Sľuby a riziká technológie Blockchain
ISACA Journal, Volume 4, 2018 – Autor Phil Zongo

Myšlienka distribuovanej účtovnej knihy, ktorá sa na verejnosti objavila v roku 2008 v publikácii „Bitcoin: Peer- to-Peer elektronický platobný systém“, sa z medializácie zmenila na skutočnosť skôr ako to experti predpovedali. Autor tejto publikácie sa po oznámení tohoto dômyselného šifrovaného systému stratil skôr, ako v roku 2011 tvorcom Bitcoin oznámil, že sa začal venovať iným aktivitám.
Posilnením mánie s kryptomenami bolo naštartovanie financovania vývoja nového webového prehliadača nazývaného „Brave“, ktorý počas počiatočnej ponuky približne za 30 sekúnd získal 35 miliónov USD. Inšpirovaný tradičným IPO – Initial Publlic Investing (štartovacia verejná ponuka na investovanie) je ICO - Initial Coin Investing metóda na získavanie finančných prostriedkov pre obchodovanie s kryptomenami. Pri tejto novej metóde začínajúce podniky poskytujú investorom digitálne tokeny na obchodovanie s kryptomenami, ako sú Ether a Bitcoin (kryptomeny - digitálne, alebo virtuálne meny, ktoré sú zabezpečené pomocou šifrovania).
Ether je kryptomena, ktorú podporuje sieť Etherum – decentralizovaná platforma, ktorá vykonáva inteligentné zmluvy (smart contract) pomocou technológie blokových reťazcov, ďalej „Blockchain“. Na rozdiel od IPO je väčšina ICO opatrne vytvorená tak, že tu nie sú klasifikované finančné aktíva, čo by automaticky znamenalo stanoviť finančné regulačné ustanovenia. Táto technológia, ktorá je základom Bitcoinu a iných virtuálnych mien je otvorená distribuovaná hlavná účtovná kniha, ktorá umožňuje dvom nezávislým partnerom, bez potreby garancie centrálnej autority ako je banka, obchodovať s hodnotami ako sú napr. duševné vlastníctvo, vlastnícke listiny, alebo virtuálne meny. Tieto transakcie sú pravidelne overované a použitím párom asymetrických šifrovacích kľúčov časovo postupne pripájané k záznamom v predchádzajúcom bloku. Na rozdiel od tradičných databáz, Blockchain nie sú umiestnené na centralizovanom mieste, ale sú distribuované medzi účastníkmi siete.
Technológia Blockchain ponúka možnosti ďaleko za sférou kryptomien, môže byť aplikovaná vo verejnom aj privátnom sektore a je predurčená zmeniť rôzne priemyselné odvetvia. Napr. umožňuje realizáciu platieb v zdravotníctve. Využitím vlastností decentralizovanej architektúry, Blockchain vytvára predpoklady nahradiť zastaralý, rozdrobený zdravotný systém a tak zlepšiť využitie zdravotníckych údajov. Ďalej vytvorením spoločnej databázy zdravotníckych informácií, lekári a poskytovatelia zdravotníckych služieb budú môcť pristupovať k rôznym zdravotníckym systémom, ktoré používajú. Z postupne vytváraných záznamov poskytne lekárom kompletný prehľad o pacientovi, čím umožní zvýšiť kvalitu zdravotníckej starostlivosti a zníženie jej nákladov. Ďalším odvetvím na využitie Blockchain je napr. komplexný svet operácií na finančných trhoch (futures, opcie, swapy, a i.)
Stratégovia Blockchain rozsah a dôveryhodnosť tejto rozkvitajúcej technológie prirovnávali k Webu, tvrdiac že Blockchain môže obnoviť Internet tým, že bude viac decentralizovaný, otvorený, privátny a dostupnejší.
Možnosti a výhody tejto technológie sú pozoruhodné, avšak skôr než vláda, spoločnosti a súkromné osoby prijmú Blockchain musia zvážiť tri základné problémy:
I. Nedostatok jasne stanovenej legislatívy,
II. Bezpečnostné zraniteľnosti
III. Spolupráca s existujúcim jadrom systému.

I. Chýbajúca legislatíva
Pre posúdenie významu tejto záležitosti je dôležité obzrieť sa do histórie, keď sa tvorili sa predpisy o bezpečnosti – s dôrazom na USA.
Následkom krachu na burze v roku 1929, pre obnovu dôvery verejnosti vo finančných trhoch

Kongres USA vydal v roku 1933 Securities Act a v roku 1934 Securities Exchange Act. Kvôli zabráneniu podvodných praktík pri ponukách cenných papierov na verejný predaj boli dané tiež požiadavky prikazujúce organizáciám viesť finančné priznania. Aby sa ešte viacej sprísnil dozor na trhu s cennými papiermi a boli chránení investori, v nasledujúcich rokoch vláda USA vydala mnoho ďalších zákonov - v roku 1939 Trust Indenture Act (Správa dlhových cenných papierov), ďalej v roku 1940 Investment Company Act (Riadenie podielových fondov) a v roku 1940 Investment Advisers Act (Regulácia investičných poradcov). Približne o 70 rokov neskôr v reakcii na Enron, WorldCom a Tyco, ktoré vykazovali nepravdivé finančné správy a kvôli ktorým zbankrotovalo niekoľko investorov, bol v roku 2002 podpísaný zákon Sarbanes-Oxley Act (SOX). Jeho cieľom bolo znížiť riziká a príčiny vzniku finančných podvodov v podnikoch a zvýšiť dôveru investorov.
Avšak až donedávna bolo len málo celosvetových pravidiel pre riadenie digitálnych mien a ICO. Strážcovia zákona sú si toho vedomí a začínajú konať. Odozvy sú sporadické a rozdielne. Krajiny ako Čína, Hong Kong majú nezákonné ICO, zatiaľ čo Austrália, Švajčiarsko a USA vydali jasné návody na bezpečnosť ICO. SEC - US Securities and Exchange Commision verejne napomenula celebrity, ktoré neuvážene propagovali ICO cez svoje účty na Twiteri. Jedna z najväčších afrických bánk - Centrálna banka Nigéria sa dištancovala od vydaných predpisov pre Bitcoin s vyjadrením: „Centrálna banka nemôže riadiť alebo usmerňovať Bitcoin, podobne ako nikto nemôže riadiť a usmerňovať Internet. Nevlastníme ho“. V snahe vysporiadať s touto novou výzvou, sa mnoho iných právnych výkladov ešte stále dotvára.
Rôznorodé predpisy a medzery v legislatíve vytvárajú pre používateľov vážne riziká. Krátko po celosvetovej finančnej kríze v roku 2007 bolo cieľom Bitcoinu pôsobiť ako protiváha centrálnemu riadeniu veľkých bánk a iných politických systémov – princíp označený ako kryptoanarchia (použitie asymetrickej kryptografie). Kryptoanarchisti nepredpokladali, že softvér a šifrovanie samo o sebe nedokáže chrániť investorov pred nevyhnutným vlastným konaním, nenásytnosťou a inými priestupkami komerčného sveta. Vynorili sa tri vážne problémy:
1) Výbuch Ponzi schémy
Nedostatok legislatívy a zmätok na danom trhu nalákal podvodníkov a zástancov pyramídových investícií (Ponzi schémerov). Po sľuboch o výnimočných výnosoch podvodnícki podnikatelia vlákali investorov do pasce a po uzavretí vkladu zmizli. Krutý príklad prišiel z Indie, kde spoločnosť OneCoin uviedla Blockchain vytvorený v Exceli a strácajúci sa portál zobrazoval podvodnícke obchody. V apríli 2018 Indický finančný úrad vykonal raziu, zabavil 2 milióny USD a poslal do väzenia 18 zamestnancov. Cez spracovateľa platieb v NSR OneCoin, ktorý sa vyhlásil za nasledovníka Bitcoinu dovtedy do podvodných fondov údajne stiahol najmenej $350 miliónov.
2) Nedostatok údajov pre porovnávanie výkonnosti ICO
Je potrebné povedať, že významná časť začiatočníkov nevytvárala podvodné ICO. Väčšina kryptomien obchodovaných na verejnosti nebola evidovaná a v účtovníctve nebola na strane aktív uvedená. Tento nedostatok uviedol BaFin - German Federal Financial Supervisory Authority, ktorý varoval investorov vyhlásením, že väčšina projektov financovaných pomocou ICO sú vo väčšine prípadov v štádiu experimentovania, a preto ich výkonnosť a obchodný model nebol nikdy testovaný. Bez historických dát je pre investorov ťažké výkonnosť ICO ohodnotiť a porovnávať.
3) Vysoká zložitosť zmlúv pre obchodovanie s kryptomenami
Návody pre obchodovanie väčšinou popisujú podmienky, základnú filozofiu a vlastnú zmluvu medzi investormi a vydavateľmi ICO. Tieto podmienky a zmluvy sú uplatňované bez centrálnej autority - formou inteligentnej zmluvy, ktorou je samostatný program a ten akonáhle sú základné podmienky splnené, vykoná prenos digitálnych aktív. Tu je však riziko,

že takéto inteligentné zmluvy môžu byť vykonané unáhlene, alebo podmienky sú nesprávne pochopené, alebo program nemusí spĺňať očakávania investora. Ďalšou zložitosťou je používanie žargónu pre šifrovanie ako napr. segwit, altcoins, halving, multsig atď. Väčšina investorov tiež často neporozumie, čo podpisujú a s čím súhlasia.

Zhrnutie nedostatočnej legislatívy

Z histórie máme skúsenosť, že súčasné výstrelky nedôsledne riadeného trhu s kryptomenami pripomínajú praktiky, ktoré predchádzali finančnej kríze v roku 2008. Ako o finančnej kríze uvádza vyšetrovacia správa vlády USA „ Kríza bola výsledkom ľudských zásahov, nečinností a nie zásahom prírody, alebo nefungujúcich počítačov. Narastajúci zoznam sprenevery najvyššieho stupňa pokračuje a vyžaduje uviesť tvrdý a jasný odkaz: Investori idú do vysokých strát na ICO trhu, ibaže vláda nezasahuje. Tento príklad popisujúci riadenie vývoja cenných papierov naznačuje, že regulačné orgány boli v minulosti nečinné, alebo spevnili zákony, až keď investori zaznamenali vysoké straty. Toto by sa nemalo stať s kryptomenami! Bolo by nerozumné úplne ICO zakázať, ktoré pri správnom použití predstavujú rozumnú alternatívu začínajúcich podnikateľov k získaniu kapitálu na financovanie strategických projektov. Ako tvrdí jeden učenec,"...bola by škoda, ak by kvôli prehnanej regulácii ICO zanikli tak rýchlo, ako sa objavili, pretože by mohli byť užitočné." Zákonodarcovia si môžu vziať podnet od Canada's Autorite des marches financiers (Kanadský úrad pre finančné trhy), kde pre ICO využívajú testovací systém (Regulatory Sandbox) slúžiaci na zaistenie súladu s legislatívou, oslobodenie ICO od prísnych registračných požiadaviek, ako napr. vydanie podnikateľského zámeru, registráciu ako obchodníka s cennými papiermi a i.

Pre tvorcov legislatívy je tiež dôležité vydávať zákony, ktoré nepovolia investovanie penzijných fondov a iných zdrojov verejného majetku do nestálych a neistých kryptomien alebo ICO. Ak sú pri obchodovaní s kryptomenami finančné prostriedky verejnosti významnou mierou rizika ohrozené, môže to mať dopad na celú ekonomiku. Taktiež predstavenstvo spoločnosti musí jasne definovať podmienky pre investovanie finančných prostriedkov do kryptomien a ICO.

II. Kybernetická bezpečnosť a zraniteľnosti

Zatiaľ čo sa spoločnosti s digitálnou transformáciou vyrovnali, občania vedia, že každá rodiaca sa technológia prináša nové zraniteľnosti s dopadmi, ktoré neboli doteraz celkom objasnené. Blockchain naviac prináša zložité riziká najmä v týchto dvoch prípadoch:

1) DAO štúdia - pohľad na mýtus o odolnosti Blockchain

Základný princíp, podľa ktorého by sa mal Blockchain odlišovať od tradičných aplikácií bola jeho odolnosť t j. predpoklad, že ak bola raz transakcia uložená do účtovnej knihy, digitálne opečiatkovaná, stáva sa trvalou a nezvrátiteľnou; vymazanie a zmena potvrdenej transakcie je nemožná. Na druhej strane transakcie spracované tradičnými aplikáciami môžu byť bez veľkej námahy zmenené, vymazané alebo zabudnuté.

2) Autori Blockchain prehlasujú, že jeho významnou vlastnosťou je dôvernosť. Na zvrátenie transakcie je potrebné veľké množstvo počítačového výkonu, pretože Blockchain na šifrovanie a dešifrovanie obsahu používa dva asymetrické kľúče, čím je zabezpečená vysoká úroveň autentizácie a odmietnutia. Naviac Bitcoin, ako prvá najúspešnejšia implementácia Blockchain, bola navrhnutá tak, aby odolávala možným útokom. Dann Kaminsky, vysoko uznávaný vedec na informačnú bezpečnosť, ktorý predtým v Internete objavil zraniteľnosť DNS - Domain Naming System, priznal, že sa veľakrát, ale márne pokúšal napadnúť a prelomiť Bitcoin.

Ak berieme do úvahy osud DAO - Decentralized Autonomous Organization, je názor o nezrušiteľnosti záznamov pridaných do Blockchain prehnaný. DAO založená v roku 2016, bola aplikácia pre Etherum, ,ktorá mala predávať tokeny pre investorov obchodujúcich s

kryptomenami. Títo investori mali za to nadobudnúť zisky vytvárané budúcimi DAO projektami. DAO bol hitom, ktorý od viac ako 11 tisíc fanatikov získal 150 milión USD, z ktorých 11 percent je dodnes vlastníkom kryptomeny Etherum.
V máji 2016, keď DAO začalo svoju činnosť, sa však sny a nádeje investorov rozplynuli. Hacker, ktorý využil chybu v programe, odčerpal z DAO približne 50 miliónov USD do duplikátu pôvodného DAO. Hodnota Etheru sa zrútila. Spoločnosť Etherum mala tri možnosti ako krádež riešiť :
1) potvrdiť hlavné princípy odolnosti a nechať útočníkovi ukradnuté prostriedky,
2) zničiť duplikát DAO a zaistiť aby hacker z toho nemohol profitovať, alebo
3) prepísať záznamy Etherum a vymazať krádež, čo sa nazýva „Hardfork“. (Hardfork znamená
zmenu záznamu predtým vytvoreného neplatného bloku s transakciami na platný a vyžaduje sa tiež upgrade záznamov u všetkých investorov).
Väčšina investorov bola za Hardfork. Zástancom Etherum nebola po vôli myšlienka vymazať, alebo úmyselne vybrať z Blockchain digitálne podpísané transakcie. Základné princípy boli pre nich sväté a šifrovanie bolo zákonom. Finančnú hodnotu útoku na DAO možno porovnať s mnohými inými vysoko profesionálnymi útokmi, ktorých dôsledky a výsledok Hardfork zvlnili hladinu istoty investorov Etherum. Komisia SEC - US Securities and Exchange Commission požadovala vyšetrenie a zverejnenie výsledkov. Tieto výsledky medzi expertami pre Blockchain podnietili prudké diskusie a tiež vyvolali vzburu medzi zástancami Etherum, ktorí sa rozhodli vydržať s pravou verziou Etherum, teraz známou ako Etherum Clasic.
DAO štúdia uvádza dve dôležité poučenia:
1) Všeobecne vyhlasovaná teória, že šifrovanie môže ochrániť Blockchain od vplyvov ľudského zásahu je prehnané. Ako jasne poukazuje prípad DAO, digitálne podpísané transakcie môžu byť ľudským zásahom manipulované. Idealistom, ktorí podporovali Hardfork, padli dva hlavné princípy – odolnosť a decentralizácia a riešenie je obdobou finančnej pomoci nasledujúcej po finančnej kríze v roku 2007, hoci mnohé banky vyhlásili, že sú príliš silné na to aby skrachovali.
2) Blockchains boli v minulosti vychvaľované, že sú dobre chránené, spoľahlivé a odolné. Avšak táto predpokladaná vlastnosť sa skoro stala Achilovou pätou. Falošný názor o odolnosti poskytovaný spoločnostiam, nebol podložený overeným stanoviskom o ich bezpečnosti.
Napríklad, začiatkom roku 2018 hackeri z japonskej burzy na kryptomeny Coinback ukradli 534 miliónov USD. Podľa všetkého coiny boli prístupné z Internetu na princípe horúcej peňaženky. Nedostatkom tu bola chýbajúca viacnásobná signatúra, ktorá je podobná viacfaktorovej autentizácii používanej pri elektronických transakciách. Iný príklad prišiel od Mt. Gox, inej japonskej burzy pre obchodovanie s Bitcoinami, ktorá v roku 2014 zbankrotovala, keď zlodeji z nej ulúpili 400 miliónov USD. Mt Gox podľa viacerých správ nemala dostatočné kontrolné procedúry a stala sa obeťou zlomyseľnosti dôverných osôb, ktoré na prezradenie privátnych šifrovacích kľúčov použili klasickú pascu (phishing). Zdá sa, že problémy s bezpečnosťou Blockchain sú viac ľudské ako technické.

Zvýšená zraniteľnosť Blockchain pri prístupe k údajom
Mnohé prípady použitia Blockchain vyžadujú úspešné pripojenie s existujúcimi úložiskami dát. Dobrým príkladom sú inteligentné zmluvy - softwér, ktorý zabezpečí, overenie a zrealizovanie zmluvy. Tieto zmluvy však žijú v uzavretom prostredí Blockchain a nevedia získať dáta vlastnými možnostiami. Riešenia tohto obmedzenia sa ujali mnohé firmy, ktoré rozvinuli špeciálne aplikácie (Smart Oracle - druh smart kontraktov), ktoré umožňujú Blochchain komunikovať s externými zdrojmi dát. Tu si treba však uvedomiť, že je nedostatok skúsených vývojárov, ktorí sa vedia vysporiadať so zložitosťou tejto technológie.

Výskum z polovice roku 2016 odhaduje 5 tisíc špecializovaných vývojárov schopných tvoriť softvér pre kryptomeny. Nedostatok skúsených vývojárov pre Blockchain zvyšuje možnosť zavedenia škodlivých vírusov a znefunkčnenia platformy Blockchain.
Navyše, prepojenie základných systémov s novo-vybudovanými platformami Blockchain rozširuje možnosti pre kybernetické útoky. Neisté rozhrania programovania aplikácií (API), nešifrované relácie, nedostatky v podnikovej logike, neisté koncové body, slabé overovanie, nechránené šifrovacie kľúče a iné zraniteľnosti sú zdrojom bezpečnostných problémov. Preto implementácie Blockchain s inými systémami vyžadujú starostlivú rovnováhu medzi ich vzájomnou spoluprácou a bezpečnosťou.

Riešenie problémov týkajúcich sa kybernetickej bezpečnosti
Systém, alebo technológie môžu proti počítačovým hrozbám poskytnúť nepriepustnú ochranu. Správny súbor kontrol by mal byť daný hodnotou a zraniteľnosťou podkladových aktív. Pri prijímaní Blochchain, by mali spoločnosti zvážiť týchto päť zásadných úloh:
1) Zaviesť pre projekty Blockchain prísne riadiace postupy a bezpečnostné kontroly,
2) Zaviesť technológie a procesy, ktoré zabezpečia, že kryptografické kľúče budú chránené pred neúmyselnou stratou alebo spreneverou.
3) Zvážiť uloženie súkromných kľúčov pre digitálne peňaženky mimo systému, napríklad na prenosné USB, použiť bezpečnostné schránky, alebo samostatné hardvérové peňaženky. Tu je však dôležité zdôrazniť, že žiadne z nich neposkytuje úplnú odolnosť proti finančným stratám.
4) Na prevod prostriedkov z konkrétnej adresy používať na prístup do digitálnych peňaženiek viacnásobný podpis (multisig) pomocou dvoch alebo i viac súkromných kľúčov, ktoré sú uložené oddelene.
5) Vypracovať podrobné bezpečnostné testovacie scenáre a zabezpečiť, aby účinnosť každej povinnej kontroly bola pred realizáciou nezávisle overené v karanténnom prostredí.

Prekážky transformačných zmien
Podobne ako pri iných trendoch, vzostup Blockchain vznietil dynamickú súhru kontinuity a inovácie. Dosiahnutie rovnováhy medzi inováciou a stabilitou podnikania nemôže byť riadené oddelene. Podniky, ktoré slepo bojovali proti zmenám, nedokázali sa im prispôsobiť a stratili tak svojich zákazníkov. Podľa výskumu, úradujúce firmy, zanedbávajúce digitálne inovácie môžu stratiť až 50 percent tržieb a 30 percentné zníženie príjmov a výnosov.
Blockchain môže nahradiť širokú škálu zastaralých, decentralizovaných aplikácií, najmä tých, ktoré podporujú procesy pre back-office. Pridaním ďalšej vrstvy zložitosti väčšina týchto systémov dlhé roky pretrváva a stále podporujú strategické výnosy. Tak je to v prípade austrálskej burzy cenných papierov (ASX), ktorá v roku 2017 oznámila, že svoj elektronický systém na registráciu zúčtovacieho domu CHESS - Clearing House Electronic Subscriber System, implementovaný v deväťdesiatych rokoch minulého storočia, nahradí riešením pomocou distribuovanej účtovnej knihy. Podniky boli transformované, ale dokumentácia, ako pre väčšinu týchto archaických aplikácií nebola dôsledne aktualizovaná, pretože tvorcovia sa buď presťahovali, alebo zomreli.
Okrem toho podniková kultúra, prvky spoločenského správania, ktoré sú stabilné a silne odolávajú zmenám, môžu tiež predstavovať významnú zotrvačnosť pri zavádzaní Blockchain, pretože zamestnanci odolávajú zmenám a držia sa svojich starých spôsobov práce.
Odpovede
Aby sme na prijatie zmien prekonali tieto technologické a kultúrne prekážky, významní podnikatelia si stanovili realistické ciele predtým ako prijali Blockchain. Namiesto toho, aby podnikli kroky na realizovanie Blockchain, kladú si otázky:
- Vykonal podnik hĺbkovú diagnostiku na odhalenie byrokracie a starých predsudkov? Ak

áno, navrhol podnik efektívne stratégie riadenia zmien na ich odstránenie?
- Aké strategické výhody môže získať využívaním technológie Blockchain?
- Ktoré strategické platformy, nahradené technológiou Blockchain, vedú k zníženiu dlhodobých problémov s prevádzkovými nákladmi, k zvýšeniu stability podnikov a k lepšiemu využitiu digitálneho prostredia?
- Aké odborné znalosti sú potrebné na vývoj Blockchain platformy, odstraňovanie a migráciu starších aplikácií a prepojenie rozhraní pôvodných aplikácií s Blockchain?
Blockchain, ktorý sa stále vyvíja, sľubuje riešenie niekoľkých naliehavých globálnych výziev. Napríklad, očakáva sa, že inteligentné zmluvy založené na Blockchain uľahčia priamy, transparentný a nezvratný prevod finančných prostriedkov od darcov k tým, ktorí to potrebujú, čím sa odstránia zbytočné sprostredkovateľské náklady. Ale ak sú problémy uvedené v tomto článku zľahčované, mohli by podkopať dôveru k tejto dôležitej technológii. Autor tejto myšlienky hovorí: "Ak to urobíme zle, technológia Blockchain, ktorá pôsobí tak sľubne, bude obmedzená alebo dokonca zmarená".

Preklad: Ing. Dušan Makoš, CISA