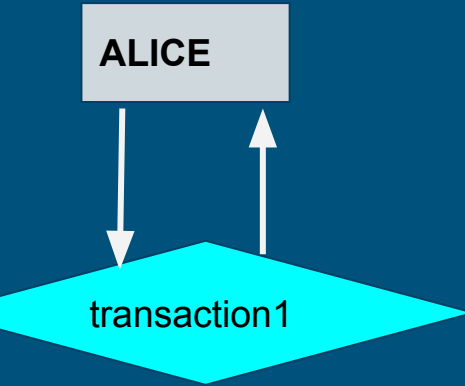
2019.10

Wasabi transaction count:	583
Samurai transaction count:	1542
Wasabi total volume:	16572 BTC
Samurai total volume:	301 BTC
Wasabi total mixed volume:	10779 BTC
Samurai total mixed volume:	301 BTC
Wasabi anonset weighted volume mix score:	418963
Samurai anonset weighted volume mix score:	1506

Bitcoin Mixers



SNICKER



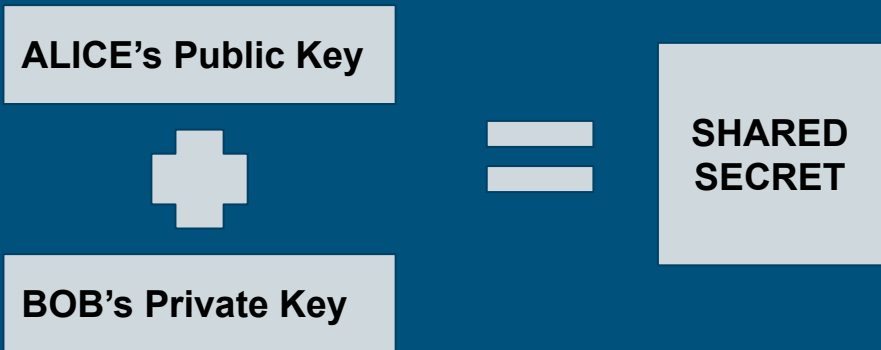
Step1. Reusing address, marking UTXO as available to be mixed:

- UTXO visible
- public key visible

BOB

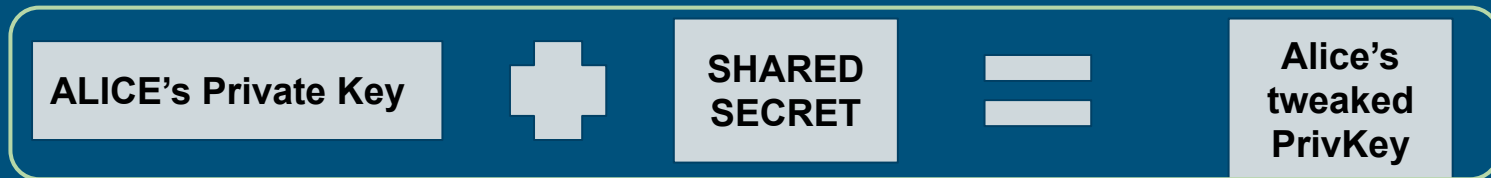
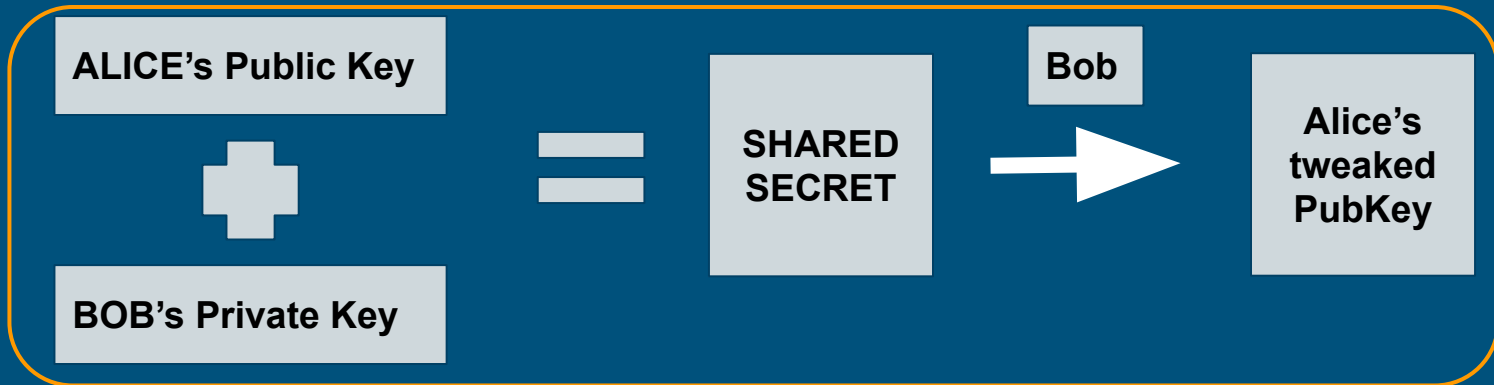
SNICKER

Step2. Generating a Shared Secret



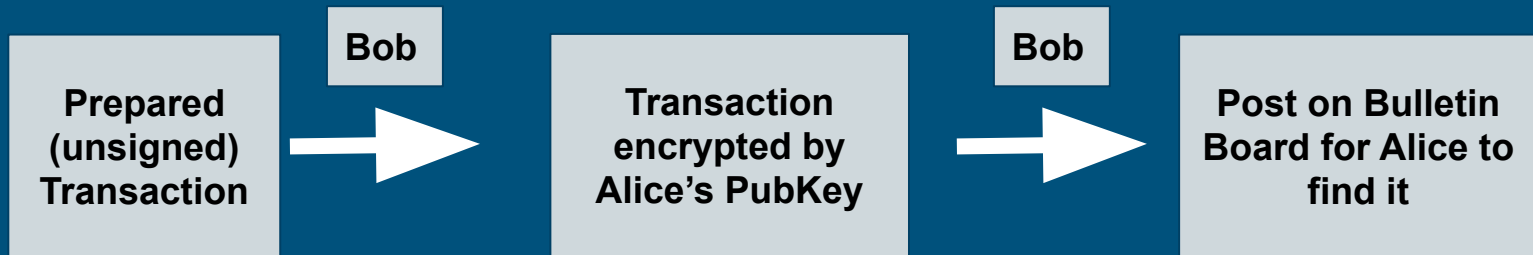
SNICKER

Step3. Generating a “tweaked PubKey” and “tweaked PrivKey”



SNICKER

Step4. Posting transaction
on the Bulletin Board for
Alice to find



SNICKER Problems

- Only a proposal so far
- Low anonymity set
- A LOT of false positives
- SPAM and filtering

P2EP



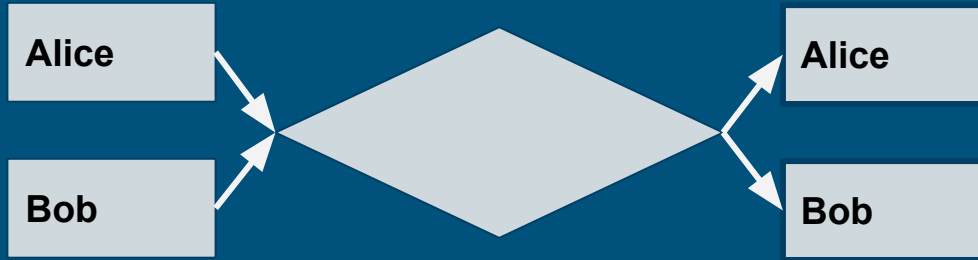
P2EP

Alice

Bob

```
bitcoin:175tWpb8K1S7NmH4Zx6rewF9WQrcZv245W  
?endpoint=http://3g2upl4pq6kufc4m.onion
```

P2EP



- Alice sends her UTXO to the endpoint (Bob's)
- Bob responding with a series of UTXOs of his own (100)
- Alice signs all the transactions, sends them back to Bob
- Bob signs the one valid transaction out of the set, proceeds to publish it

Recommendations (Coin -FU)

- Proper wallets
- Mixing coins
- Separating Wallets
- Reusing addresses (don't!)



Sources


- Andreas Antonopoulos - Mastering Bitcoin
- Chainalysis Blog
- ErgoBtc - Tracking the PlusToken Whale
- Samourai wallet docs
- Wasabi wallet docs
- BitcoinMagazine articles

Cool resources

- All technical BitcoinMagazine articles
- [ErgoBTC: Tracking the PlusToken Whale](#)
- [Raspiblitz](#)
- [BtcPayServer](#)
- [Blockstream Block Explorer](#)
- [Hardware Wallet Interface](#)
- [BitcoinOpTech Newsletter](#)

Thank you!

twitter.com/SanakTony



EXPLORE CRYPTO WITH TONY


- LIGHTNING NETWORK
- HARDWARE WALLETS
- SECURITY

Twitter M

Explore Crypto CSV Export Add competitor ✓ Subscribed 2.4K

Home Videos Playlists Community Channels About Trending Stats

Recent activities




BITBOX V2 15:53

BitBox 02 (v2) Hardware Wallet Review

Explore Crypto

378 views • 1 month ago • 100%




CRYPTOSTEEL CAPSULE 18:55

Cryptosteel Capsule - Review/Comparison/Tutorial

Explore Crypto

862 views • 1 month ago • 93%




BITCOIN IN PYTHON 41:37

BIP39 basics: generating mnemonic and seed from entropy

Explore Crypto

337 views • 2 months ago • 95%




DIGITAL BITBOX V1 7:49

Digital BitBox (v1) Hardware Wallet Review

Explore Crypto


379 views • 5 months ago • 100%

Must Watch!!!




BitcoinMeister

Subscribe




Shlomi Zeltsinger

Subscribe



SF Bitcoin Developer

Subscribe



KIS BITCOIN

Subscribe