Bitcoin fungibility

The absolute state of it

TDevD, Samourai Wallet, https://samouraiwallet.com/pgp

Original sin

We dropped the ball and allowed Bitcoin to be defined as "money".

Satoshi's white paper : "digital cash"

Bitcoin == text, 1st amendment

"Wallets" == keychains

Pseudonymous bitcoin : Did Satoshi think things through ? Did he place too much faith in an emerging circular economy ?

Regulatory capture

- KYC/AML
- FATF "guidelines"
- Pre-emptive compliance (ex. : La Maison du Bitcoin, Bull Bitcoin)

Financialisation

- GBTC
- ETFs : Bermuda, Canada
- Futures : CBOE, CME (also offers options on futures)

Stockholm syndrome

- NgU is enslavement to fiat
- "NgU tech" is intellectual sloth
- Magical thinking : "designed to pump forever"
- KYC-DCA : CashApp, RobinHood, Revolut
- LNStrike
- Podcast "influencers" pimping KYC on-boarding services and/or accepting them as sponsors.

Privacy : stunted protocol growth

- Toxic elitism, NIH ("not invented here")
- Foot dragging by Core. Anyone remember Dandelion ? Still think we will see on-chain sigagg ?
- BIP bureaucrapping
- *"Ossification"* is a euphemism for **knee capping**
- Appeals to authority : **Fuck GMax**, he never coded a coinjoin

What is happening now ?

Good cop (walled garden)

Stealth white listing via walled garden approach :

- KYC of withdrawal addresses
- Chain analysis applied to deposits
- Chain analysis applied to withdrawals
- Rapid growth of 'de facto L2' : PayPal, CashApp, Revolut, RobinHood

Bad cop (rogue addresses)

- Black listing
- OFAC
- Brave New World... Newspeak : "unhosted wallets"
- Wokeness creep : "compliant miners" and associated investment funds, VCs
- Flagging of coinjoins

Fungibility

- Dread looks elsewhere
- DarkNet Bible looks elsewhere
- DNMs look elsewhere : Wall Street Market
- Chainalysis raises $100m, valued at $4.2b

"Use the tools" (h/t @Diverter_NoKYC)

Lightning network

- Hub & spoke, not decentralized, LNBig, Bitrefill
- Designed for consumer market, "bank ready"
- Strong tendency to resort to custodial UI/UX
- Privacy pitfalls of Lightning are better understood : https://abytesjourney.com/lightning-privacy/

Liquid

- Originally presented as tool for exchange clearing but...
- …custodial trojan horse
- Sucks in and neuters privacy features : today Confidential Transactions ("CT", crippled on Liquid), tomorrow Schnorr signature aggregation (CISA, "sigagg")

Ricochet

- Add hops to transaction history
- Stump blacklisting
- Protect against 3rd party account closures
- Based on fungibility talk given by Adam Back and Blue Matt

BIP47 / PayNyms

- Just send to PayNym. No need to request an address
- Built-in refund/return addressing
- User does not have to be online : no watchtowers, non-custodial
- No published address removes starting point for chain analysis
- V3 soon, test vectors replicated

Coinjoin : done wrong

- Wasabi never implemented ZeroLink...

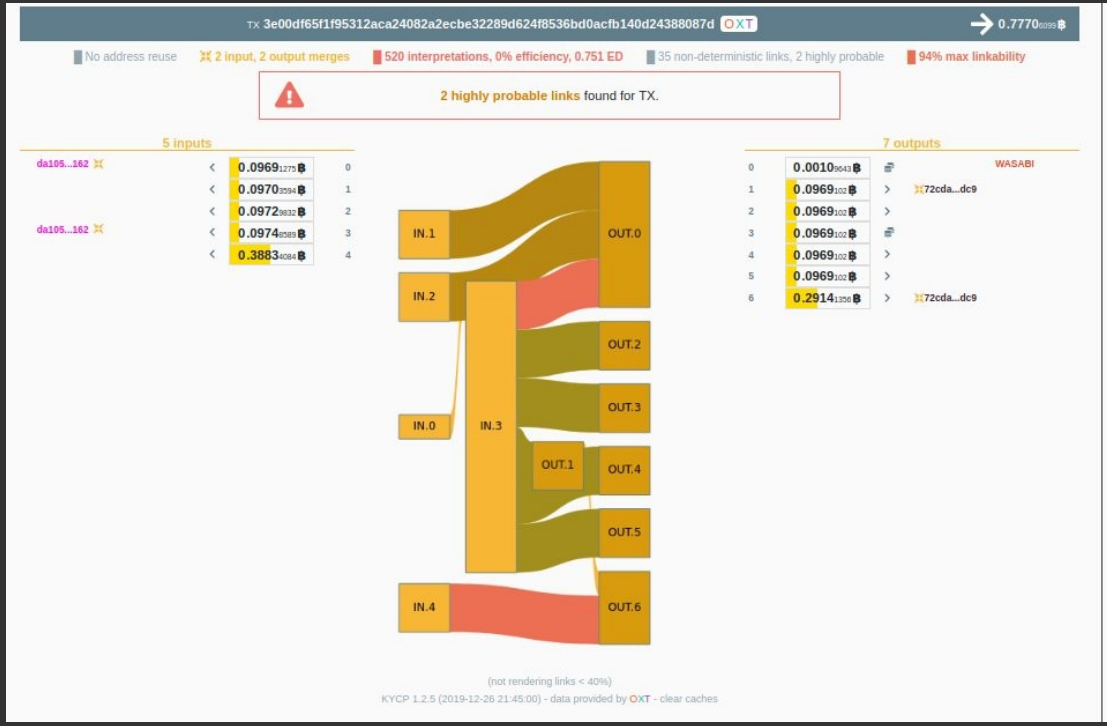
  but soon : stenographic ì

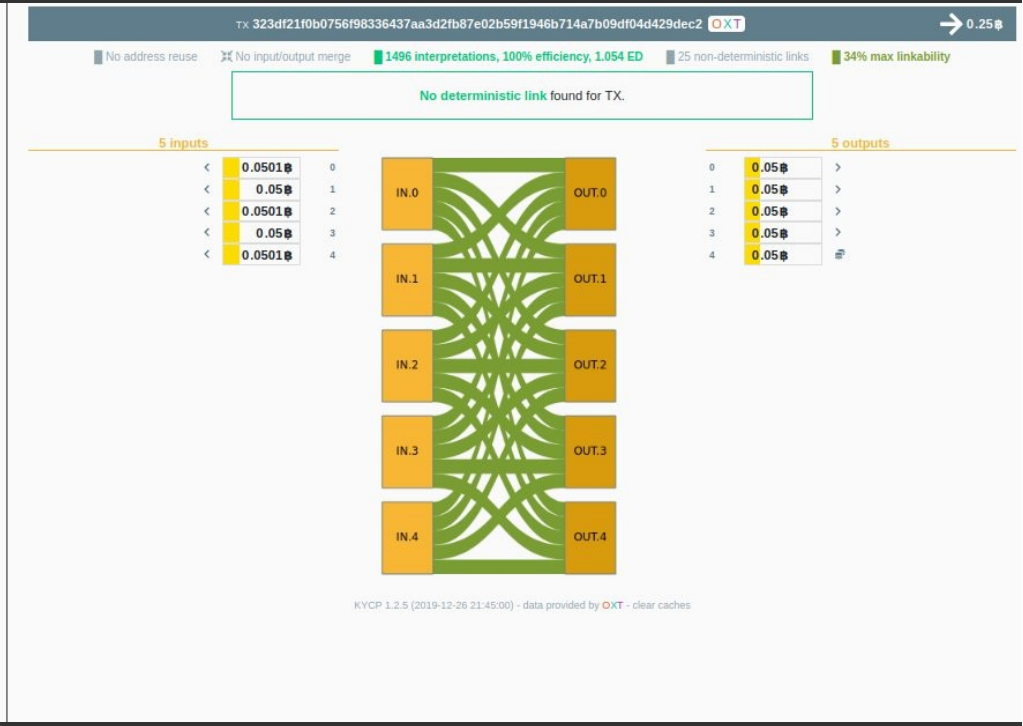
- The "war on coinjoin" started from within : paid cronies refused to acknowledge, and still refuse to do so, deep flaws in ì
- Influencer FUD (check Bio) : "likely illegal"
- CoinSwap : "Specifically, Belcher said that some users may prefer to use CoinJoin in situations where it is desirable to publicly prove that a UTXO's transaction history has been broken." https://archive.is/eM97I
- Nevermind the BIPs, here's stillborn P2EP : ignored by its own paid shills

Coinjoin : done right

- Samourai Whirlpool only ZeroLink implementation to date : only 100% entropy coinjoins are guaranteed link busters
- Cahoots : Stowaway, STONEWALL(x2). More Cahoots to come.

Coinjoin : A picture is worth 1496 combinations





XMR-BTC atomic swaps

- Swaps are trustless, permissionless, non-custodial
- Eliminates need for centralized swap services that have been known to shotgun-KYC
- Bitcoin and Monero are natural allies (Bitcoin maxis and Monero maxis, not so much)
- Bitcoin needs private, trustless, non-custodial "L2". Also needs to get back in touch with its ethos. Monero provides both.
- Monero needs permissionless on/off ramps. Exchanges not delisting will request view keys.