BtcPayServer a crowdfunding

BtcPayServer je služba, pomocí které je možné přijímat bitcoin (*on-chain* i *Lightning Network*) bez jakékoliv třetí strany (stačí si pouze stáhnout software na vlastní *node*). *Crowdfunding* je způsob kolektivního financování, který může eliminovat problém černého pasažéra u veřejných statků pomocí selektivních podnětů (viz).

Téměř všechny crowdundingové platformy jsou založeny na technologii *all or nothing*, spočívající v tom, že když se v dané kampani nevybere požadovaná cílová částka, peníze se vrátí zpět k jednotlivým přispěvatelům. Tím mizí náklady v podobě nedostatku informací spojených s volbou ostatních. V momentě, kdy o úspěšnosti kampaně nerozhoduje pouze Vaše volba přispět, ale i volba ostatních, které neznáte, je z hlediska teorie her dominantní strategií i Shellingovým (ohniskovým) bodem na daný projekt nepřispět. Strategie all or nothing náklady spojené s tímto problémem eliminuje.

Proč je to ale u Bitcoinu problém? Bitcoin jako takový umožnuje vytvářet pouze velmi jednoduché *smart kontrakty* (*multisig* či *timelock* transakce). Dnes není možné ve *spendovacím skriptu* bitcoinové transakce nastavit, že když se v crowdfundingové kampani nevybere dostatek peněz, *sats* se vrátí zpět k lidem, kteří se rozhodli pomoci financovat onen projekt. A smart kontrakty tento problém ani vyřešit nelze, protože nedokáží komunikovat s reálným světem (viz the oracle problem). Kvůli tomu, že mají jednotliví uživatelé v decentralizovaném světě tendenci si vzájemně nedůvěřovat, pokud prospěch z jejich rozhodnutí přímo závisí na rozhodnutích ostatních, vybere se v těchto kampaních méně peněz (*ceteris paribus*) než při stejném způsobu financování s technologií all or nothing.

Řešení? *Multisig*, *escrow*. Tedy vytvoření adresy, z níž bude možné utrácet *UTXOs* pouze s poskytnutím více než jednoho *digitálního podpisu*. *Privátní klíč* k *adrese* by tak měl jak člověk, který se snaží vybrat dostatek finančních zdrojů, každý jeden přispěvatel, tak i samotná platforma (v tomto případě BtcPayServer). Ovšem to jde proti hlavní myšlence BtcPayServeru, tedy *P2P* službě přijímání btc bez jakékoliv třetí strany. Tudy tedy cesta nevede... Dalším možným řešením je v crowdfundingové kampani nastavit větší rozsah jednotlivých cílů, například, pokud se vybere 10 sats, tyto peníze budou využity na X, pokud 100 sats, tak na Y, pokud 1000, tak na Z... A to by skutečně mohlo být řešením toho problému, že se v případě neúspěchu kolektivního financování u BtcPayServer nevrátí bitcoiny zpět na adresy přispěvatelů, a tato *informační asymetrie* demotivuje některé potenciální přispěvatele projektu finančně pomoci. Ale má to jeden háček, ne všechny projekty lze takto škálovat. Pokud potřebuji na realizaci určité činnosti vybrat (minimálně) přesně 100 sats, 10 sats mi v uskutečnění tohoto projektu nepomůže a bylo by žádoucí, kdyby se tyto prostředky vrátily zpět k přispěvatelům.

BtcPayServer je skvělá služba, která výrazně snižuje náklady na přijímání bitcoinu bez jakéhokoliv prostředníka, zkrátka tak, jak byl Bitcoin navržen – P2P digitální peníze. Služba crowdfundingu, kterou BtcPayServer poskytuje však neřeší jeden z hlavních problémů, co crowdfunding řešit má – eliminovat náklady spojené se závislostí rozhodnutí jednotlivce na rozhodnutích ostatních lidí, které nezná a přirozeně nemá sklon k tomu, jim důvěřovat. Řešením může být větší škála různých způsobů realizace projektu, ovšem tu nelze

implementovat u veškerých projektů. BtcPayServer může ale skvěle sloužit k charitativním účelům (viz třeba https://bitcoinsmiles.org/), kde není nutné vybrat jednu konkrétní sumu, s pomocí využití Lightning Network je totiž možné na charitu přispět již od pár satoshi, tedy opravdu malé sumy (v řádech jednotek haléřů).