Kryptosystémy a potenciál ich využitia v súkromnom a verejnom sektore

Kľúčové slová:

Kryptosystémy, kryptomeny, Bitcoin, verejné služby, finančné služby, transparentnosť, efektívna verejná správa.

Riešené otázky

Na akých princípoch fungujú kryptomeny resp. kryptosystémy? Akú technologickú evolúciu prinášajú? Aké sú základné možnosti ich využívania v súkromnom a verejnom sektore?

Autori

Pošvanc Matúš, Cabaj Andrej, Havran Tomáš, Lindák Martin, Stancel David, Thurzo Andrej

Editor:

Oravec Ján

Nadácia F. A. Hayeka, 2016

Text bol pripravený s podporou

Friedrich Naumann STIFTUNG FÜR DIE FREIHEIT

Obsah

1. Abstrakt

V súčasnosti už existuje relatívne rozsiahle povedomie o existencii kryptosystémov, resp. kryptomien a ich využiteľnosti vo finančnej oblasti. Dnes najznámejším kryptosystémom, resp. kryptomenou je Bitcoin. Málokto si však dnes uvedomuje revolučný potenciál toho, čo kryptosystémy prinášajú. *Zmenu paradigmy riadenia mnohých spoločenských javov a to nielen finančného charakteru.*

Dnešná spoločnosť čelí hlavne vo verejnom sektore mnohým problémom. Môžeme spomenúť finančnú transparentnosť, či transparentnosť v rozhodovaní, vysoké administratívne zaťaženie obyvateľstva i podnikateľov, relatívne pomalú a neefektívnu komunikáciu verejného sektora voči občanom, problém prepojenosti jednotlivých IT systémov vo verejnom sektore, vynakladanie verejných zdrojov na administratívu a samotný výkon verejných politík, problémy pri verejnom obstarávaní súvisiace s nedostatočnou transparentnosťou, či obchádzaním a prispôsobovaním si pravidiel a v neposlednom rade problém adresnosti pri využívaní akejkoľvek formy sociálnej podpory zo strany štátu (dotácie na dopravu, sociálnu oblasť, vzdelávanie, kultúru a pod.).

Technológia, ktorú so sebou prinášajú kryptomeny umožňuje posunúť tieto riešenia na úplne novú úroveň fungovania. Kryptosystémy umožňujú spoločnosti dôverovať automatizovaným činnostiam, ktoré sú dnes vykonávané rozsiahlym verejným aparátom, bez potreby tohto aparátu. Umožňujú automatizovane poskytovať nemenné a zabezpečené údaje užívateľom verejných databáz, zabezpečiť vysokú mieru transparentnosti vo verejnom obstarávaní, či verejnom rozhodovaní, programovať cashflow vo verejnom sektore, pridávať podmienky a práva pre užívateľov verejných dávok (doprava, vzdelávanie, sociálne služby), resp. vopred definovať vlastnosti týchto dávok a automatizovať ich používanie a kontrolu. Môžeme tvrdiť, že kryptotechnológie umožnia v budúcnosti vysoko zefektívniť celé fungovanie spoločnosti.

2. Popis a princípy fungovania

Kryptosystém alebo kryptomena je technológia, ktorá existuje vo virtuálnom svete. Najznámejším kryptosystémom v súčasnosti je tzv. Bitcoin. Nie je len najznámejším, ale i najviac rozvinutým a najbezpečnejším kryptosystémom vôbec. Ostatné kryptosystémy môžu mať podobný charakter, resp. sú od bitcoinu priamo alebo nepriamo odvodené, iné majú rozdielnu filozofiu. Našu prácu začneme stručným popisom fungovania kryptomeny bitcoin. Tento popis môže poslúžiť ako úvod do chápania fungovania kryptosystémov a ich funkcionality.

Bitcoinová sieť rieši problém nutnosti dôveryhodnej tretej strany v transakciách medzi dvoma subjektmi a jej náhradu kryptografickým (matematicky overiteľným) dôkazom. Vzhľadom na to, že tento systém rieši problematiku transakcií, na jeho popis sa používa i názov „kryptomena“.

Spôsob fungovania je pomerne jednoduchý a je realizovaný podobne ako normálna banková transakcia s drobnými rozdielmi. Každý účastník transakcie vlastní verejný kľúč – adresu, ktorá je obdobou bankového účtu a súkromný kľúč, ktorý je obdobou

hesla alebo PIN-u, oprávňujúceho majiteľa nakladať s bitcoinmi na svojom účte. Rozdiel medzi bankou a kryptosystémom je v tom, že zatiaľ čo bankový účet a heslo k nemu Vám pridelí banka, v bitcoinovom svete vám tento pár navzájom spojených kľúčov (súkromný a verejný), vygeneruje software voľne stiahnutý z internetu do PC alebo mobilu.

Samotná transakcia však už prebieha diametrálne odlišným spôsobom, ako sme navyknutí z bankového sveta. V banke zabezpečí jej interný systém, že z účtu odosielateľa bude požadovaná suma odpísaná a pripísaná v prospech prijímateľa. Nato, aby banka danú operáciu vykonala, nutne potrebuje poznať identitu oboch strán transakcie, čo zvyšuje náklady na transakciu a na ochranu osobných údajov, predlžuje čas na jej vykonanie a v neposlednom rade umožňuje transakciu kedykoľvek zvrátiť na základe rozhodnutia samotnej banky či iného orgánu.

V bitconovom prostredí niet nikoho, kto by túto operáciu vykonal uvedeným spôsobom a rovnako bitcoinový systém nepotrebuje poznať identity stojace za používanými adresami. Bitcoinový systém sa s požiadavkou na vykonávanie transakcií vyrovnáva nasadením absolútne transparentného a verejného zoznamu transakcií, ktorý nazývame blockchain.

Blockchain je presný záznam všetkých transakcií v časovom slede, nespochybniteľne preukázaný kryptografickými metódami počas procesu, známeho pod pojmom mining (ťažba). Mining je súborom operácii, ktorých účelom je zhromaždiť všetky aktuálne transakcie, preveriť, či sú podpísané oprávneným disponentom príslušných adries (účtov), zistiť požadované zostatky a potvrdiť prevody na nové adresy (účty).

Bitcoin je najznámejším, najviac rozvinutým a najbezpečnejším kryptosystémom, resp. kryptomenou.

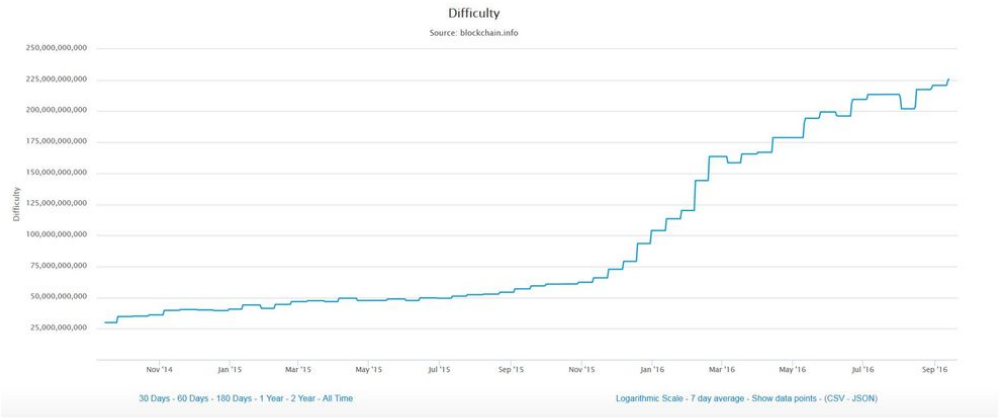
Proces prebieha tak, že set posledných transakcií sa zhromaždí do bloku a tento blok sa opatrí špeciálnym digitálnym odtlačkom – tzv. hashom, ktorý potvrdí platnosť prebiehajúcich transakcií a ich nemennosť. Každý nový blok teda obsahuje odtlačok – „hash“ predchádzajúceho bloku a zoznam ďalších nových transakcií. Znamená to, že bloky vytvárajú na sebe navzájom závislú reťaz - tzv. chain blokov.

Účastníkom bitcoinovej siete sa môže stať ktokoľvek s nainštalovaným softvérom bitcoinovej siete. Sieť mu umožní vytváranie transakcií tým, že mu generuje adresy a k nim príslušné súkromné kľúče, aby mohol požiadavku na transakciu odvysielať do siete k minerom na potvrdenie.

Mineri sú špecializovaní účastníci siete, ktorí zabezpečujú potvrdzovanie transakcií a ich nemennosť hľadaním špeciálneho hashu bloku. Aby mohli získať motivačnú odmenu vo forme nových bitcoinov a poplatkov za transakcie účastníkov, musí výsledok schváliť nadpolovičná väčšina účastníkov siete. Keďže bitcoinov je iba limitovaný počet (21 mil.), odmena pre minerov vo forme nových bitcoinov neustále klesá, čo je ale kompenzované rastom počtu transakcií a poplatkov z nich.

Mineri sú neustále nútení vzájomnou konkurenciou o čo najrýchlejšie potvrdenie bloku v intervale zhruba každých 10 minút, pretože iba najrýchlejšiemu z nich pripadne celá odmena. Aby sa dodržal konštantný takt v tomto časovom intervale, sieť neustále modifikuje kryptografický mechanizmus nájdenia bloku - hashu. Tento proces nazývame aj parametrom obťažnosti siete. Ak sa niektorému minerovi podarí nájsť správny hash skôr ako za 10 minúť, obťažnosť nasledujúceho bloku sa zvýši exponenciálne. Naopak, ak sa čas nájdenia predĺži, obťažnosť úmerne klesne. Tento automatický proces neustále núti minerov investovať svoje zdroje do nového výpočtového výkonu tak, aby obstáli v konkurencii.

Obťažnosť siete – Bitcoin



Zdroj: blockchain.info

Vidíme teda, že prostredníctvom automatizovaného kryptografického blockchainu dokáže bitcoinová sieť realizovať transakcie bez potreby inštitucionalizovanej tretej strany, transparentne, bez potreby osobných údajov účastníkov, pričom proces je garantovaný demokratickou silou nadpolovičného výpočtového výkonu samotných účastníkov.

Revolučný technologický potenciál Bitcoinu a iných jemu podobných kryptosystémov spočíva v technológii, ktorá tvorí jeho základ – v blockchaine. Blockchain funguje ako register či účtovná kniha, v ktorej je zaznamenaná história všetkých transakcií, ktoré sa kedy uskutočnili. Jej história je nemenná, pričom nemennosť je chránená kryptografiou (odtiaľ pochádza aj názov kryptosystémy, resp. kryptomeny). Významnou vlastnosťou blockchainu je, že je nemenný, v princípe nenapadnuteľný akýmkoľvek útočníkom a verejný. Na nemennosť a správnosť je možné sa spoľahnúť bez toho, aby bol potrebný kontrolór, či tretia strana. Z týchto vlastností vyplýva i potenciálne využitie kryptosystémov (kryptomien), ktoré popíšeme nižšie.

3. Kryptosystémy: zmena paradigmy

Vyššie definované vlastnosti a možnosti využitia nemusia byť na prvý pohľad revolučnými. Dovolíme si však tvrdiť, že sú. Rozdiel, ktorý je oproti dnešnému fungovaniu sveta zásadný, sa dá popísať v oblasti kryptotechnológií filozoficky nasledovne.

V súčasnom „*centralizovanom*“ svete sa spotrebitelia pri mnohých činnostiach spoliehajú na rozhodnutia tretích strán; príkladom môže byť banka, notár, štátna inštitúcia, štátna administratíva, verejné registre, zúčtovacie centrum, atď., za ktorými stoja vždy ľudia. Užívatelia im veria niekedy preto, že musia (verejný sektor), inokedy pre dobrú povesť a značku (keď nemusia). Tento systém je spojený s ľudskou spoločnosťou už tisícky rokov. Užívatelia vždy museli veriť tretej strane. V mnohých prípadoch len preto, lebo v minulosti nebolo technicky možné odovzdať odkaz, previesť peniaze, či zabezpečiť zhodu inak ako prostredníctvom dôveryhodnej tretej strany.

V decentralizovanom svete kryptosystémov sa spotrebitelia spoliehajú na automatizované rozhodnutie, ktoré je držané vo vopred zadefinovaných medziach prostredníctvom kryptografie a matematických zákonitostí. Vysvetlime si to na príklade. V súčasnosti užívateľ zverí peniaze banke. Ona predstavuje tretiu dôveryhodnú stranu.

Stranu, ktorej užívateľ dôveruje, že za neho napr. presunie peniaze na účet inému klientovi, ktorý jej dôveruje rovnako. Vo svete kryptomien sa tento prenos realizuje priamo, napr. medzi dvoma osobami. A na to, aby užívateľ nemohol nikoho oklamať – napr. skopírovať bitcoin dva krát alebo ho dvakrát minúť, dávajú pozor matematické zákonitosti a kryptografia. Zjednodušene povedané, nie „*dôveryhodná*“ tretia strana, ale matematika, resp. jej zákonitosti zaručujú dôveryhodnosť transakcií, či aktivít užívateľov. Dôležitým a významným aspektom je, že kryptosystémy dokážu zabezpečiť konsenzus o určitej veci medzi mnohými aktérmi, ktorí majú veľakrát rozdielne motivácie. Hlavne v prípade, že niekto chce daný konsenzus napadnúť zvonka (napr. hacker).

Otázkou, ktorú si môžeme na základe tohto popisu položiť je, aké dôsledky budú mať kryptosystémy pre budúcnosť fungovania našej spoločnosti.

4. Oblasti využiteľnosti

Z popisu uvedených vlastností explicitne vyplýva, že kryptosystémy sú jednoznačne využiteľné v oblasti finančných transferov. Umožňujú posielať ekvivalent finančnej hodnoty z jedného konca sveta na druhý; rýchlo, priamo medzi užívateľmi a za nižšie ceny v porovnaní so súčasnými existujúcimi systémami zameranými na transfer finančnej hodnoty. Nie je to však ich jediné možné využitie.

Vo všeobecnosti sa hovorí o využití kryptosystémov aj v iných oblastiach ako v oblastiach finančných transakcií. Toto využitie je popísané v tzv. projektoch „Bitcoin 2.0“, ktorými sa väčšinou zaoberajú rôzne malé IT spoločnosti. V súčasnej dobe sa predpokladá, že technológia zasiahne mnohé oblasti, či už podnikania ale i každodenného života ľudí.

V nasledujúcom texte stručne popíšeme päť oblastí zo súkromného sektora a rozsiahlejšie päť oblastí z verejného sektora, ktoré môžu využívaním kryptosystémov výrazne zmeniť svoje fungovanie.

4.1 Potenciálne využitie kryptosystémov v súkromnom sektore

V oblasti súkromného sektora sa predpokladajú rôzne možnosti využívania kryptosystémov. Je zároveň pravdepodobné, že to bude práve súkromný sektor, ktorý začne tieto systémy využívať skôr ako verejný. Ktoré oblasti sa dajú považovať za najzaujímavejšie z pohľadu kryptosystémov?

4.1.1 Finančný Clearing

Jednou z možností využívania kryptosystémov vo finančnom svete, nad ktorou sa intenzívne uvažuje, je ich využitie na potreby zúčtovania svetového obchodovania. Náhrada dnes už „*staromódneho*“ mechanizmu SWIFT. Na danom riešení už pracuje spoločnosť, ktorej kryptosystém nesie názov Ripple. V komunite síce nie je kvôli jeho čiastočne centralizovanému charakteru najviac obľúbeným krytosystémom, ale niektoré banky sa ho už rozhodli využívať.

4.1.2 Využitie side-chains vo finančných službách

Kryptosystém Bitcoin je pre súčasné obchodovanie titulov na burzách relatívne pomalým systémom. Overovanie transakcie každých 10 minút nie je dostatočné pre dnešný systém vysokofrekvenčného obchodovania, ktoré prebieha v milisekundách. Avšak už dnes uvažujú viacerí nad vznikom tzv. side chains, samostatne fungujúcich registrov, ktoré by neboli obmedzované relatívne pomalou infraštruktúrou bitcoinu. Umožňovali by rôzne druhy obchodovania s tým, že bitcoin – ako najdôveryhodnejší systém – by sa používal len na clearing medzi obchodníkmi, kde je 10 minútová frekvencia dostatočná.

4.1.3 Internet vecí

Predstavme si, že užívateľ príde do kina. Za lístok zaplatí kryptomenou. Priloží mobilný telefón k turniketu, ktorý ho pustí dnu. Príde k sedadlu, na ktoré si kúpil lístok, priloží k nemu telefón a ono sa automaticky sklopí. A môže pozerať film. Alebo si predstavme, že dron priletí k oknu užívateľa (alebo priamo k užívateľovi, kdekoľvek sa nachádza), doručí balík, pizzu, tovar. Užívateľ priloží telefón, ktorý skenuje potvrdenie o zaplatení kryptomenou a dron vec vydá. Uvedené príklady a ďalšie možnosti, môžu v budúcnosti užívateľov kryptosystémov čakať.

Kryptosystémy umožnia postupnú implementáciu internetu vecí a zabezpečia spoľahlivosť automatizovaných činností strojov.

Pri riešení problematiky internetu vecí môže vykonanie transakcie a jej detekcia spustiť automatizovanú sadu prednastavených inštrukcií, čo môže slúžiť k riadeniu prakticky všetkého, čo sa dá pripojiť na elektrický prúd alebo iný zdroj energie. Využitie kryptosystémov zároveň zabezpečí, že riadenie daných zariadení nebude zneužité treťou stranou na nežiaduce úkony.

4.1.4 Úpis akcií

V súčasnosti je značne náročné zrealizovať úpis akcií alebo akýchkoľvek iných inštrumentov na burze. Nie je to samozrejme nemožné, avšak úkon je často finančne i procesne náročný. Nie však vo svete kryptosystémov. Úpis akcií, majetkový záznam k nim a ich obchodovanie na decentralizovaných trhoviskách je pravdepodobne jedna z ďalších oblastí, v ktorej budú kryptosystémy už čoskoro využívané. O dané služby sa už pokúšajú systémy ako Omni, či Counterparty.

4.1.5 Decentralizované úložiská dát / decentralizovaný internet

Každý sa už určite stretol s informáciami o tom, že niektorým spoločnostiam unikli osobné dáta klientov. Pri využívaní decentralizovaných aplikácií sa to už stať nemôže. Niektoré projekty uvažujú dokonca tak ďaleko, že dáta sa budú nielen bezpečne ukladať (automatické kryptovanie), a omnoho rýchlejšie vyvolávať zo siete, ale bezpečnosť internetu sa posunie na úplne novú úroveň, čo je využiteľné pri zabezpečovaní webových stránok, elektronickej komunikácie vo finančnom systéme, či samotnej elektronickej komunikácii. Tieto a podobné vlastnosti sú cieľom napr. projektu MaideSafeNet.

4.2 Potenciálne využitie kryptosystémov vo verejnom sektore

V súčasnosti už nie je využívanie informačných technológií vo verejnom sektore žiadnou výnimkou. Informačné technológie umožňujú znižovať napr. administratívne zaťaženie podnikania, zrýchľovať komunikáciu verejného sektora voči občanovi, ako aj zvyšovať transparentnosť verejného sektora. Okrem klasického využitia kryptomien na

transparentnú, efektívnu a kontrolovateľnú úhradu daní a poplatkov (počnúc daňami z príjmov, DPH v celej reťazi platieb až po akékoľvek poplatky), je možné využívať kryptosystémy aj v iných oblastiach s efektom úspory zdrojov, zvýšenia transparentnosti a efektívneho vynakladania verejných zdrojov.

4.2.1 Verejné obstarávanie

Jedným z príkladov využitia kryptotechnológii vo verejnom sektore je práve oblasť verejného obstarávania. Verejné obstarávanie zvyčajne zahŕňa verejné práce, služby a zásobovanie vykonané verejnou inštitúciou. Je zároveň jednou z najviac kritizovaných oblastí na Slovensku. Kritici hovoria o nedostatočnej transparentnosti, či obchádzaní a prispôsobovaní pravidiel.

Verejné tendre organizované vládnymi agentúrami môžu byť transparentnejšie, zautomatizované a samo vynútiteľné použitím tzv. smart kontraktov (inteligentných kontraktov), ktoré by mali na starosť celý proces. Transparentnosť by bola dosiahnutá aj samotným faktom, že pri zverejňovaní verejných kontraktov by bola využívaná technológia blockchainu (bitcoinu alebo jeho špecializovaného derivátu). Týmto spôsobom by si každý vedel overiť, či tender vyhrala naozaj najlepšia ponuka. Zároveň nie je nevyhnutné zverejniť identitu všetkých zúčastnených, pokiaľ to nie je žiaduce. Všetky ponuky môžu byť pseudo-anonymné, nakoľko adresy v blockchaine nemusia mať zverejnenú reálnu identitu, ktorá za nimi stojí. Napriek tom by ktorýkoľvek z účastníkov tendra mohol poskytnúť nepochybný dôkaz prepojenia jeho reálnej a virtuálnej identity prostredníctvom digitálneho podpisu.

Automatizácia obstarávania by sa dala zvýšiť až do takej miery, kedy smart kontrakt automaticky vyberie najvýhodnejšiu ponuku (napr. najmenej nákladnú) po vypršaní doby určenej na prijímanie ponúk. Následne ďalší, podmienený (escrow) kontrakt môže ošetriť vyplatenie odmeny až po splnení podmienok ukotvených v predchádzajúcom kontrakte. Odmena sa uvoľní po tom, čo dostane input od poverenej autority (či autorít). V prípade, ak by dodávateľ nedodal dohodnuté služby alebo tovary, finančné prostriedky by boli automaticky vrátené naspäť zadávateľovi verejného obstarávania. V prípade splnenia služby či dodania tovaru by uchádzač mohol automaticky získavať i referencie, ktoré by mohli byť následne využívané v ďalších verejných obstarávaniach (napr. v zmysle § 34 súčasného zákona č.343/2015 Z. z. o verejnom obstarávaní).

V rámci takéhoto fungovania verejného obstarávania by mohli mať uchádzači rovnako uľahčené napr. preukazovanie splnenia ostaných podmienok (napr. v zmysle §26), kedy by systém plnenie podmienok kontroloval a automaticky pod..

4.2.2 Notárske zápisy

Notársku oblasť sme zaradili medzi verejné služby vzhľadom na to, že notár je štátom určenou osobou na vykonávanie notárskej činnosti, pričom súbor týchto právomocí mu je udelený štátom na dobu neurčitú.

Prevod majetku. Vlastnícke tituly. Potvrdenia. Dohody. Závete. Pre realizáciu týchto druhov záznamov môže byť využívaná technológia blockchainu. Výsledkom je bezpečný záznam bez možnosti jeho zmeny a tým pádom s maximálnou mierou zabezpečenia autenticity, či s dostatočnou mierou transparentnosti. Notársky zaznamenané dáta na základe kryptosystémov môžu byť následne využívané pre ďalšie úkony a ich aplikáciu pri automatizácii platieb, prevode majetku, či automatizácii úkonov bez zásahu človeka. Príkladom môže byť automatické naplnenie podmienok závetu, prevod vlastníctva majetku na základe vopred definovaných podmienok plnenia

(napr. realizácia platby za kupovaný majetok), či automatické naplnenie sankcií pri neplnení zmluvných vzťahov, a pod..

4.2.3 Registre

Prepojiteľnosť registrov. Zaručená autenticita dát. Nenapadnuteľnosť zapísaných údajov. Vlastnosti, ktoré umožnia rôzne druhy automatizovaných činností, dnes realizovaných ľudským faktorom.

Využitie blockchain technológie si môžeme predstaviť aj pri vytváraní a používaní akýchkoľvek druhov verejných registrov. Používanie údajov bude zodpovedať kritériám nemeniteľnosti, zaručenej autenticity a nenapadnuteľnosti, zároveň však s poskytnutím dostatočnej miery súkromia i transparentnosti. Dané údaje budú zároveň kedykoľvek prístupné akýmkoľvek elektronickým zariadením. To rieši mnohé problémy, ktoré dnes so sebou nesú súčasné IT riešenia.

Na využiteľnosť kryptosystémov pri riešení skutočných reálnych problémov v tejto oblasti ukazuje napr. aj „*Národná koncepcia informatizácie verejnej správy Slovenska*“. Tá si kladie za cieľ racionalizáciu prevádzky informačných systémov pomocou vládneho cloudu, ako aj zvýšenie ochrany a zabezpečenia týchto dát. Výsledkom snáh má byť racionalizácia a zefektívnenie verejnej správy, ako pre štát, tak aj pre občana alebo podnikateľa.

Jedným z hlavných problémov v uvedenej oblasti je, že v súčasnosti sú jednotlivé databázy (napr. obchodný register, register trestov) od seba nezávislé. V prípade požiadaviek zo strany užívateľov (napríklad vyžiadanie dokumentácie), tak vzniká pre nich zbytočná záťaž, keď si musia jednotlivé dokumenty vyžadovať od každej spravujúcej inštitúcie osobitne.

A práve tu je možné uvažovať v budúcnosti s využitím kryptosystémov. Jeden z projektov, ktorý sa danej problematike venuje je projekt „Factom“.

Príklad decentralizovaných registrov. Projekt Factom

Projekt Factom existuje od septembra 2015 a je zameraný na tvorbu a správu registrov, či databáz. Názov Factom pochádza z latinského slova Factum, ktoré v preklade znamená: „čo je uvedené, je skutočné.“ Factom je kryptosystém, ktorý využíva blockchain Bitcoinu a nedávno i Etheru (iná kryptomena) pre bezpečné ukladanie záznamov alebo dát. Zápis dát môže realizovať verejná alebo súkromná inštitúcia. Dáta zapísané do systému Factom sú nezmazateľné a nemenné. Dáta nie sú ohrozené žiadnou treťou stranou napr. v podobe útočníka (hackera) a sú dôveryhodné.

Využitie systému Factom

Systém môžeme najjednoduchšie popísať z hľadiska jeho používateľov. Na jednej strane z pohľadu štátnej inštitúcie, ktorá má záujem napr. evidovať údaje o svojich občanoch, pričom údaje musia byť zabezpečené a užívateľský prístupné, editovateľné alebo zmazateľné. Na strane druhej to budú obyvatelia, ktorí využívajú databázu napr. v zmysle jej previazanosti na iné databázy, čím sa zjednoduší administratíva spojená s overovaním a využívaním predmetných dát, pričom by samozrejme by mali mať prístup len k vlastným údajom, nie iným.

V prípade kryptosystému Factom musí verejná inštitúcia pri tvorbe databázy postupovať nasledovne. Po prvé musí nakúpiť menu Factomu – tzv. factoidy. Factoid môžeme prirovnať k bitcoinu, čiže ho môžeme chápať ako finančnú jednotku – token systému. Nakúpené factoidy drží v zabezpečenej elektronickej peňaženke. Následne za ne nakupuje práva na ukladanie dát do systému. Týmito právami sú tzv. entry kredity.

Zapísanie jedného gigabajtu dát do systému Factom stojí v súčasnej dobe približne 2000 dolárov. Na jednej strane je táto cena niekoľkonásobne vyššia ako cena bežných zabezpečených cloudov. Ceny cloudov závisia od poskytovateľa, od množstva

ukladaných dát a hlavne od času na aký ich ukladáte, keďže za uložené dáta sa platí ročne. Na strane druhej kryptosystém Factom poskytuje možnosť vytvorenia vysoko bezpečnej databázy s nemožnosťou zmeny dát bez vedomostí užívateľa (napr. štátu), ktorých zapísanie je prakticky doživotné. Rovnako je v rámci kryptosystému možné previazať jednotlivé registre. Napríklad osobné údaje s lekárskymi záznamami alebo s registrom trestov.

Popis fungovania systému Factom

Úplne najmenšou jednotkou je tzv. entry súbor (v nami popisovanom prípade konkrétne údaje o obyvateľovi), ktorý užívateľ (štát) vloží do vytváranej predmetnej databázy (tzv. chainu).

Predmetné databázy (chainy), si môžeme predstaviť ako zložky s dátami, pričom každá zložka je určená pre iné dáta. Jedna zložka bude obsahovať len dáta o obyvateľoch a druhá len lekárske záznamy. Nikdy sa nemôže stať, že dáta s lekárskymi záznamami sa dostanú do zložiek s údajmi o obyvateľoch. Na jednej strane by sa to nedostalo cez pravidlá, ktoré si každý užívateľ môže na začiatku v databáze definovať. Na strane druhej každý vkladaný entry má svoju tzv. chain ID. To je identifikačné číslo vkladaného údaju, na základe ktorého sa ukladajú dáta do jednotlivých predmetných databáz (chainov).

Štát môže navyše definovať napr. databázu, ktorá bude brať do úvahy aj konkrétnu legislatívu alebo iné pravidlá a kritériá. Samozrejme v prípade zmeny legislatívy alebo pravidiel je možné ich primerane meniť v samotnej databáze, čo znamená, že pravidlá sa dajú priebežne aktualizovať. Využitie predmetných databáz je teda veľmi široké a záleží len od používateľa, povahy samotných dát a ich vzájomnej kombinovateľnosti.

Bezpečnosť

Systém je zabezpečený vysokou mierou kryptografie. Každú minútu sa chainy (databázy) zaradia do vyššej vrstvy, ktorou je blok chainov, obsahujúci niekoľko chainov. Tie sa následne uložia do najvyššej vrstvy - tzv. directory bloku. Na konci každej minúty sa vytvorí jeden directory blok, kde sú uložené bloky chainov. Tento proces sa zopakuje 10 krát, pričom po zostavení 10-teho directory bloku, teda na konci 10 minúty, sa vytvorí celkový hash týchto blokov, ktorým sa 10 directory blokov na konci 10 minúty uloží do blockchainu . Všetky uložené dáta a rovnako aj jednotlivé úrovne dát sú tak zabezpečené kryptograficky.

Tu je potrebné upozorniť, že Factom nie je len obyčajná databáza, kde užívateľ niečo zapíše. Prvý entry, ktorý vkladá užívateľ do Fatcom- sú vlastnosti predmetnej databázy (napr. register obyvateľstva v podobe, mena, priezviska, rodného čísla, adresy, národnosti, dátumu narodenia, čísla sociálneho poistenia, či iných údajov). V rámci nej môže verejná inštitúcia definovať parametre, na základe ktorých sa budú ukladať alebo neukladať dáta do systému.

Benefity užívateľov databázy systému Factom

Prvým a najhlavnejším benefitom systému Factom je jeho bezpečnosť. To znamená, že nikto iný, okrem samotného tvorcu chainu (našej databázy) nemá možnosť do neho zasahovať. Druhou výhodou je spomínaný už prvý vstup (entry), teda aplikácia, ktorá sa dá flexibilne meniť v kontexte požiadaviek na štruktúru dát a ich funkcionalitu. Tretím benefitom je, že systém môže ušetriť náklady, či už sú to náklady na udržiavanie rôznych databázových systémov alebo náklady spojené s bezpečnosťou, s únikom dát a pod. Ako štvrtú výhodou môžeme uviesť možnosť previazanosti jednotlivých databáz.

Možnosť previazanosti si môžeme popísať na príklade. Predstavme si situáciu obyvateľa uchádzajúceho sa o prácu v armáde alebo polícii. V jeho prípade môže byť potrebné, aby bol bez záznamu v registri trestov, nemal žiadne vážne ochorenie, mal určité vzdelanie, disponoval niektorými overenými zručnosťami a bol držiteľom vodičského preukazu. Štátne inštitúcie môžu vytvoriť systém, ktorý bude tieto údaje vyberať automaticky z jednotlivých databáz. Presnejšie z registra trestov, z databázy zdravotných záznamov, z databázy vydaných vodičských preukazov, databázy dosiahnutého vzdelania, či získaných certifikátov zručností. Tento systém v prípade zistenia, že uchádzač spĺňa požadované kritériá, len automaticky odporučí jeho prijatie. Systém sa dá aplikovať aj na iné oblasti, napr. na samotné vydávanie vodičských preukazov, pasov, víz, atď..

Možnosti využitia Factom technológie existujú aj v ďalších oblastiach ako sú napr. oblasti pozemkových registrov, registrov patentov, obchodného, či živnostenského registra, registra obyvateľstva, registra automobilov, registra neplatičov a pod..

Vlastnosť relatívnej „*immutability*“ (nemeniteľnosti) záznamu je pre zdravotné dáta mimoriadne významná a kryptotechnológie budú hrať v oblasti zdravotníctva už čoskoro významnú úlohu.

4.2.4 Databázy v oblasti e-health

Ako už bolo spomenuté, kryptografia umožnila kryptotechnológiám stať sa významnou inováciou. Šifrovanie ponúka ochranu vo virtuálnom elektronickom svete a pri súčasnej digitalizácii dát a procesov v zdravotníctve je to práve ich ochrana, ktorá ostane najvyššou prioritou. Digitalizácia bez on-line dostupnosti je len polovica cesty. On-line dostupnosť však so sebou prináša mimoriadne riziká. Niektoré diskrétne zdravotné údaje budú možno v dohľadnej budúcnosti úzkostlivejšie chránené ako sú chránené peniaze. V súčasnosti je pre ich ochranu potrebná dôvera človeka/pacienta v štát/nemocnicu/ambulanciu resp. iného sprostredkovateľa, ktorý tieto citlivé dáta uchováva. Kryptotechnológie umožňujú naopak fungovanie v prostrediach, ktoré nie sú založené na dôvere voči sprostredkovateľovi.

Posun paradigmy v zdravotníctve teda nenastáva len vďaka aplikáciám virtuálnej reality a 3D tlače (bioprintingu), ale aj na základe uvedomenia si digitalizácie a práce s veľkými a cennými dátami. Už súčasné aplikácie blockchain technológií naznačujú, že ich výhodou je práve decentralizácia a s ňou súvisiaca bezpečnosť a relatívne nižšia nákladovosť v porovnaní s centralizovanými, nezriedka predraženými e-health riešeniami pokrývajúcimi obvykle úroveň štátu a to s rádovo nižšou úrovňou bezpečnosti dát v porovnaní s alternatívou v blockchain prevedení. Nie náhodou v lete 2016 rozhodla vládna agentúra USA aplikovať kryptotechnológie do zdravotníctva a vyhlásila verejnú súťaž pre návrhy týchto aplikácií. Rovnako je známe i spojenie spoločnosti HealthNautica a už spomínaného projektu Factom z roku 2015, kde bolo cieľom spojenie služieb vedenia zdravotnej dokumentácie s výhodami kryptotechnológií. Práve vlastnosť relatívnej „*immutability*“ (nemeniteľnosti) záznamu je pre zdravotné dáta mimoriadne významná. Ide o princíp, ktorý je v rámci dnes existujúcich databáz serióznym problémom. Zmeny záznamu, resp. anulovanie časti záznamu z akéhokoľvek iného motívu než existenčného, znamená navždy stratu kredibility v danú databázu či systém. Pozmenenie údaju treťou stranou v dnes vytváraných centralizovaných systémoch môže pacienta stáť v krajnom prípade i život.

Predstavme si príklad šifrovaného elektronického záznamu, ktorého časť majiteľ/pacient zámerne ponechal verejnú. Napríklad svoju krvnú skupinu pre prípad núdze. Alebo dokonca širší súbor údajov niečo ako „*Emergency Care Data Set (ECDS)*“, čiže unikátny biometrický identifikátor majiteľa/pacienta, ku ktorému sa personál v sanitke v mimoriadnej situácii bez problémov dostane. Nezmeniteľnosť údajov, teda aspoň bez majoritného konsenzu o tomto údaji, je kľúčovým pilierom

bezpečnosti dát. A práve nemennosť údajov vyplýva z podstaty kryptosystémov. Predstavme si, že sám pacient bude rozhodovať (bez námahy), komu svoje bezpečne uložené údaje sprístupní a možno že nebude nevyhnutnosťou, aby takúto aplikáciu pre kryptosystém vyvinul a zastrešoval štát, či iná centralizovaná inštitúcia.

Ďalším príkladom využitia kryptotechnológií môže byť jednoduchá automatizovaná, anonymná a rýchla procedúra v prípadoch, keď je potrebné potvrdiť spôsobilosť človeka na nejaký konkrétny úkon alebo vylúčiť prítomnosť vysoko-infekčného ochorenia a pod.. Automatizovaný IT systém napr. v turnikete pri pokuse človeka prejsť na verejné kúpalisko, či detské ihrisko, letisko na základe jeho biometrickej identifikácie, skenu ciev priloženej ruky a pod., overí konkrétnu položku v jeho zdravotnom zázname (ktorá je zaznamenaná na blockchaine určitého kryptosystému). Systém preverí, či nie je mimoriadnou biohazardnou hrozbou pre ostatných v danom chránenom priestore a podľa toho ho vpustí alebo nie. To všetko bez potreby interakcie tretej osoby, či nešifrovanej identifikácie, bez potreby záznamu o danom automatizovanom dopyte alebo prezradenia konkrétnej informácie daného človeka tretej strane (v prípade centralizovaných systémov napr. osobe, ktorá daný údaj kontroluje).

Aplikácia kryptotechnológií do existujúcich procesov v zdravotníctve je preto logická. Nepôjde pravdepodobne len o on-line uchovávanie a sprístupňovanie zdravotných záznamov, ale aj o prácu s veľkými dátami, či dynamickú možnosť analýzy a reakcie na informáciu v čase, napr. v prípade šírenia epidémie. Kryptosystémy v zdravotníctve umožnia týmto spôsobom vyššiu efektivitu, redukciu nákladov a zvýšenie bezpečnosti.

Krypto-technológie umožňujú vyraďovať sprostredkovateľov z existujúcich procesov, ktoré doteraz vyžadovali intermediátora, či už to bola banka, štát alebo v prípade zdravotníctva inštitúcia medzi pacientom a lekárom uchovávajúca centrálne jeho zdravotné údaje v „ére založenej na dôvere“. Ak by došlo k zrúteniu centralizovaných systémov resp. ku kríze dôvery, je tu technológia, ktorá vie spoľahlivo fungovať bez potreby dôvery v tretí článok a konkrétne pre bezpečnosť pacientskych dát to môže v takomto svete znamenať, že budú bezpečné presne do tej miery, do akej to bude preferovať ich majiteľ.

4.2.5 Smart kontrakty na verejné služby

Jedným z problémov, ktorý je dnes v oblasti poskytovania verejných služieb prítomný a o ktorom sa často diskutuje, je adresnosť pri využívaní akejkoľvek formy sociálnej podpory zo strany štátu. Za sociálnu podporu môžeme považovať nielen sociálne dávky, ale i prístup k vzdelaniu, k dopravným službám, či iným podporným politikám. Pri použití kryptotechnológií je možné tento problém čiastočne zmierniť a zároveň zabezpečiť, aby proces nebol byrokraticky náročný.

Smart kontrakty umožnia pridať peniazom nové vlastnosti a naprogramovať cashflow v ekonomike.

Potenciálne využitie kryptosystémov v oblasti verejnej sociálnej podpory v kombinácii s protokolmi ako „Colored coins“ bude umožňovať vytvoriť tzv. smart kontrakty (inteligentné kontrakty) a zautomatizovať cashflow v ekonomike alebo len v niektorých jej častiach. Umožní to vymedziť účel či služby, na ktoré budú peniaze použité. V princípe bude možné vytvoriť podmienené finančné príspevky, ktoré sa budú dať minúť len na vopred presne vymedzený konkrétny účel - na zdravotnú starostlivosť, lieky, potraviny a pod. u autorizovaných poskytovateľov tejto služby či produktu.

Ako oblasti využiteľnosti sa dajú uviesť - príspevky na vzdelávanie, verejná osobná doprava (MHD, železnice, autobusová doprava, spoplatnenie cestnej siete), verejné dotácie rôzneho druhu, či viazanosť sociálnych dávok na splnenie iných podmienok (napr. majetkových, platových, a pod.).

Dôležitý je fakt, že k tomu všetkému nebude potrebný byrokratický aparát, ktorý by kontroloval a vymáhal dané pravidlá, pretože všetky pravidlá môžu byť jednoducho vopred naprogramované do vlastností tokenu daného kryptosystému. Je do nich dokonca možné naprogramovať vlastnosť, ktorá peniaze vráti naspäť poskytovateľovi, v tomto prípade štátu, ak nebudú použité do určitého termínu.

Týmto to však ešte nekončí. Verejná organizácia si môže pomerne jednoducho naprogramovať náklady na mzdy, materiál či údržbu do svojho rozpočtu. Takéto vymedzenie účelu zamedzuje využitiu peňazí na neželané účely. Navyše, automatizácia týchto procesov vedie k dramatickému zníženiu byrokracie a šetrí nielen finančné a ľudské zdroje, ale aj čas.

5.Stručný popis technickej realizácie databázových zápisov

Informácie, ktoré dnes môžeme priamo využívať na zápis v blockchaine musia spĺňať dve základné podmienky. Po prvé presnú kvantifikovateľnosť. Tejto podmienke zodpovedá napr. presný počet metrov štvorcových na Slovensku vs. presný počet tokenov bitcoinového blockchainu (21 miliónov). Z tohto hľadiska je napr. kataster nehnuteľností vhodným príkladom na priame využitie blockchainu. Druhou podmienkou priameho využitia je, že vzťah medzi tokenmi blockchainu a v našom prípade presne definovaným počtom m^2 katastra musí byť po vzájomnom spárovaní vstupov a výstupov rovný nule, pričom nespárované výstupy tvoria vstupy budúcich transakcií na konci chainu.

Informácie zhora počtom neohraničené (napr. zdravotne záznamy obyvateľstva) by nemohli byť priamo zapisované do blockchianu, vzhľadom na to, že veľkosť databázy by mohla teoreticky narastať do nekonečna, čo je nezmyselná požiadavka, a zároveň by medzi nimi nejestvoval žiaden priamy vzťah umožňujúci anihiláciu vstupov a výstupov. Technicky je nezmyselnosť takejto požiadavky reprezentovaná nemožnosťou vykonania kontrolného súčtu. Kontrolný súčet je známy napr. z účtovníctva, kedy sa strana „ma dať“ musí rovnať strane „dal“. Inak dané účtovníctvo nie je správne a je nedôveryhodné. V prípade kryptosystémov by v prípade nesúladu nasledovala strata dôvery v daný blockchain a jeho následne zrútenie.

Avšak technológie krypto-sveta sa samozrejme dajú využiť aj na zhora neohraničené záznamy. Príklad môže byť zdravotný záznam. Ten, ako vieme, ma potenciálne neobmedzenú informačnú veľkosť („hrúbka zdravotného záznamu“ je rôzna pre každého človeka. Tento zdigitalizovaný záznam bude zašifrovaný a môže sa bezpečne distribuovať na užívateľov v celom zdravotnom systéme (poisťovne, nemocnice, lekári a pod.) alebo aj iným potenciálnym užívateľom (rodina, zamestnávateľ, štátna inštitúcia a pod.). Záznam by mohol mať samozrejme rôzne stupne dešifrovateľnosti a pridelene prístupové práva.

Na prístup k tomuto zašifrovanému súboru je možné opätovne využiť kryptosystémy a ich technológiu blockchainu. Ten poskytuje tzv. multisignature transakcie, čo z technického hľadiska umožňuje vygenerovanie prístupového kľúča k predmetnej úrovni zašifrovaných údajov. Napríklad k celému záznamu sa dostane iba jeho majiteľ (občan) použitím napr. Master Privat Key. Avšak v prípade jeho nehody / zranenia budú mať

prizvaní účastníci, napr. rýchla zdravotná služba možnosť vygenerovať prístup napr. ku krvnej skupine pacienta už podľa definovaných pravidiel a praktických situácií. Pre tento prípad (a podobné prípady zhora neobmedzených dát) by zároveň prichádzal do úvahy robustný a hlavne dôveryhodný blockchain (napr. špecializovaný derivát blockchainu Bitcoinu), ktorý bezpečne uschová záznamy o dobe, ale aj o úrovni vygenerovaných prístupových práv.

6. Záver

Využívanie krypto-technológií v bežnom živote obyvateľov si dnes vie málokto predstaviť. Ako je však vidno, potenciál ich využitia nie je len v súkromnej, ale i verejnej sfére. Môžu priniesť vyššiu bezpečnosť, transparentnosť, verejnú kontrolovateľnosť a automatizáciu mnohých činností, na ktorú dnes či už súkromný ale i verejný sektor vyžadujú mnohé ľudské zásahy. Tieto automatizované činnosti budú možné práve na základe dôvery v zápis a uchovávanie dát a ich využiteľnosti prostredníctvom blockchain technológií (napr. Bitcoinu).

Použitá literatúra

1. Andreas M. Antonopoulos. L.A. Bitcoin Meetup. (9.1.2014). WWW DOCUMENT <https://www.youtube.com/watchv=bTPQKyAq-DM>
2. Antonopoulos. A.M. (21.4.2014) L.A. Bitcoin Meetup - "Innovation without Permission". WWW DOCUMENT <https://www.youtube.com/watch?v=ctlPWdoe86A>
3. Bitcoin. WWW DOCUMNET <https://en.bitcoin.it/wiki/Main_Page>
4. Brown, R.G., A simple explanation of Bitcoin “Sidechains”. WWW DOCUMENT <https://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/>
5. Cabaj, A. Facebook diskusia. Česká Bitcoinová komunita. WWW DOCUMENT <https://www.facebook.com/groups/bitcoincz/?fref=ts>
6. Blockchain.info. Bitcoin Difficulty Chart. WWW DOCUMENT < https://blockchain.info/charts/difficulty?timespan=2year>
7. Counterparty. WWW DOCUMENT <http://counterparty.io/>
8. EARYLTEMPLE. Smart contracts for next-generation business. WWW DOCUEMNT <https://earlytemple.com>.
9. Etherum. WWW DOCUMENT <https://www.ethereum.org/>
10. Factom Blog. WWW DOCUMENT <https://www.factom.com/healthnautica-factom-announce-partnership/>
11. Factom. WWW DOCUMENT <www.factom.org>
12. MaideSafenet. WWW DOCUMENT <http://maidsafe.net/safecoin.html>
13. MCCRUDDEN, Christopher. Buying social justice: equality, government procurement, and legal change. New York: Oxford University Press, 2007, li, 680 p. ISBN 978-019-9232-437.
14. Omni. WWW DOCUMENT <http://www.omnilayer.org/>
15. Prisco, G. The Blockchain for Healthcare: Gem Launches Gem Health Network With Philips Blockchain Lab. WWW DOCUMENT <https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938>
16. Redman, J. U.S. Gov’t Announces Blockchain Healthcare Contest. WWW DOCUMENT <https://news.bitcoin.com/us-government-blockchain-healthcare/>
17. Ripple. WWW DOCUMENT <https://ripple.com/>
18. Snow, P. Deery, B. Lu, J. Johnston, D., Kirby, P. Factom. White paper. Business Processes Secured by Immutable Audit Trails on the Blockchain. WWW DOCUEMNT<https://github.com/FactomProject/FactomDocs/raw/master/Factom_Whitepaper.pdf>
19. Šíp, M. Facebook. (2.7.2016) Česká Bitcoinová komunita. WWW DOCUMENT <https://www.facebook.com/groups/bitcoincz/?fref=ts>
20. Zákon č. 323/92 Zb. o notároch a notárskej činnosti (Notársky poriadok)
21. Zákon č.343/2015 Z. z. o verejnom obstarávaní