BITCOIN WHITEPAPER

BLOCKCHAIN
SLOVAKIA

Autor: Satoshi Nakamoto | 31.10.2008

Prvý slovenský preklad | Preložil: Andrej Andil | Spracovalo: Blockchain Slovakia, o.z.

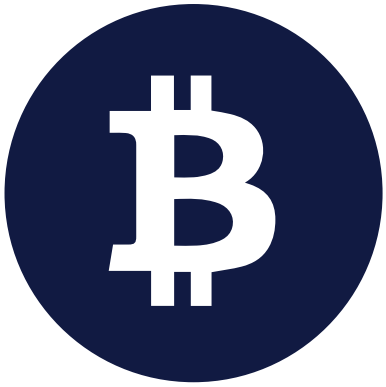
Bitcoin

Často označovaný ako digitálne zlato, Bitcoin postupne preniká do našich každodenných životov. Väčšina čitateľov bude vedieť, že Bitcoin predstavuje akýsi počin vyvoriť digitálne peniaze. Avšak niektorých prekvapí, že Bitcoin nie je prvý takýto počin, avšak je prvý, ktorý ešte nezlyhal a nikto ho nezastavil.

Bitcoin vznikol v roku 2009 po finančnej kríze ako odpoveď na neschopnosť centralizovaného systému ochrániť naše financie. Aj preto sa dodnes neznámy autor, Satoshi Nakamoto, rozhodol zapečatiť názov článku z britského denníka "The Times", do prvého bloku, ktorý započal bitcoinový reťazec. Názov tohto článku bol: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks", v preklade: "The Times 03.01.2009 Kancelár na pokraji druhej záchrannej pôžičky bankám". Vtedy začala nová epocha kryptografických inštrumentov na výmenu hodnôt, známych ako kryptomeny. Blok ktorý túto referenciu obsahuje, poznáme pod označením ako blok 0 alebo tkz. "Genesis" blok, čo vo voľnom preklade znamená pôvodný blok. Každým pokorením predošlej najvyššej ceny, Bitcoin získava na popularite a oslovuje nových záujemcov a predošlých skeptikov. Avšak cena v konečnom dôsledku je iba ukazovateľ, ktorý nás má silu vtiahnuť do kryptosveta, a kam sa potom vyberieme je už na nás.

My v Blockchain Slovakia veríme, že „investícia do vedomostí vypláca najlepšie dividendy" (Benjamin Franklin), a keďže by tu blockchain (reťaz blokov) bez Bitcoinu nebol, aspoň nie v takej forme v akej ho poznáme, rozhodli sme sa sprostredkovať vám historicky prvý kompletný slovenský preklad tohto kľúčového dokumentu. Dokumentu, ktorý to celé započal, bez ktorého by tu Blockchain Slovakia pravdepodobne nebol, a vy ste pravdepodobne žili finančne nezaujímavým životom do ďalšej finančnej krízy.

* vysvetlivky jednotlivých pojmov nájdete na konci článku



Bitcoin:

Elektronický peňažný systém na báze rovný s rovným
(A Peer-to-Peer Electronic Cash System)
Satoshi Nakamoto
www.bitcoin.org

Abstrakt. Verzia elektronických peňazí, ktorá operuje v sieti horizontálne postavených účastníkov (peer-to-peer = rovný s rovným) by umožnila odosielanie on-line platieb priamo medzi stranami, bez prietoku cez finančnú inštitúciu. Digitálne podpisy poskytujú čiastočné riešenie problému, avšak kým je dôveryhodná tretia strana hlavným aktérom v zabraňovaní dvojitej útraty (double-spending), prínosy budú stále mizivé.

Navrhujeme riešenie problému dvojitej útraty pomocou siete s horizontálne postavenými uchádzačmi, na ktorých budeme ďalej odkazovať ako rovný s rovným (peer-to-peer). Sieť označí každú transkakciu "časovou pečiatkou" (timestamp), tak že ich vloží do prebiehajúceho reťazca (chain) pomocou dôkazu práce (Proof of Work), založenom na jej transformácii do zašifrovaného kódu (hash-based). Tým vytvoria záznam, ktorý je nemenný bez zopakovania dôkazu práce (Proof of Work). Najdlhší reťazec slúži nielen ako dôkaz o postupnosti udalostí, ktorých bol reťazec svedkom, ale aj ako dôkaz, že pochádza z najväčšieho množstva výpočtovej sily v sieti (CPU power). Pokiaľ je väčšina výpočtovej sily riadená uzlami (nodes), ktoré nespolupracujú, aby úmyselne zaútočili na sieť, vytvoria najdlhší reťazec (chain) a predbehnú útočníkov. Samotná sieť vyžaduje minimálnu štruktúru. Správy sú vysielané na základe najlepšieho úsilia uzlov, ktoré môžu odísť a pripojiť sa k sieti podľa vlastného uváženia. Pri pripojení príjmu najdlhší reťazec dôkazov o práci (Proof of Work), ako dôkaz sledu udalostí počas ich absencie.

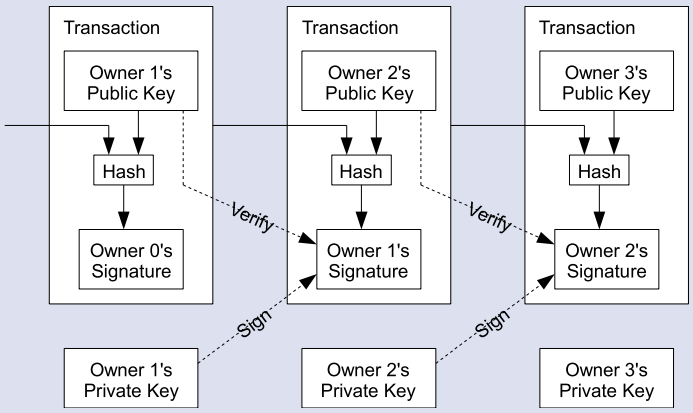
1. Úvod

Obchodovanie na internete sa takmer výlučne spolieha na finančné inštitúcie, ktoré slúžia pri spracovaní elektronických platieb ako dôveryhodné tretie strany. Zatiaľ čo systém funguje dostatočne dobre pre väčšinu transakcií, stále trpí sprievodne slabými stránkami modelu založeného na dôvere. Úplne nezvratné transakcie nie sú možnosť, pretože finančné inštitúcie sa nemôžu vyhnúť sprostredkovaniu sporov. Náklady na sprostredkovanie zvyšujú transakčné náklady a limitujú minimálnu praktickú veľkosť transakcií, čím zamedzujú možnosti vzniku malých nepravidelných transakcií, avšak strata schopnosti uskutočniť nezvratné platby za nezvratné služby má ešte širšie implikácie. Možnosť zvrátenia rozširuje potrebu dôvery. Obchodníci musia byť obozretní voči svojim zákazníkom, a požadovať od nich viac informácií než by bolo ináč nutné. Určité percento podvodov sa dokonca považuje za nevyhnutné. Týmto nákladom a neistotám pri platbách sa dá vyhnúť pri používaní fyzickej meny (FIAT), avšak dnes neexistuje mechanizmus na uskutočnenie platieb cez komunikačný kanál bez dôveryhodnej strany.

Čo je potrebné, je elektronický platobný systém založený na kryptografickom dôkaze namiesto dôvery, umožňujúc akýmkoľvek dvom stranám obchodovať priamo medzi sebou bez potreby dôveryhodnej tretej strany. Transakcie, ktoré sú výpočtovo nepraktické na zvrátenie by chránili predajcov pred podvodmi, a bežné mechanizmy podmienečných zmlúv (escrow) by sa mohli ľahko implementovať na ochranu kupujúcich. V tejto práci, navrhujeme riešenie problému dvojitej útraty (double-spending) pomocou využitia distribuovaného serveru s časovými pečiatkami, fungujúceho na báze rovný s rovným s cieľom vytvorenia výpočtového dôkazu o chronologickom poradí transakcií. Systém je bezpečný, pokiaľ čestné uzly (honest nodes) kolektívne vlastnia väčší výkon výpočtovej sily, ako ktorákoľvek spolupracujúca zlomyselná nepriateľská skupina uzlov.

2. Transakcie

My definujeme elektronickú mincu ako reťazec digitálnych podpisov. Každý majiteľ prevedie mincu na ďalšieho tým, že digitálne podpíše hash z predchádzajúcej transakcie spolu s verejným kľúčom ďalšieho vlastníka, a pridá ho na koniec mince. Príjemca platby môže overiť podpisy, a tým overiť reťazec vlastníctva.

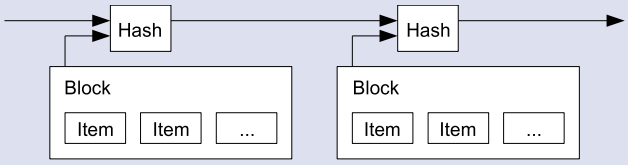


Problémom je, že si príjemca nemôže overiť, či jeden z majiteľov nezaplatil dvakrát (double-spend) jednou mincou. Bežným riešením je predstaviť dôveryhodnú centrálnu autoritu alebo mincovňu, ktorá kontroluje každú transakciu kvôli dvojnásobnej útrate (double-spend). Po každej transakcii sa musí minca vrátiť mincovni, aby vydala novú mincu, a iba mince vydané priamo z mincovne majú dôveru, že nebudú dvojnásobne utratené. Problém s týmto riešením spočíva v tom, že osud celého tohto peňažného systému závisí od spoločnosti, ktorá prevádzkuje mincovňu, pričom každá transakcia musí prechádzať cez ňu, rovnako ako v prípade banky.

Potrebujeme spôsob pre príjemcu, ktorý by mu umožňoval vedieť, že predchádzajúci vlastníci nepodpísali žiadne predchádzajúce transakcie. Pre naše účely je najskoršia transakcia tá, ktorá sa počíta, takže nás nezaujímajú neskoršie pokusy o dvojnásobnú útratu (double-spend). Jediný spôsob potvrdenia absencie transakcie je poznať všetky transakcie. V mincovom modeli si mincovňa bola vedomá všetkých transakcií a rozhodla o ich chronologickom poradí. Na dosiahnutie tohto stavu bez dôveryhodnej strany, musia byť transakcie verejne oznámené [1], a taktiež je potreba systému pre účastníkov, ktorý im umožní súhlasiť s históriou a chronologickým poradím transakcií. Príjemca potrebuje dôkaz, že v čase každej transakcie väčšina uzlov súhlasí s tým, že bola prijatá ako prvá.

3. Server s časovou pečiatkou (Timestamp server)

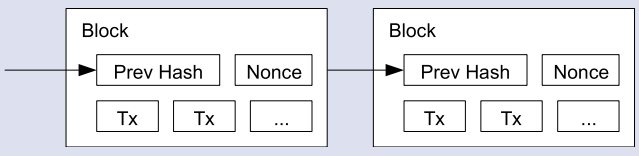
Riešenie, ktoré navrhujeme, má počiatok v servere s časovou pečiatkou. Tento server funguje tak, že odoberá hash bloku položiek, ktorý má byť časovo označený a široko publikovaný, napríklad v novinách alebo v Usenet oznámení [2-5]. Časová pečiatka dokazuje, že údaje museli existovať v tom čase, na to aby sa dostali do hashu. Každá časová pečiatka obsahuje predchádzajúcu časovú pečiatku vo svojom hashi, formujúc reťazec, kde každá ďalšia časová pečiatka zosilňuje predošlé.



4. Dôkaz o práci (Proof-of-Work)

Na implementáciu distribuovaného servera s časovými pečiatkami na báze rovný s rovným, budeme musieť použíť systém dôkazu o práci skôr podobný Hashcashu [6] od Adama Backa, než novinovým alebo Usenet príspevkom. Dôkaz o práci zahŕňa hľadanie hodnoty, ktorá pri zadaní do hashovacej funkcie, ako napríklad pri SHA-256, začína s počtom nulových bitov. Priemerná požadovaná práca je exponenciálna v počte požadovaných nulových bitov, a môže byť overená vykonaním jedného hashu.

Implementáciu dokladu o práci v našej sieti s časovou pečiatkou vykonáme pripočítaním tzv. Nonce v bloku, dokým sa nenájde hodnota, ktorá pridáva hashu bloku požadované nulové bity. Akonáhle sa vynaloží výpočtová sila na uspokojenie dôkazu o práci, blok nemožno zmeniť bez opätovného vykonania tejto práce. Keďže neskoršie bloky sú reťazovo naviazané na predošlé, práca na zmenu bloku by zahŕňala opätovné prepracovanie všetkých neskorších blokov.



Dôkaz o práci taktiež rieši problém spojený s určením zastúpenia v systéme rozhodovania väčšiny. Ak by väčšina bola na jednej IP-adrese-jednom-hlase, každý kto by sa vedel rozvrhnúť na mnoho IP adries by mohol tento systém rozvrátiť. Dôkaz o práci je v podstate jedna-procesná sila-jeden-hlas (one-CPU-one-vote). Rozhodnutie väčšiny predstavuje najdlhší reťazec, pretože naňho bolo vynaložené najväčšie úsilie spojené s dôkazom o práci. Ak je väčšina výkonu procesnej sily (CPU) riadená čestnými uzlami, čestný reťazec bude rásť najrýchlejšie a predčí všetky konkurenčné reťazce. Pre upravenie minulého bloku by musel útočník opäť vykonať dôkaz o práci toho bloku, ako aj všetkých blokov po ňom, až kým nevyrovná a nepredčí reťazec, na ktorom pracujú čestné uzly. Ukážeme neskôr, že pravdepodobnosť útočníka dobehnúť čestné uzly sa exponenciálne zmenšuje s každým pridaným blokom. Aby sa kompenzovala časom zvyšujúca sa rýchlosť hardvéru a meniaci sa záujem na prevádzkovaní uzlov, náročnosť dôkazu práce je určená kĺzavým priemerom zameraným na priemerný počet blokov za hodinu. Ak sú generované príliš rýchlo, dochádza k zvyšovaniu náročnosti.

5. Sieť

Kroky na spustenie siete sú nasledovné:

1) Nové transakcie sa vysielajú do všetkých uzlov.
2) Každý uzol zhromažďuje nové transakcie do bloku.
3) Každý uzol pracuje na nájdení náročného dôkazu o práci pre jeho blok.
4) Keď uzol nájde dôkaz o práci, vysiela blok do všetkých uzlov.
5) Uzly prijmú blok iba vtedy, ak sú všetky transakcie v ňom platné a nie sú už uhradené.
6) Uzly vyjadrujú prijatie bloku tým, že pri práci na vytvorení ďalšieho bloku v reťazci použijú hash prijatého bloku ako predchádzajúci hash/referenciu.

Uzly vždy považujú najdlhší reťazec za ten správny a budú pokračovať v práci na jeho predlžovaní. Ak dva uzly vysielajú súčasne rôzne verzie ďalšieho bloku, niektoré uzly ich môžu obdržať v rôznej časovej postupnosti. V takom prípade pracujú na prvom, ktorý dostali, ale uchovajú si druhú vetvu (s druhým blokom) v prípade, že bude nakoniec dlhšia. Nerozhodnoť sa zlomí, keď

sa nájde ďalší dôkaz o práci a jedna vetva sa stane dlhšou; uzly, ktoré pracovali na druhej vetve, sa potom prepnú na dlhšiu. Nové vysielania transakcií nemusí nevyhnutne dosiahnuť všetky uzly. Pokiaľ dosiahnú veľa uzlov, dostanú sa do bloku predtým. Vysielanie blokov je tiež tolerantné k nedoručeným správam. Ak uzol blok neobdrží, uvedomí si túto medzeru pri obdržaní ďalšieho bloku, a vyžiada si správu o ňom správu.

6. Motivácia

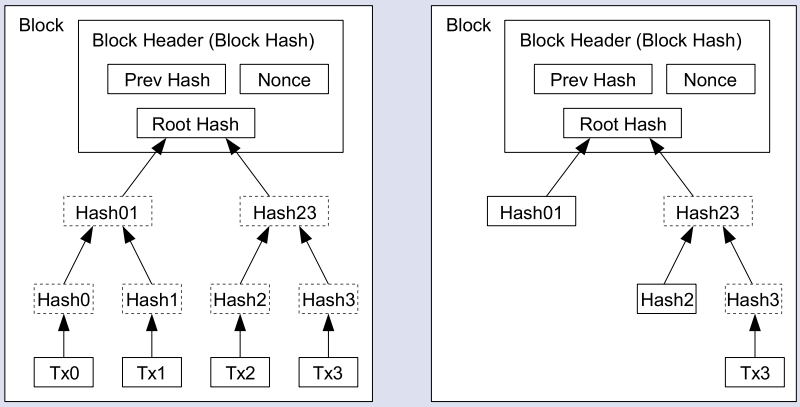
Prvá transakcia v bloku je spravidla špeciálna, pretože začína novou mincou, ktorú vlastní tvorca bloku. To motivuje uzly na podporu siete a poskytuje spôsob, ako novovyťažené mince vpustiť do obehu, nakoľko neexistuje centrálny orgán na ich vydávanie. Stály prírastok konštantného množstva nových mincí je analogický k ťažbe zlata, kde baníci vynakladajú zdroje na vyťaženie a vpustenie zlata do obehu. V našom prípade sú týmito vynaloženými zdrojmi čas a elektrina venovaná výpočtom (hashov).

Stimuly môžu byť tiež financované transakčnými poplatkami. Ak je výstupná hodnota transakcie menšia ako jej vstupná hodnota, rozdielom je transakčný poplatok. Ten sa pripočíta k stimulačnej hodnote bloku, v ktorom sa táto transakcia nachádza. Akonáhle vopred určený počet mincí vstúpi do obehu, transakčné poplatky sa stanú jediným stimulom a inflácia sa vytratí.

Tento podnet motivuje uzly nepodvádzať. Ak by bol chamtivý útočník schopný zhromaždiť viac výpočtovej sily než všetky čestné uzly, musel by si vybrať či podvedie ľudí zvrátením svojich platieb alebo vytvorením nových mincí. Potencionálny útočník by mal pochopiť, že je preňho profitabilnejšie hrať podľa pravidiel. Pravidiel, ktoré mu uprednostňujú viac mincí ako všetkým ostatným kombinovane, v porovnaní s podkopaním systému a tým aj hodnoty svojho majetku.

7. Rekultivácia priestoru na disku

Akonáhle je najnovšia transakcia pochovaná pod dostatočným množstvom blokov, uhradené transakcie pred ňou môžu byť vymazané na uchovanie miesta na disku. Na sprostredkovanie funkčnosti takejto metódy bez porušenia hashu bloku, je transakcia hashovaná v tzv. Merkle strome [7][2][5], pričom obsahuje len koreň v hashi bloku. Staré bloky môžu byť potom odstránením vetiev tohto stromu kompaktnejšie a vnútorné hashe nemusia byť uložené.



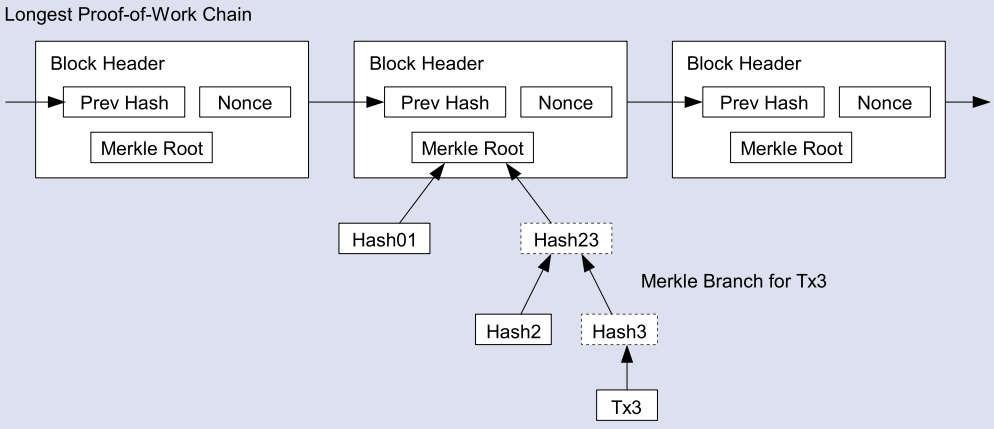
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

Hlavička bloku bez transakcií by bola približne 80 bajtov. Ak predpokladáme, že bloky sa generujú každých 10 minút, 80 bajtov * 6 * 24 * 365 = 4,2 MB ročne. S počítačovými systémami, ktoré sa od roku 2008 zvyčajne predávajú s 2 GB pamäte RAM a Mooreho zákonom, predpovedajúcim súčasný rast 1,2 GB ročne, počítame že by uchovávanie nemal byť problém, aj keby sa hlavičky blokov mali uchovávať v pamäti.

8. Zjednodušená verifikácia platieb

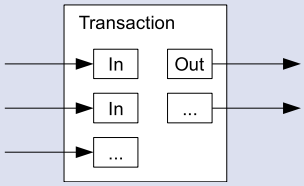
Platby je možné overiť aj bez bežania uzla s kompletnou históriou siete (full network node). Používateľ potrebuje iba uchovať kópiu záhlavia bloku najdlhšieho reťazca dôkazov o práci, ktorý môže získať dotazovaním sieťových uzlov, kým nie je presvedčený, že má najdlhší reťazec a získať vetvu Merkle stromu, ktorá spája danú transakciu s blokom, v ktorom je časovo označená. Nemôže síce sám skontrolovať danú transakciu, avšak môže vidieť jej prijatie uzlami a lokalizáciou v reťazci. Bloky pridané po tejto transakcii ďalej potvrdzujú jej akceptáciu sieťou.



V stave, kedy čestné uzly ovládajú sieť, je preto verifikácia dôveryhodná, ale je oslabená, pokiaľ sieť premôže útočník. Zatiaľ čo sieťové uzly môžu overiť transakcie pre seba, zjednodušená metóda môže byť oklamaná vykonštruovanými transakciami útočníka, až dovtedy, kým ovláda sieť. Jednou so stratégii, ako tomuto zabrániť, je akceptácia upozornení od sieťových uzlov, keď narazia na neplatný blok, čím sa vyzve softvér používateľa na stiahnutie kompletného bloku a dotknutých transakcií za účelom potvrdenia nekonzistencie. Firmy, ktoré dostávajú časté platby, budú pravdepodobne chcieť mať spustený vlastný uzol pre nezávislejšiu bezpečnosť a rýchlejšie overovanie.

9. Kombinovanie a rozdeľovanie hodnoty

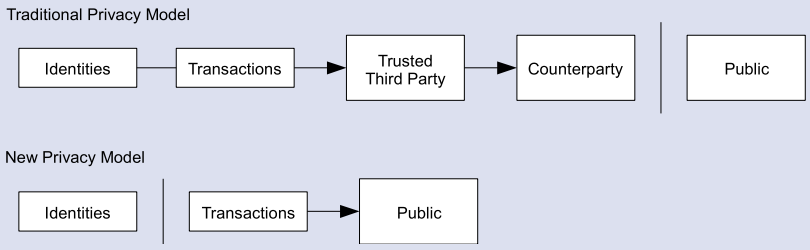
Hoci by bolo možné zvládnuť mince individuálne, bolo by ťažké uskutočniť samostatnú transakciu pre každý cent v prevode. Aby bolo možné rozdeliť a kombinovať hodnotu, transakcie obsahujú viacero vstupov a výstupov. Za normálnych okolností bude buď jeden vstup z väčšej predchádzajúcej transakcie alebo viaceré vstupy kombinujúce menšie sumy, a najviac dva výstupy: jeden pre platbu a druhý vráti prípadný výdavok späť odosielateľovi.



Treba poznamenať, že fan-out (počet vstupov, ktoré možno pripojiť k špecifikovanému výstupu), kde jedna transakcia závisí od viacerých iných transakcií a tieto transakcie závisia od mnohých ďalších, tu nespôsobuje problém. Nikdy nie je potrebné získať kompletnú samostatnú kópiu histórie transakcie.

10. Ochrana osobných údajov

Tradičný bankový model dosahuje úroveň súkromia tým, že zúčastneným stranám a dôveryhodnej tretej strane obmedzuje prístup k informáciám. Nevyhnutnosť oznámiť všetky transakcie verejne vylučuje túto metódu, avšak zachovanie súkromia sa dá docieliť zamedzením toku informácii v inej oblasti, a to zachovaním anonymity verejných kľúčov. Transakcie sú verejnosti sprístupnené, ale bez informácii, ktoré by napomáhali spájaniu s akoukoľvek osobou. Toto je podobné úrovni informácii sprístupnených burzami s cennými papiermi, kde sa zverejňuje čas a veľkosť jednotlivých obchodov (the tape/páska), ale bez zverejnenia informácií o obchodných stranách.



Na každú transakciu by mal byť použitý nový pár kľúčov, ako ďalšia ochranná vrstva zabráňujúca identifikácii vykonávateľa transakcie. Pri transakciách s viacerými vstupmi sú niektoré spojenia nezamedziteľné. Tie, ktoré nevyhnutne odhaľujú, že ich vstupy boli vo vlastníctve toho istého vlastníka. Riziko spočíva v tom, že ak je vlastník kľúča odhalený, prepojenie by mohlo odhaliť ďalšie transakcie patriace odhalenej osobe.

11. Výpočty

Zvažujeme scenár, kedy by sa útočník snažil vytvoriť alternatívny reťazec rýchlejšie ako čestný reťazec. Aj keby sa mu to podarí, nevytvorí to medzeru v systéme, ktorou by sa dali robiť svojvoľné zmeny, ako napríklad vytvoriť peniaze zo vzduchu alebo zmocniť sa peňazí, ktoré útočníkovi nikdy nepatrili. Uzly nebudú akceptovať neplatnú transakciu ako platbu, a čestné uzly nikdy neschvália blok, ktorý by ich obsahoval. Útočník sa môže pokúsiť zmeniť len jednu zo svojich transakcií, aby získal späť už utratené peniaze.

Pretek medzi čestným reťazcom a útočným reťazcom možno charakterizovať ako binomickú náhodnú prechádzku.

Úspešnou udalosťou je čestný reťazec predlžujúci sa o jeden blok, zvyšujúc svoje vedenie o +1, a neúspešnou udalosťou je reťazec útočníka rozšírený o jeden blok, zmenšujúci medzeru o -1.

Pravdepodobnosť útočníka dobehnúť daný deficit je analogická k tzv. Gambler's Ruin problému. Predpokladajme, že gambler s neobmedzeným množstvom kreditu začína v deficite, a hrá potencionálne nekonečný počet hier, kým nedosiahne bod, kedy nie je ani v zisku ani v strate. Pravdepobnosť, že niekedy dosiahne tohto bodu, alebo že útočník niekedy dobehne čestný reťazec, vieme vypočítať nasledovným spôsobom:

p = pravdepodobnosť, že čestný uzol nájde ďalší blok
q = pravdepodobnosť, že útočník nájde ďalší blok
qz = pravdepodobnosť, že útočník niekedy doženie medzeru z blokov

$$q_z = \begin{cases} , & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

Vzhľadom na náš predpoklad, že p>q, pravdepodobnosť klesá exponenciálne s počtom narastajúcich blokov, ktoré musí útočník dohnať. Ak nespraví veľký náhodný skok vpred hneď na začiatku, jeho šance pomaly upadajú a náskok sa zväčšuje. Pravdepodobnosť je preto v jeho neprospech.

Treba zvážiť, ako dlho musí príjemca novej transakcie čakať, kým si bude istý , že transakcia nemôže byť zrušená odosielateľom. Predpokladáme, že je odosielateľ útočníkom, ktorý chce aby príjimateľ uveril na určitý čas, že platba prebehla, aby následne zvrátil túto platbu. Príjimateľ bude upozornený, že sa také niečo deje, avšak útočník bude dúfať, že je už neskoro.

Prijímateľ si vytvorí nový pár verejných kľúčov, ktoré dá odosielateľovi tesne pred podpisom. Tento spôsob zabraňuje použitiu dopredu pripraveného reťazca blokov odosielateľom, na ktorom by pracoval nepretržite dokým by nemal dosť šťastia a dostal sa dosť ďaleko, a potom vykonal transakciu v ten potrebný moment. Po odoslaní transakcie začne nečestný odosielateľ tajne pracovať na paralelnom reťazci, ktorý obsahuje alternatívnu verziu jeho transakcie.

Príjemca čaká, kým sa transakcia pridá do bloku a z blokov sa naň potom napojí.Nevie aký

pokrok útočník spravil, ale ak predpokladáme, že čestným uzlom trvá jeden blok priemerný predpokladaný čas, útočníkov pokrok bude Poissonovo pravdepodobnostné rozdelenie s predpokladanými hodnotami:

$$= z \frac{q}{p}$$

Na získanie pravdepodobnosti útočníka stále dohnať náskok, vynásobíme hustotu Poissona za každú jemu možnú dosiahnuteľnú časť pokroku, pravdepodobnosťou ktorú má na dobehnutie z toho bodu:

$$\sum_{k=>}^{\infty} \frac{k \quad -}{k!} \cdot \begin{Bmatrix} (q/p)^{(z-k)} & if\ k \le z \\ , & if\ k > z \end{Bmatrix}$$

Preusporiadanie na zabránenie súčtu nekonečného chvosta distribúcie …

$$, -\sum_{k=>}^{z} \frac{k \quad -}{k!} \left(, -(q/p)^{(z-k)}\right)$$

Prevod do kódu C …

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Pri zopár výpočtoch môžeme vidieť, že pravdepodobnosť klesá exponenciálne s z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Riešenie pre P menej ako 0,1% …

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Záver

Navrhli sme systém elektronických transakcií bez spoliehania sa na dôveru. Začali sme s obvyklým rámcom mincí vyrobených z digitálnych podpisov, ktorý poskytuje silnú kontrolu nad vlastníctvom, avšak bez spôsobu ako zamedziť dvojitej útrate (double-spending.). Na vyriešenie tohto problému sme navrhli sieť typu rovný s rovným (peer-to-peer), používajúcu dôkaz o práci na zaznamenanie verejnej histórie transakcií, ktorých zmena sa rýchlo stáva výpočtovo nepraktická pre útočníka, pokiaľ čestné uzly disponujú väčšinou výpočtovej sily v sieti. Sieť je robustná svojou neštruktúrovanou jednoduchosťou. Všetky uzly pracujú naraz iba s malou koordináciou. Nie je potrebné ich identifikovať, pretože správy nie sú smerované na žiadne konkrétne miesto a musia byť doručené iba na základe najlepšieho úsilia (best effort basis). Uzly sa môžu k sieti svojvôľne odpojiť a znovu pripojiť, akceptujúc reťazec s dôkazom o práci ako dôkaz o tom, čo sa stalo počas ich neprítomnosti. Hlasujú so svojou výpočtovou silou, prejavujúc prijatie správnych blokov pracovaním na ich predĺžení a odmietnutím nesprávnych blokov, tým že odmietnu s nimi pracovať. Akékoľvek potrebné pravidlá a stimuly sa môžu presadzovať prostredníctvom tohto konsenzuálneho mechanizmu.

Referencie

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure, http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.
[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Definície pojmov:

"Peer-to-peer sieť, taktiež označovaná ako sieť so vzájomným sprístupňovaním, alebo sieť typu rovný s rovným, je sieť, ktorá sa viac spolieha na výpočtovú silu koncových zariadení (počítačov) ako na sieť samotnú. Čistý P2P prenos súborov neobsahuje ani klientov, ani servery, ale iba rovnocenné sieťové uzly, ktoré súčasne plnia voči iným uzlom v sieti úlohu servera aj klienta."
(https://sk.wikipedia.org/wiki/Sieť_so_vzájomným_spr%C3%ADstupňovan%C3%ADm)

Problém dvojitej útraty je potenciálnym nedostatkom v systéme digitálnej hotovosti, v ktorom môže byť utratený rovnaký digitálny token viac ako raz. Je to možné, pretože digitálny token pozostáva z digitálneho súboru, ktorý môže byť duplikovaný alebo falšovaný. (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174)

Časová pečiatka sa používa na overenie elektronického podpisu ako časový údaj vytvorenia podpisu. (http://www.qsign.sk/ako-ziskam/casova-peciatka)

Uzly sú miestom v prenosovej sieti alebo zariadení, v ktorom sa vzájomne prepája niekoľko susedných okruhov sietí." (https://sk.wikipedia.org/wiki/Uzol)

Hashovacia funkcia je funkcia (predpis), pre prevod vstupného reťazca dát na krátky výstupný reťazec. Tento reťazec sa označuje ako hash (angl. hash), charakteristika, odtlačok vstupných dát. Dĺžka hashu je závislá od zvolenej hashovacej funkcie, má fixnú dĺžku pár desiatok bitov."
(https://sk.wikipedia.org/wiki/Ha%C5%A1ovacia_funkcia)

Nonce je v kryptografii vynútené čislo, ktoré môže byť použité iba raz. Je to často náhodné alebo pseudo-náhodné číslo vytvorené na autentifikáciu protokolu, pre zaručenie neopakovateľnosti predošlej komunikácie a zabráneniu tzv. Replay útokom.
(https://en.wikipedia.org/wiki/Cryptographic_nonce)

Hashcash je systém dôkazu o práci, používaný na zachytávanie a limitovanie emailového spamu a útokov, kde sa odopiera služba. Nedávno sa stal známym ako algoritmus používaný na ťaženie bitcoinu a iných cryptomien. (http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp_abs.html)

Usenet (User's Network) bola sústava vzájomne prepojených uzlov, ktoré si medzi sebou predávali sieťové správy. Vznikla spolu so vznikom internetu. Časom sa z nej stala virtuálna sieť, resp. služba poskytovaná v rámci iných sietí." - https://sk.wikipedia.org/wiki/Usenet

Poissonovo rozdelenie alebo Poissonovo pravdepodobnostné rozdelenie je v teórii pravdepodobnosti a štatistike diskrétne rozdelenie pravdepodobnosti, ktoré môžeme interpretovať ako rozdelenie pravdepodobnosti výskytu zriedkavých udalostí v sérii veľkého počtu nezávislých pokusov. Patrí k pravostranne zošikmeným rozdeleniam."
https://sk.wikipedia.org/wiki/Poissonovo_rozdelenie