Blockchain & Lightning network

Michal Švamberg

EurOpen, Žatec, jaro 2018

Základní pojmy o digitálních měnách

Co je bitcoin

Bitcoin is an **experimental** digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses **peer-to-peer** technology to operate with **no central authority**: managing transactions and issuing money are carried out collectively by the network.

zdroj: https://github.com/bitcoin/bitcoin

Satoshi Nakamoto

Popis návrhu: 2008 (první příspěvek v emailové konferenci)
Implementace: 2009 (vydání potřebného SW, spuštění sítě)
Předání komunitě: 2010 (zdrojové kódy, doména bitcoin.org)

Digitální měny

Je hodnota, která náleží konkrétní peněžence (privátnímu klíči).

Adresy jsou odvozeny od veřejných klíčů tohoto privátního klíče.

Pro příjem stačí udat adresu libovolného účtu (veřejného klíče).

Kdo vlastní privátní klíč, může nakládat s prostředky uvedených na účtech (adresách) jež jsou z tohoto klíče vytvořeny.

Pro odeslání je nutné podepsat transakci privátním klíčem, síť kontroluje zda podpis souhlasí s adresou ze které jsou prostředky odeslány.

https://www.systemonline.cz/clanky/blockchain-pro-zacatecniky.htm

Veřejný a privátní klíč

Privátní klíč = peněženka (schováno podpisové právo k účtům)

- nejčastěji soubor
- měl by být šifrovaný
- maximálně chráněný
- zálohovaný!
- kdo jej má, vlastní vše co k němu náleží
- **znalostí klíče se prokazuje vlastnictví hodnoty**

Veřejný klíč - číslo účtu (variabilní symbol k privátnímu klíči)

- vystavuje se pro příjem
- k jednomu privátnímu klíči jich může být vydáno více (doporučuje se)

proof-of-...

Existuje několik přístupů jak bez centrální autority zařídit spolupráci uzlů.

proof-of-work - většina digiálních měn, zájem projevuji investicí do práce (hledání hashe - nákup HW, platby za el. proud, ...), Bitcoin, Litecoin, ...

proof-of-stake - čím déle a více měny držím, tím jsem důvěryhodnější a mám z toho další zisk, BlackCoin, PeerCoin, částečně Ethereum, ...

proof-of-importance - čím více mám transakcí, tím spíše nebudu podvodník, NEM

proof-of-burn, -capacit, -deposit, ...

https://cryptosvet.cz/navod-zacatecnika-rozdil-proof-of-work-proof-of-stake-proof-of-burn-dalsimi-proof-of/

Další využití blockchainu

Blockchain se uplatňuje i v jiných oblastech, ideální jsou takové, kde je zájem mít veřejnou kontrolu.

https://open-music.org/ - správa vlastnických práv (náhrada OSA)

https://ujomusic.com/ - podobné, na Ethereum a další distribuované technologie

https://ipfs.io/ - distribuovaný souborový systém (náhrada HTTP), používá ujomusic

https://www.velox.re/ - katastr nemovitostí (evidence vlastnictví, převody, ...)

https://www.provenance.org/ - sledování potravin

https://www.augur.net/ - předpovědi trhu (Ethereum Smart contracts)

https://arcade.city/ - spolujízda, snaha nahradit centralizovaný Uber

https://www.r3.com/ - konsorcium bankovních institucí (>100) za účelem spolupráce

Nejvážnější rizika digitálních měn

Rizik s kterými se síť musí vypořádat je více, nejznámější jsou

Double spend - pokusit se jedny peníze utratit vícekrát. Například tím, že do sítě odešlu dvě platby současně z jedno účtu.

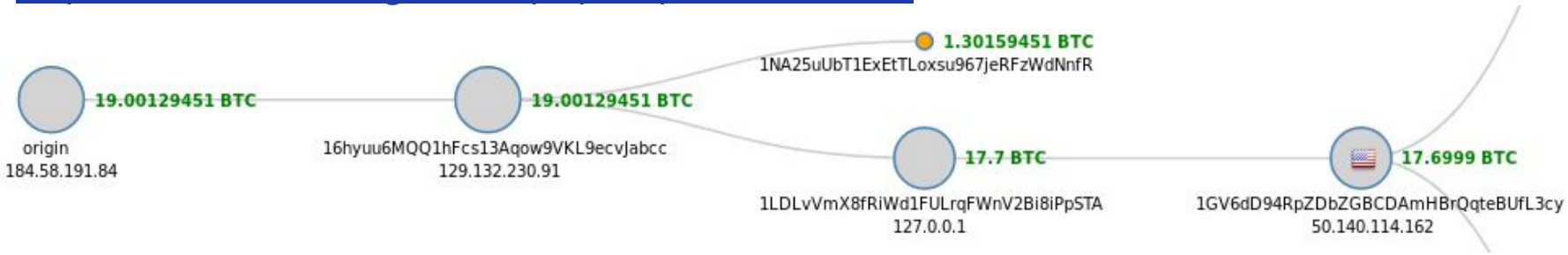
51% podíl - nikdo nesmí mít většinu, vznikla by centralizovaná moc, která by měla možnost podvádět (nelze podepisovat nebo měnit transakce, ale lze některé záměrně vynechat).

Síla kryptoměn je v decentralizaci, proto se skupiny těžařů v minulosti rozdělily. Hodnota kryptoměny, která by byla v takovém ohrožení by stejně klesla.

Chyby se neodpouští

Zabezpečit privátní klíč je prioritou, neexistuje arbitr nebo nadřízená moc

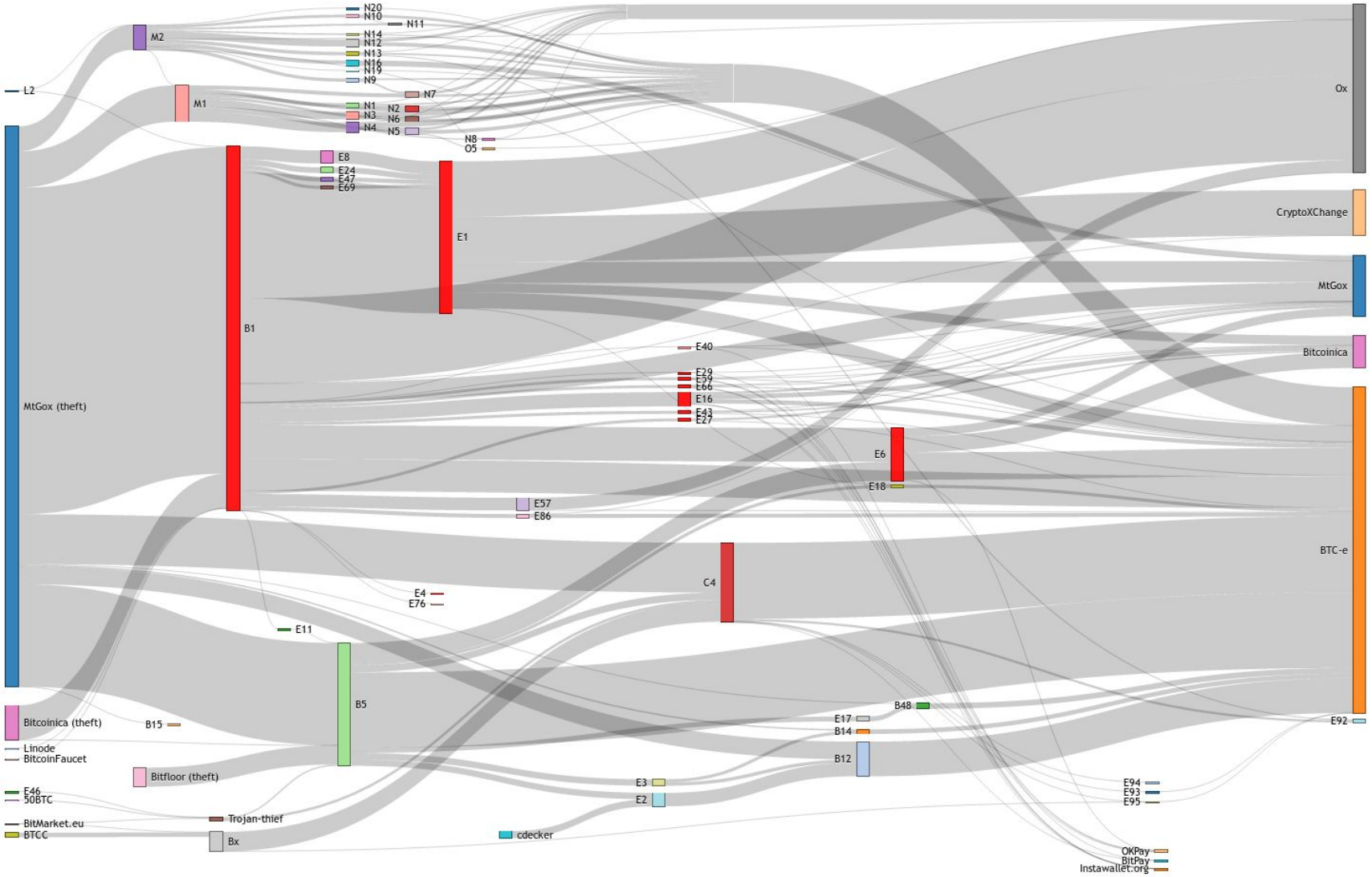
https://bitcointalk.org/index.php?topic=303726.0 - krádež 19BTC



Transakce nelze revokovat, chyby v zadání se nedají napravit.

Zapomenuté heslo k privátnímu klíči = ztráta privátního klíče, lze předejít seedem.

Tok ukradených BTC z burzy Mt. Gox

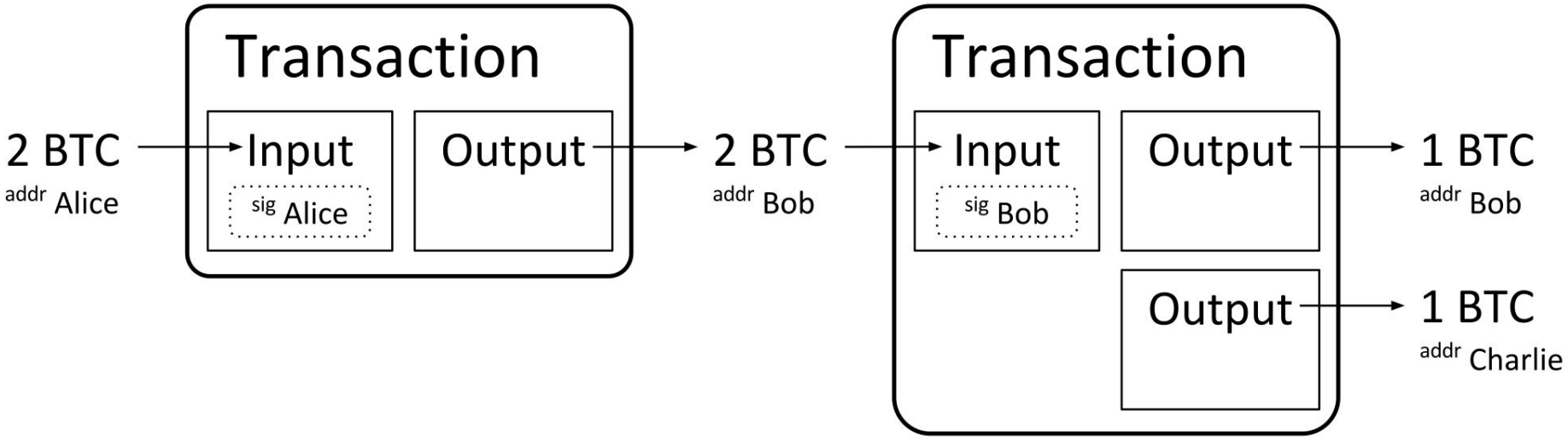


Technický pohled na blockchain bitcoinu aneb základní pojmy detailněji

Adresa v Bitcoinu

Prakticky se jedná o hash veřejného klíče:

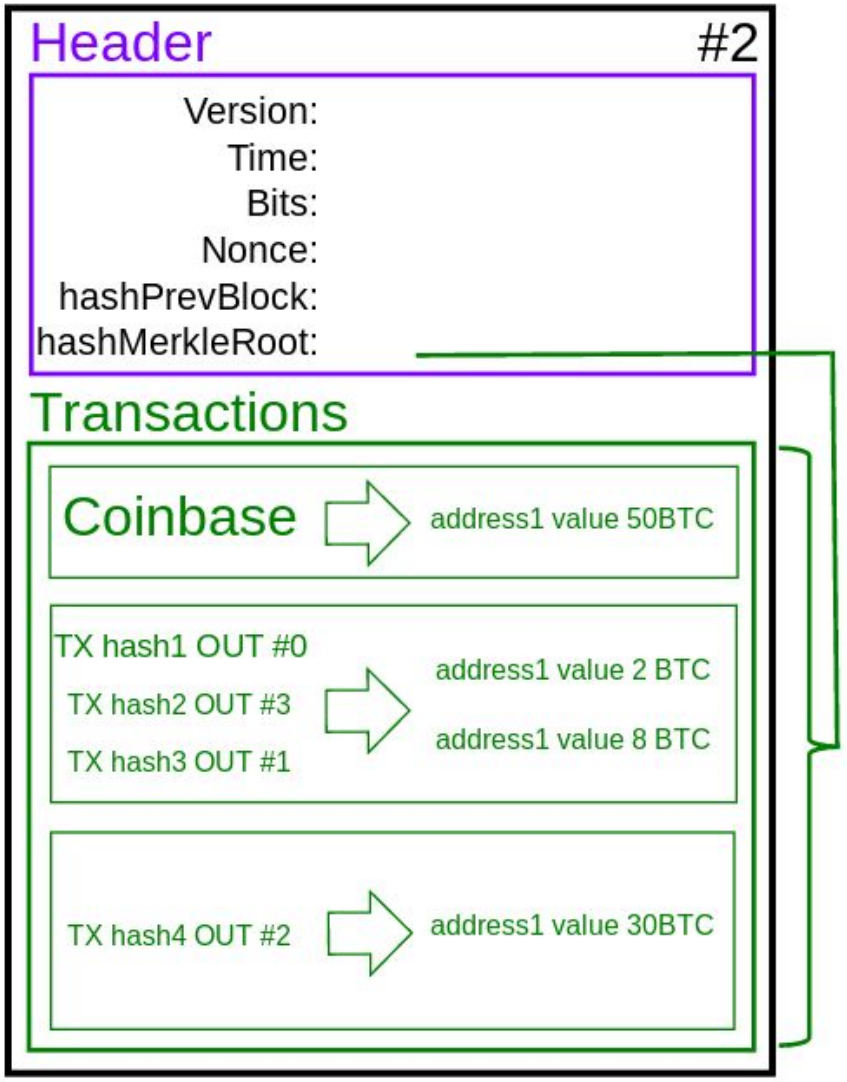
```
$version = '1';
$keyHash = $version . ripemd160(sha256($pub_key));
$checksum = first4bytes(sha256(sha256($keyHash)));
$address = base58encode($keyHash . $checksum);
```



Block

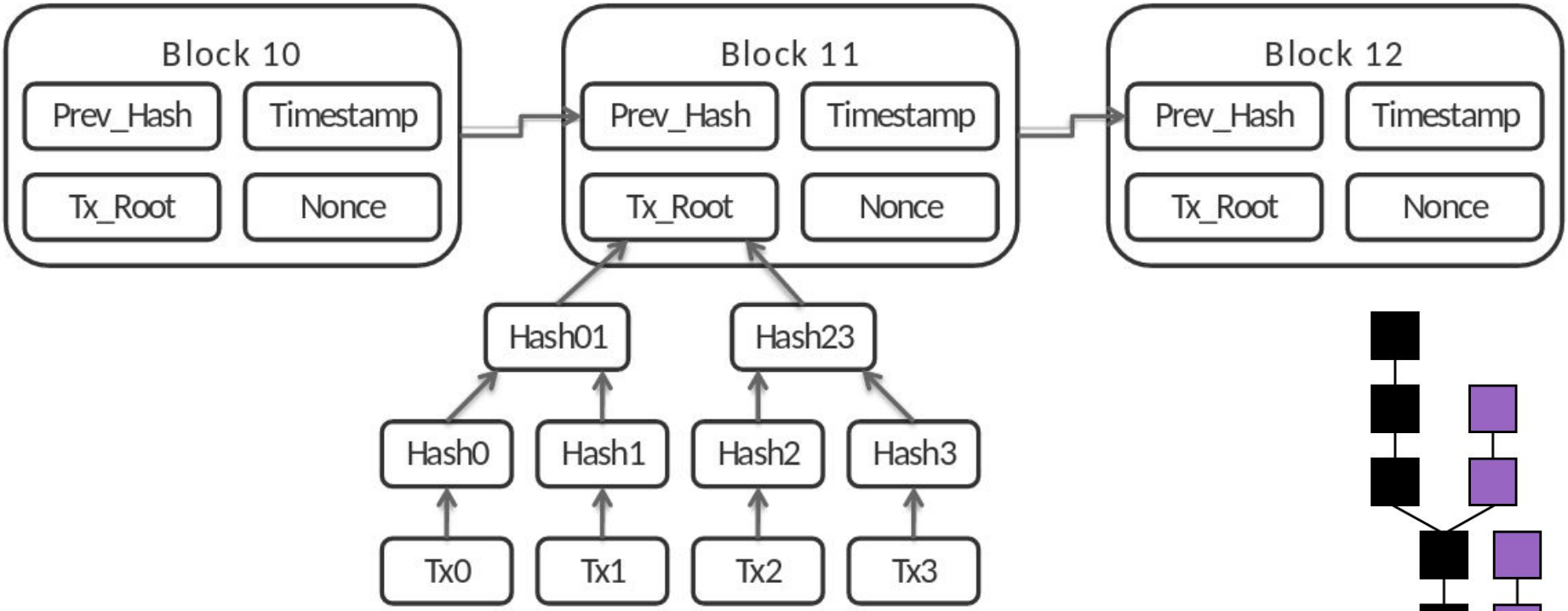
Informační jednotka se záznamem transakcí uložených v hashovém stromu (MerkleRoot).

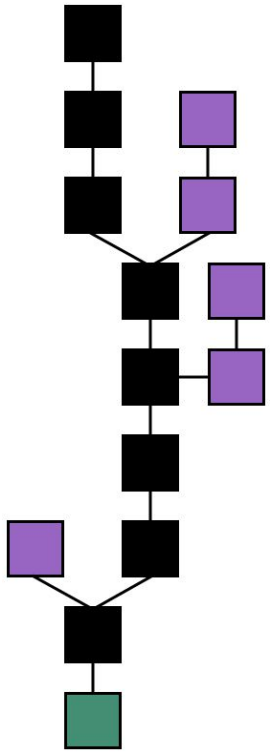
Mezi transakcemi je odměna těžaři za nalezení správné Nonce => do oběhu se uvolní nové bitcoiny.



https://www.lupa.cz/clanky/jak-porozumet-blockchainu-v-deseti-minutach-aneb-jak-funguje-technicky-a-k-cemu-je/

Chain of blocks = blockchain





Těžba

Těžař hledá vhodný tvar hashe záhlaví bloku, tak aby vyhovoval “tvarem”. Za to je odměněn nový bitcoiny a poplatky z transakcí na uvedenou adresu.

```
$version = '1';
$prevBlockHash = '00000000000008a3a41b85b8b29ad444 … eab02cd81' );
$rootHash = '2b12fcf1b0928f797d71e950e71ae42b91e8bdb23047 … ffc2b620e3' );
$time = '1305998791'; # Sat May 21 2011 19:26:31 UTC+0200 (CEST)
$bits = '440711666'; # obtiznost
$nonce = '2504433986'; # volitelná oblast (32 bytů)
$pass1 = sha256($version . $prevBlockHash . $rootHash . $time . $bits .
$nonce);
$finalHash = sha256($pass1); # vysledný hash (32 bytů)
```

Chybí zde ještě některé operace, jako je převod hexa čísel do binárních, otočení pořadí a převod na littleEndian formát. Důležité je, že samotné transakce jsou v hashi zastoupeny hashem kořene stromu hashů.

Těžař si strom transakcí může vybrat podle sebe, nejčastěji vybírá podle poměru výše poplatku vůči velikosti transakce. Celý blok je limitován 1MB v případě Bitcoinu.

Odměna

U bitcoinu tzv. halving (půlení), celkem bude vytvořeno 21M BTC, odměna se snižuje každé 4 roky na polovinu (jen odhad, aktualně se doluje o cca 9% rychleji):

2009: block 0: odměna 50BTC

2013: block 21.000: odměna 25BTC (vytěženo 50% zbývajících bitcoinů)

2016: block 42.000: odměna 12,5BTC (vytěženo 75%)

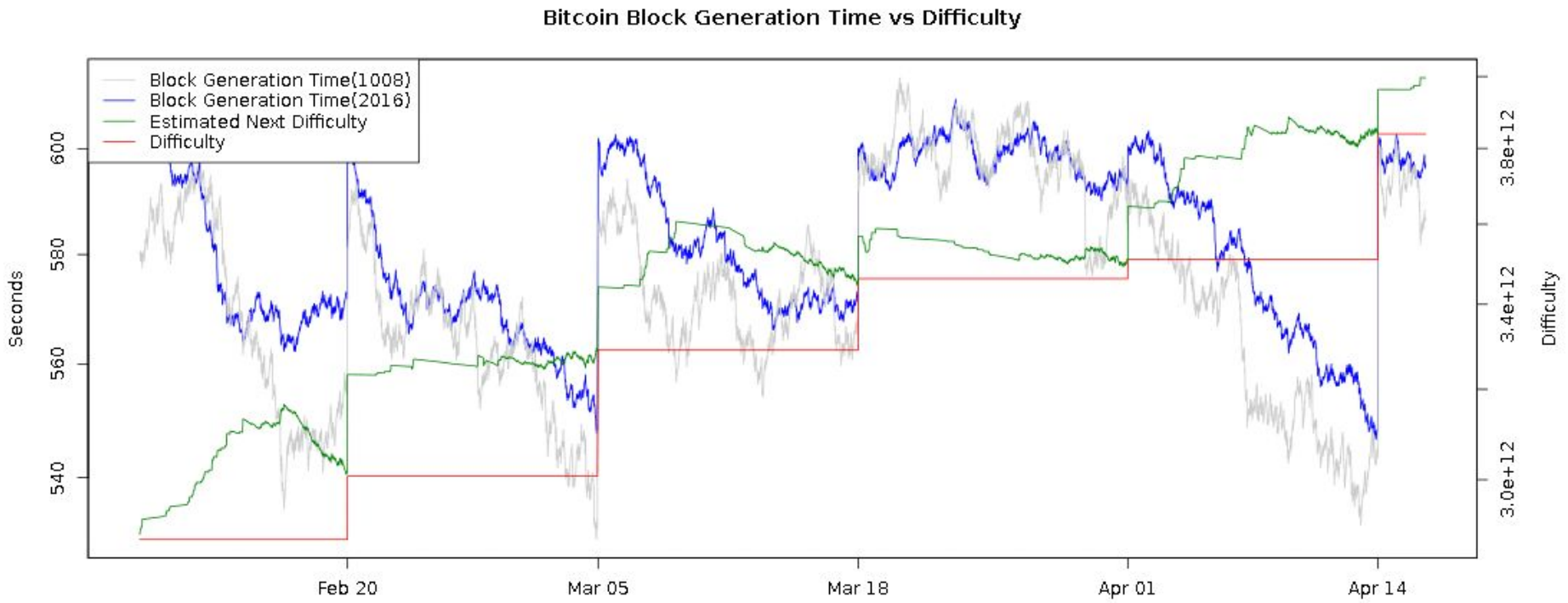
...

2136: block 6.720.000: odměna 144 Satoshi (zbývá vytěžit 0,00021BTC)

2140: block 6.930.000: odměna 0BTC (vytěženo 100%)

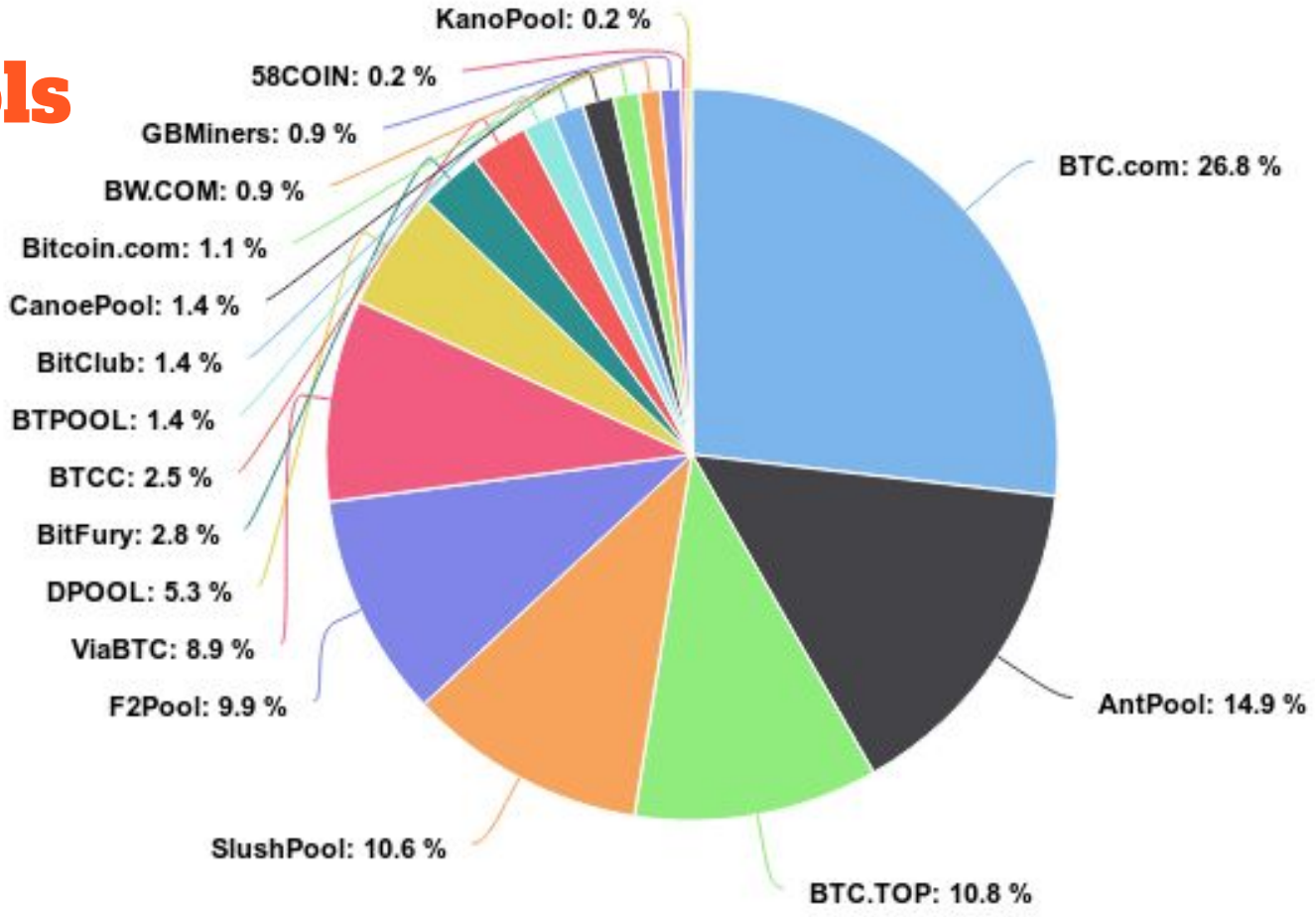
https://docs.google.com/spreadsheets/d/12tR_9WrY0Hj4AQLoJYj9EDBzfA38XIVLQSOOOVePNm0/edit#gid=0

Obtížnost



Upravuje nároky na výsledný tvar hashe tak, aby průměrně vznikl 1 blok za 10 minut (600s). Bitcoin to dělá 1x za 14 dnů (2016 bloků). Určuje kolikrát je náročnější najít správný hash než při obtížnosti 1, kdy je každý hash správný. Průměrně je třeba na jeden blok zkontrolovat *obtížnost* * 2^{32} hashů.

Mining pools



- Riziko 51%
- Důvěra
- Poplatky poolu

Sdružení těžařů do skupin a dělení odměny dle poskytnutého výkonu do poolu. První těžební pool je z česka - SlushPool.

https://en.bitcoin.it/wiki/Comparison_of_mining_pools

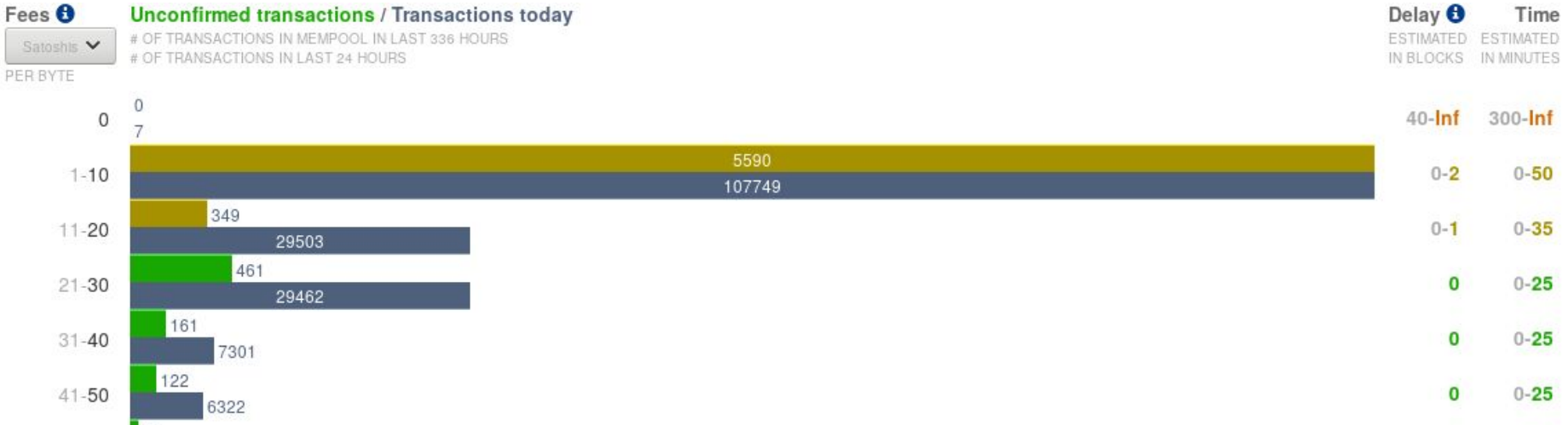
Transakce s nízkým poplatkem

Transakce zůstane v mempoolu dokud se nestane:

- expirace: po 72hod výmaz z mempool => návrat peněz, nesmí být rebroadcast
- bude zařazena těžařem a potvrzena sítí ve vytěženém bloku
- jiná magie: volba Replace-by-Fee (RBF) - navýšení poplatku
- budete mít štěstí (zařazen do bloku na základě zamezení double spend)

https://bitcoinfees.earn.com/ - odhad ceny poplatků

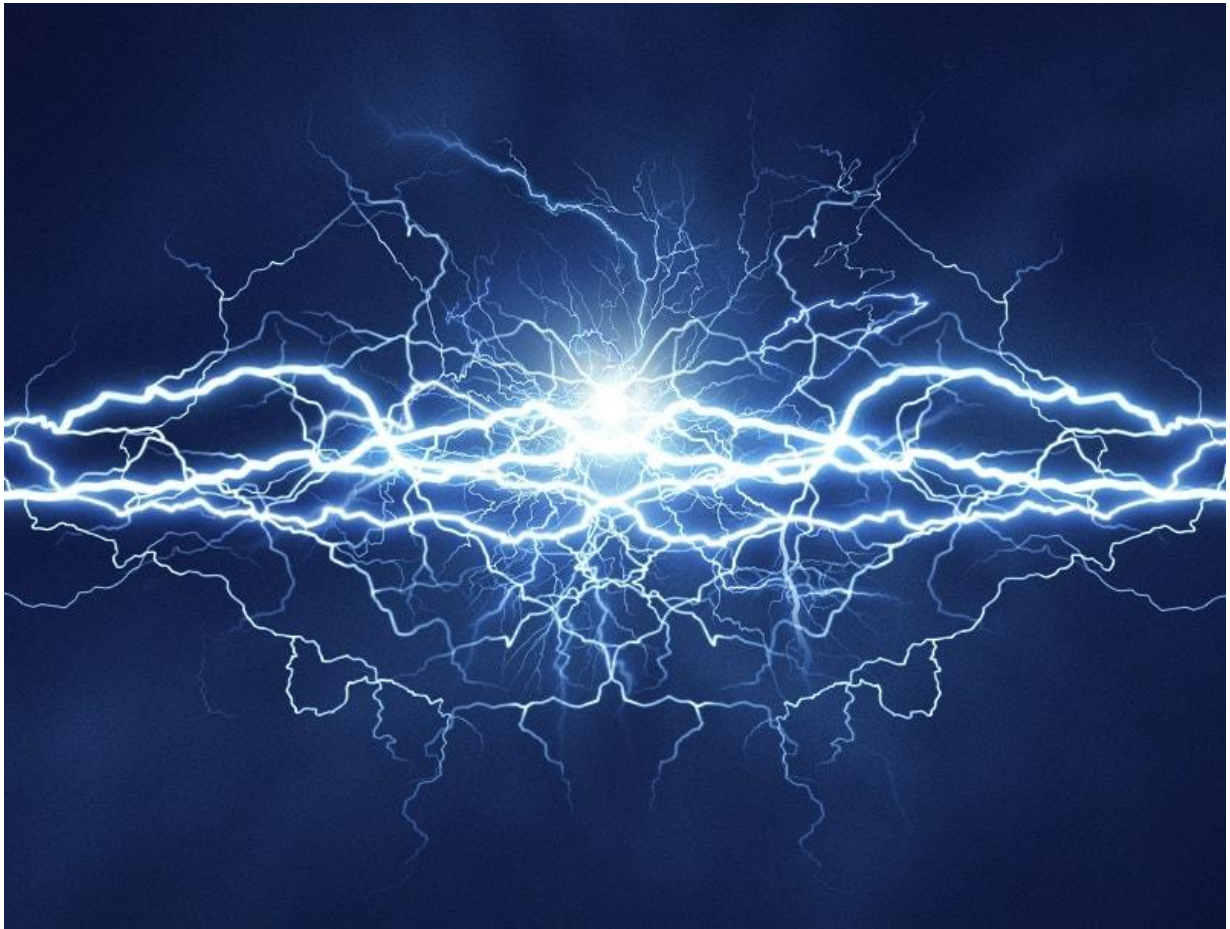
https://blockchain.info/unconfirmed-transactions - přicházející transakce



Lightning Network
nad
Blockchainem Bitcoinu

Lightning Network

Lightning is a decentralized network using smart contract functionality in the blockchain to enable instant payments across a network of participants.



Problémy k řešení

Okamžité platby bez čekání na potvrzení v blockchainu.

Zvýšení kapacita blockchainu (nyní cca 7 trasakcí za vteřinu).

Výše poplatků u bitcoinových trasakcí (přímo zapisovaných do blockchainu)

Možnost platit mezi blockchainy (litecoin - bitcoin) skrze zprostředkovatele.

Smart contracts

Jde o dvoustranné (peer-to-peer) dohody, které budou vykonány na základě okolností.

U automatu se očekává jak se bude chovat:

- vydá zboží a ponechá si peníze
- nevydá zboží a vrátí vložené peníze

Ale dohodu nemáte s automatem, máte ji s provozovatelem, automat je jen technické zařízení. Stejně se chovají i chytré kontrakty (dohody). Provádou se podle toho, jak se chovají obě strany. Přitom každa ze stran má nějakou páku, jak si vynutit, aby ji druhá strana nepodvedla. Jako arbitr zde vystupuje blockchain.

Základy Lightning Network

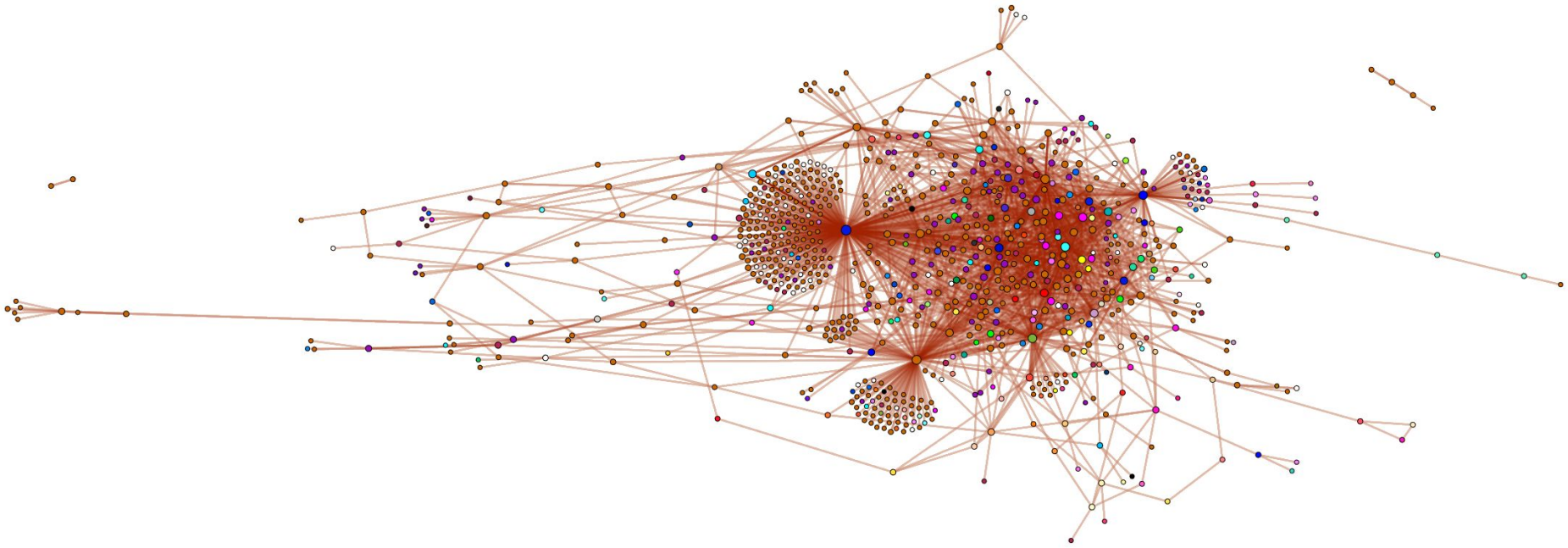
- existence nezveřejněných transakcí
- ochrana před vícenásobným utrácením
- podpora více podpisů pro jednu transakci (multisignature)
- časové zámky pro jednotlivé transakce

Otevření platebního kanálu se provede převodem vlastních prostředků na společný účet - složí se depozit. Ze společného účtu (multisign adresa) lze čerpat prostředky jen, pokud transakci podepíší obě strany.

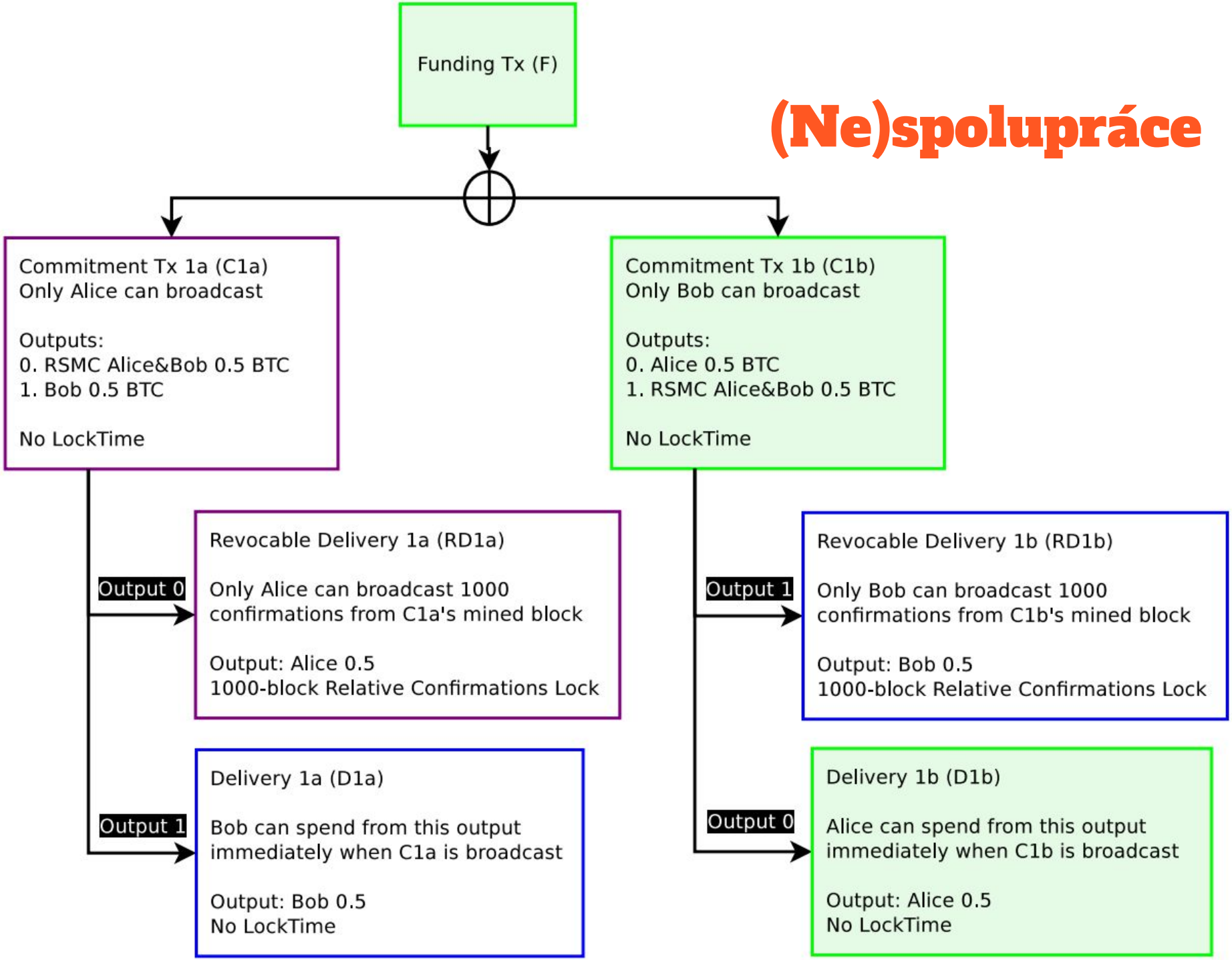
Obě strany si vymění částečně podepsané transakce, tak aby prostředky bylo možné vrátit na původní adresy pokud druhá strana přestane spolupracovat nebo bude chtít podvádět.

V případě platby si částečně podepsané transakce nahradí novými. Uzavření kanálu se provede zveřejněním podepsané transakce do blockchainu.

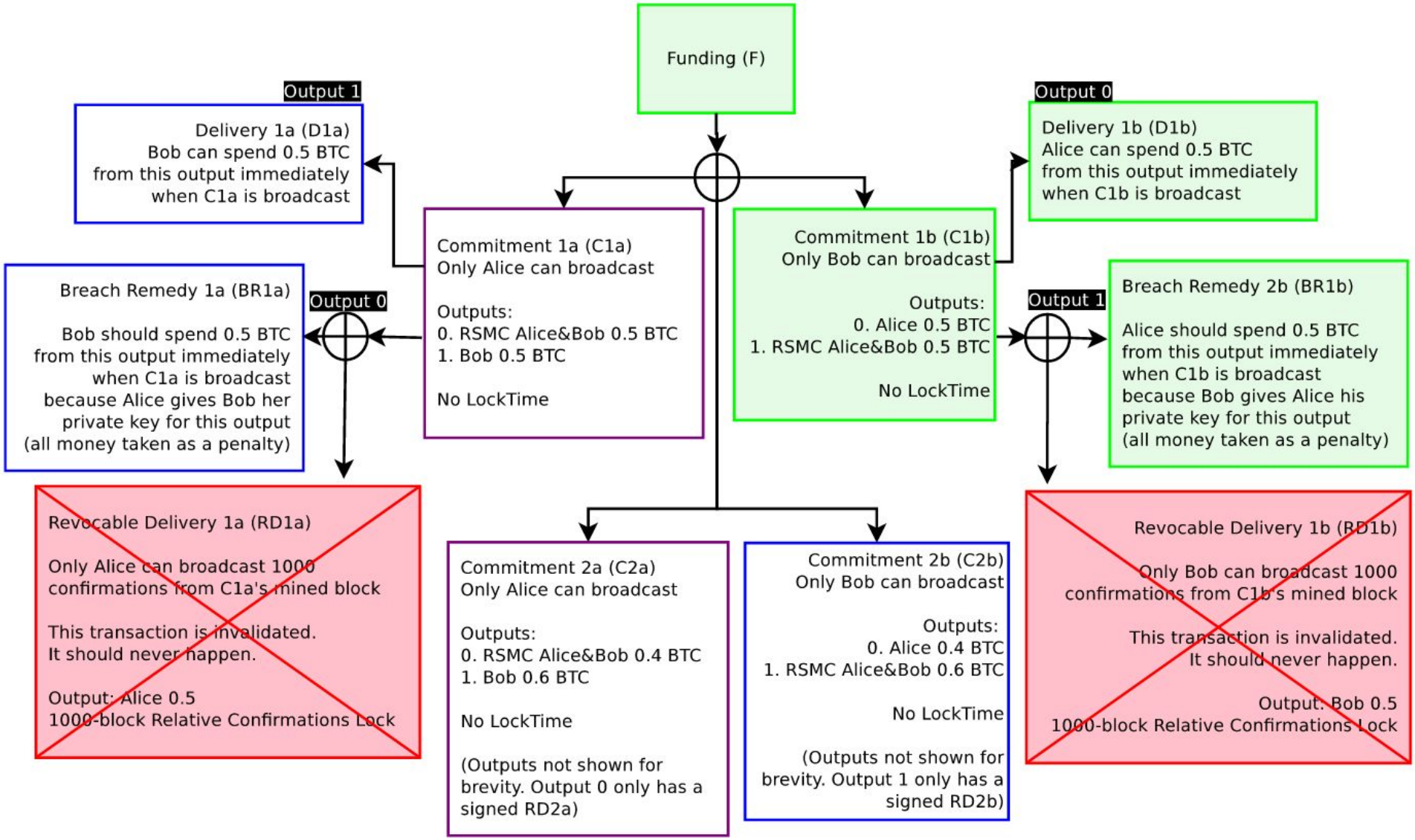
Vizualizace Lightning Network (testnet)



(Ne)spolupráce



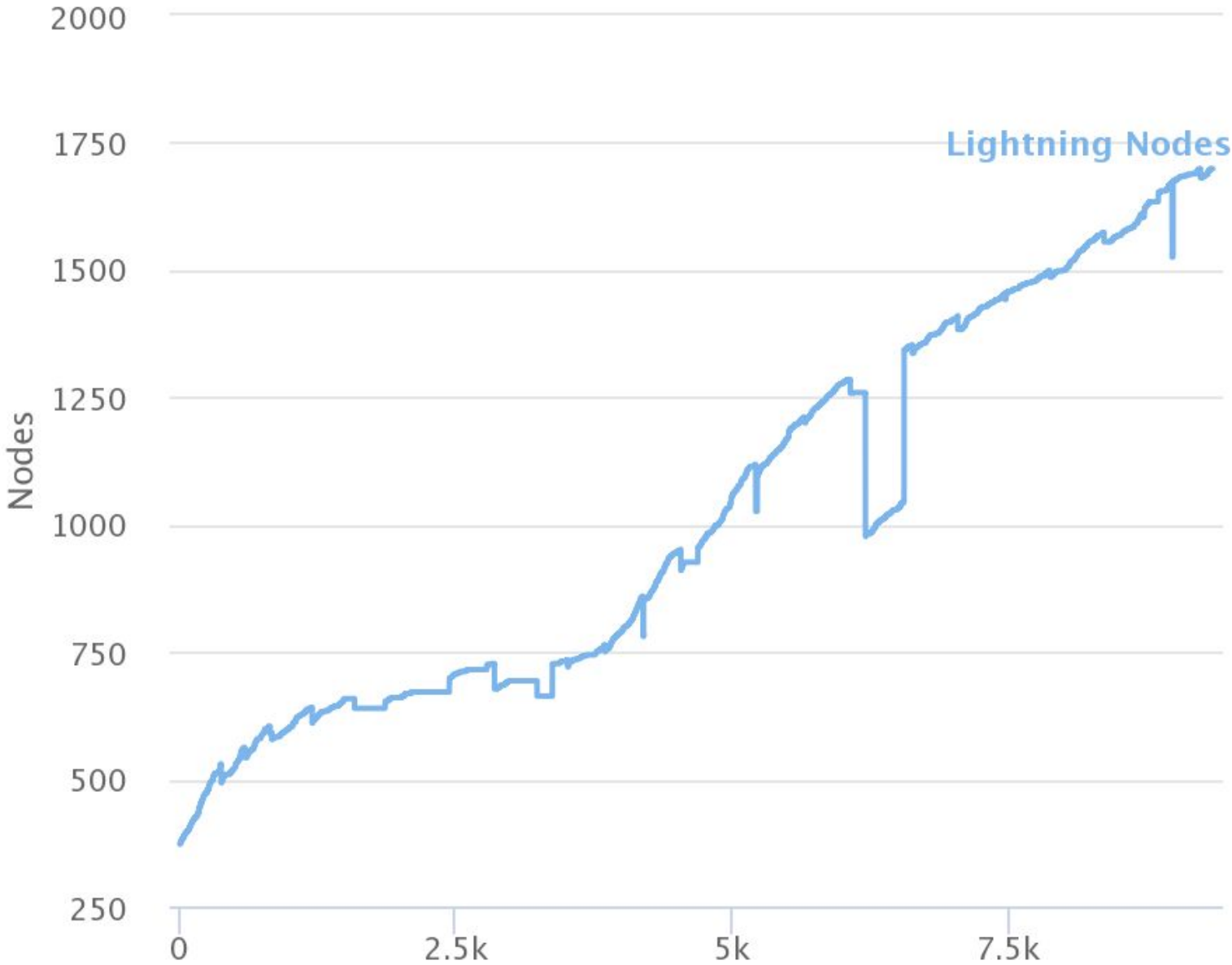
Zveřejnění staré dohody = trest



Stav k 12.5.2018

uzlů: 1699

kanálů: 15304



Čas na otázky a odpovědi