Anarchokapitalismus

Díl šestatřicátý:

Anonymita Bitcoinu a její rizika

Přednáší Pavel Ševčík

4. března

v klubu (de)Centrála

pristav.urza.cz

O čem budeme mluvit?

- Vlastnosti dobrých peněz
- Současný stav finančního světa
- (Ne)anonymita Bitcoinu a jak jí řešit
- Možné nástrahy a jejich řešení

Vlastnosti peněz

pristav.urza.cz

- Prostředek směny (medium of exchange)
- Uchovatel hodnoty (store of value)
- Účetní jednotka (unit of account)

Vlastnosti dobrých peněz

pristav.urza.cz

- Dělitelnost (divisibility)
- Trvanlivost (durability)
- Nedostatečnost (scarcity)

Vlastnosti dobrých peněz

pristav.urza.cz

- Zaměnitelnost (fungibility)
- Nevystopovatelnost (untraceability)
- Necenzurovatelnost (uncensorability)

Vlastnosti dobrých peněz

pristav.urza.cz

- Nejlepší peníze historicky vzešly ze svobodné volby
- Trh vždy konverguje k nejlepším penězům
- Bitcoin má potenciál stát se nejlepšími penězi

Finance nyní

pristav.urza.cz

- Centrální autority mají přímou kontrolu nad vznikem nových peněz
- Peníze v bance nejsou vaše – banka je může zabavit, či zakázat transakce
- Mezinárodní platební styk je drahý a pomalý

Finance nyní

pristav.urza.cz

- Díky digitalizaci jsou transakce stopovatelné a cenzurovatelné
- Státy regulují možnosti použití hotovosti

Finanční diktatura

pristav.urza.cz

- Státy se již připravují na úplné zrušení hotovosti
- Systémy jako EET poslouží k dalšímu špiclování
- Státy budou mít neomezenou kontrolu nad tokem financí a neomezenou možnost danění

Řešení problému

pristav.urza.cz

- Návrat ke zlatému standardu není v 21. století možný
- Jako jediné řešení se nabízí Bitcoin
- Ale…

(Ne)anonymita Bitcoinu

- Bitcoin je pseudonymní, nikoliv anonymní
- Všechny transakce jsou navždy zapsány v blockchainu
- Kryptoměnové burzy musí splňovat KYC/AML pravidla → zákazníci jsou jasně identifikováni

(Ne)anonymita Bitcoinu - řešení

- Privacy oriented altcoiny – Monero, Zcash atd.

- Postrádají mnohé vlastnosti dobrých peněz
- Jsou velmi centralizované
- Nemusí umožňovat některá vylepšení, jako třeba Lightning Network
- Chyba v implementaci může vést k nezjistitelné možnosti inflace

(Ne)anonymita Bitcoinu - řešení

- Implementace Confidential Transactions do Bitcoinu

- Vyžaduje konsensus mezi všemi uživateli – hard fork
- Aby to mělo účinek, muselo by být vynuceno použití pro všechny transakce
- Chyba v implementaci může vést k nezjistitelné možnosti inflace

(Ne)anonymita Bitcoinu - řešení

- Obfuskace pomocí CoinJoin technik

- Použitelné již dnes
- Při správné implementaci jednoduché na použití
- Efektivně rozbíjí linkovatelnost transakcí

Co je CoinJoin

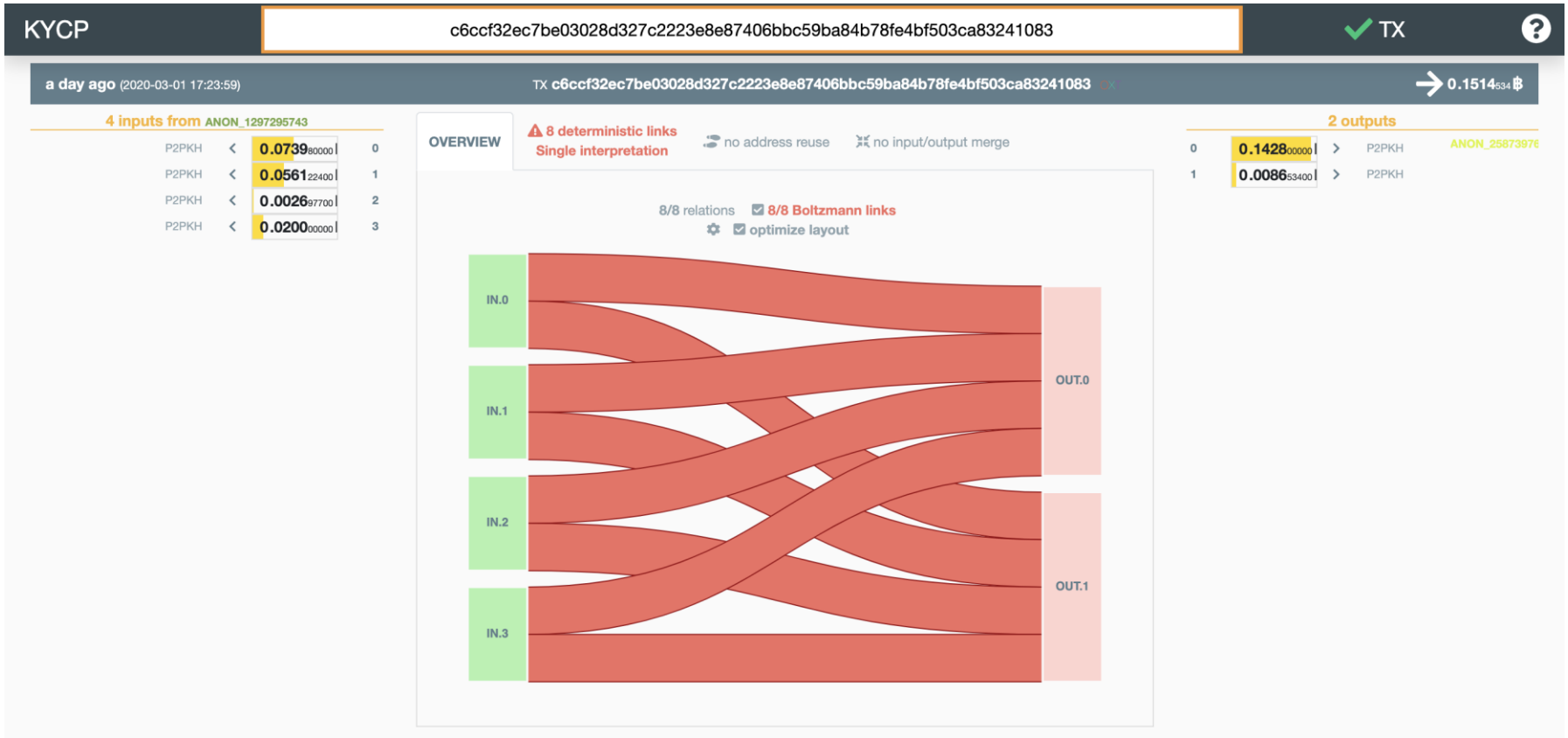
pristav.urza.cz

- CoinJoin je spolupráce několika uživatelů na jedné transakci
- Efektivně rozbíjí existující heuristiky analytických společností
- Při správném použití umožňuje zachování transakčního soukromí

Co je CoinJoin - příklady

pristav.urza.cz

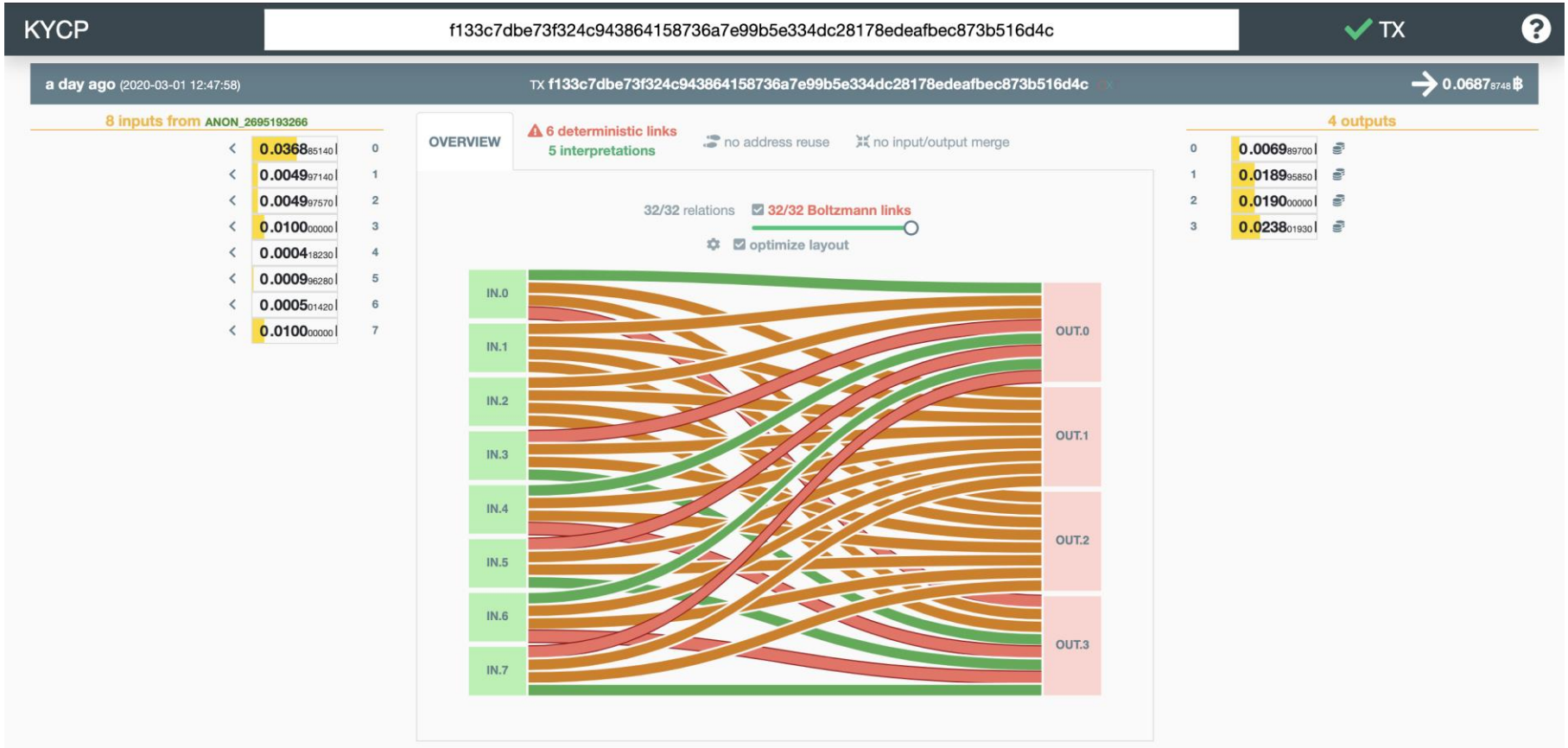
Příklad běžné transakce



Co je CoinJoin - příklady

pristav.urza.cz

Příklad CoinJoin transakce



Co CoinJoin způsobí

- Díky CoinJoinu není možné identifikovat, které výstupy patří ke vstupům
- Nejlepší typ CoinJoinu je takový, který vypadá jako běžná transakce (tzv. PayJoin)
- Lze vytvořit i simulaci CoinJoinu

Jak na CoinJoin dnes

- Ruční vytváření správných CoinJoinů je velmi složité
- Existuje několik peněženek, které jej umí dělat bez důvěry (trustless) – JoinMarket, Wasabi a Samourai Wallet

Aktuální problémy s mixováním

- Burzy nedovolí směňovat bitcoiny, které byly v CoinJoinu
- CoinJoin není řešení všeho (tzv. silver bullet) – při neopatrném zacházení s bitcoiny může stále uživatel odhalit svojí transakční historii
- Naivní implementace může působit důvěryhodně i když není bezpečná

Aktuální problémy s mixováním

- Nebezpečný precedens: burza Binance zablokovala účet uživateli jež vybral Bitcoiny a poslal je mixovat
- Podvodníci z PlusToken scamu byli zatčeni i když použili CoinJoin
- Mluví se o plošné perzekuci všech, co používají CoinJoin

Jak to dělat správně

pristav.urza.cz

- Nemixujte svoje bitcoiny pokud je plánujete opět poslat na burzu

- CoinJoin je ideální používat před/při platbě za služby/zboží

Jak to dělat správně

pristav.urza.cz

- Pokud zmixujete svoje coiny a všechny následně pošlete na jednu adresu, žádné transakční soukromí jste nezískali

- Čím více lidí bude CoinJoin techniky používat, tím méně budou postupy analytických společností relevantní

Co je cíl

pristav.urza.cz

- Právo na transakční soukromí je stejně důležité jako právo na svobodu slova
- Jen s dostatečným soukromím se Bitcoin může stát nejlepšími penězmi
- Jen opravdu svobodné peníze mohou vést ke skutečně svobodným trhům

Závěr

pristav.urza.cz

- Tvrdé peníze jsou zapotřebí k tomu, aby byl trh zdravý
- Aktuální stav spěje k finanční diktatuře
- Bitcoin je naší jedinou možností na spravení rozbitého systému
- Při správném použití CoinJoin technik lze získat transakční soukromí již dnes

Přijďte příště

pristav.urza.cz

- První dubnovou středu bude na apríla přednášet **Dan Steigerwald** o tom, proč je levice ve všem lepší… tedy až na jeden detail – ekonomii.

Středa 1. dubna

v 19 hodin v (de)Centrále