Sustainability - Environment - Safety ´2017
Zborník zo VII. medzinárodnej vedeckej konferencie, Bratislava, 24. november 2017
Proceedings of the 7th International Scientific Conference, Bratislava, November 24, 2017, Slovak Republic
Žilina: Strix et SSŽP, ESE-38, First Edition, ISBN 978-80-89753-14-7

VÝVOJ KRYPTOMIEN AKO SÚČASTI PODNIKATEĽSKÉHO PROSTREDIA

Antonín KORAUŠ - Stanislav BACKA

BUSINESS ENVIRONMENT AND CYBERSECURITY AS ITS COMPONENT

ABSTRAKT
Tento príspevok sa zaoberá problematikou podnikania a jeho prepojením s kybernetickou bezpečnosťou. V rámci vnútorného členenia sú vysvetlené základné pojmy, prepojenosť medzi podnikom a informačnou bezpečnosťou a legislatívne nariadenia. Vznik virtuálnych peňazí by nebol možný bez obrovských zmien v oblasti informačných a komunikačných technológií. Hlavne internet znamenal zásadnú revolúciu v dejinách ľudstva. Práve vďaka internetu bol možný vznik nových spôsobov komunikácie, služieb, elektronického obchodovania a dokonca virtuálnych svetov s vlastnou virtuálnou ekonomikou a vlastnými virtuálnymi peniazmi.

KĽÚČOVÉ SLOVÁ: *kybernetická bezpečnosť, podnikateľské prostredie, globalizácia, informačné a komunikačné technológie.*

ABSTRACT
This paper addresses business issues and their links to cyber security. Within the internal breakdown, the basic concepts explained the link between business and information security and legislative regulations. The creation of virtual money would not be possible without huge changes in the area information and communication technologies. Especially the internet was crucial a revolution in the history of mankind. It was through the Internet that new ways were created communications, services, e-commerce, and even virtual worlds with their own a virtual economy and its own virtual money.

KEY WORDS: *cyber security, business environment, globalization, information and communication Technologies.*

ÚVOD

Peniaze nás obklopujú každý deň, nie je človeka, ktorý by tento pojem nepoznal. Od vzniku peňazí uplynuli už stovky rokov. Počas tejto doby sa menila ich forma a ľudia neustále hľadali nové a lepšie spôsoby, ako uskutočniť obchod a platby za tovary a služby. Potrebujeme ich na uspokojenie svojich základných potrieb, na kúpu potravín, hygienických potrieb, ale pomáhajú nám aj si dopriať nejaký ten luxus do života. Peniaze často vystupujú ako investičný prostriedok, nielen fyzických osôb, ale častejšie u podnikateľov, firiem a rôznych korporácii. Ich cieľom je zainvestovať tak, aby ich návratnosť bola väčšia ako vklad.

Peniaze sa postupne vyvíjali od drahých kovov, papierových peňazí až k dnes vo veľkej miere rozšíreným elektronickým peniazom. V posledných rokoch je však veľká pozornosť venovaná pomerne novej forme – virtuálnym peniazom. Tento pojem predstavuje nejakú digitálnu menu, ktorou sa platí na internete, či už využívaná v hrách alebo sa za ne dajú kúpiť reálne služby a tovary.

Tento článok je zameraný na problematiku kybermien, ich počiatočného historického vývoja, ako vznikli, na akých systémoch vôbec pracujú, ich charakteristiku, čo sa pod nimi rozumie a čím sú od klasických peňazí odlíšené a prečo sú v niektorých smeroch výhodnejšie. Ďalej je charakterizovaná prvá digitálna mena DigiCash, ktorá sa stala akýmsi základným kameňom pre ostatné kryptomeny, ktoré po nej nasledovali, ako napríklad Bit Gold. Je tu tiež vysvetlený pojem „blockchain“, s ktorým sú kryptomeny spájané a na ktorom sú v podstate postavené. Je akýmsi stavebným kameňom fungovania digitálnych mien.

CHARAKTERISTIKA KRYPTOMENY

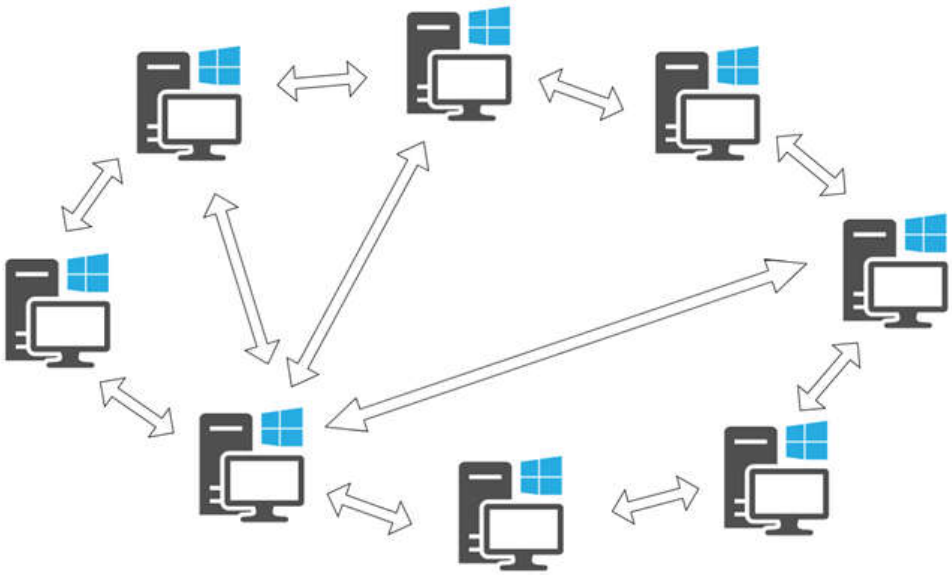
Kryptomena predstavuje pojem pre digitálne a virtuálne využívanú menu, ktorá je šifrovaná a chránená kryptografiou kvôli jej bezpečnosti, vďaka čomu je veľmi ťažké ju falšovať. To, čo je pri kryptomenách rozhodujúce a definuje ich „krásu“ je fakt, že kryptomeny nie sú vydávané žiadnym ústredným orgánom a tak sú teoreticky imúnne voči vládnym zásahom a manipulácii. Vďaka anonymnému pôvodu transakcií kryptomien sú kybermeny dobre nastavené a využívané pri nezákonných a škodlivých aktivitách ako napríklad pranie špinavých peňazí alebo daňové úniky. [9]

Kryptomeny sú vo svojej podstate peer-to-peer verzie elektornickej hotovosti, čo znamená, že pri platbách na internete, online platbách, sú peniaze priamo poslané druhej strane bez toho, aby platba prechádzala cez niektorú finančnú inštitúciu = decentralizovaná mena. [4]

Priame prenosy platieb pri kryptomenách je znázornené na obrázku číslo 1, kde je možné vidieť, že platby alebo dáta prechádzajú z jedného zariadenia na druhý bez toho, aby prechádzali cez ďalšieho prostredníka. Kryptomeny sú definované ako digitálna a virtuálna mena, často krát bývajú tieto pojmy brané ako rovnaké, pri najlepšom ako podobné. Avšak v tomto prípade sú tieto slová postavené ako slová s rozdielnym významom. Lee vysvetľuje, že je potrebné sa na tieto slová pozerať s iným významom, pretože hovoríme o finančnej mene založenej na elektronickom médiu, a teda slovo „virtuálna“ predstavuje menu, ktorá sa zdá byť reálna, avšak nie je a je držaná v „digitálnom“ (elektronickom) registri. Mena je teda reálna, ale nie reálna po fyzickej stránke (v čínskom jazyku znamená slovo „virtuálny“ byť vytvorený z ničoho), ale je generovaná počítačom. [4]

Oxfordský slovník definuje kryptomenu ako digitálnu menu, ktorej šifrovacie techniky sú použité na regulovanie generovania jednotiek meny a na overovanie transferov finančných prostriedkov a pracuje nezávisle od centrálnych bánk. [2]

Vzhľadom na to, že ide o decentralizovanú kontrolu, hodnoty kurzov kryptomien sú riadené ich užívateľmi a takisto zložitými protokolmi založené na ich riadiacich predpisoch, nie sú upravované vedomými rozhodnutiami centrálnych bánk alebo inými regulačnými orgánmi. Pre stabilitu a hladkú funkciu týchto kryptomien je rozhodujúca aktivita baníkov = používatelia šifrovacích systémov, ktorí využívajú obrovské množstvo výpočtovej sily na zaznamenávanie transakcií, na oplátku dostávajú novovytvorené kryptopremenné jednotky od iných používateľov. Je dôležité, že kryptomena môže byť vymenená za peniaze, tzv. fiatové peniaze (z ang. fiat money), preto každá z existujúcich kryptomien má svoj variabilný výmenný kurz s hlavnými svetovými menami (napríklad americký dolár, britská libra, európske euro a japonský jen). Kritiky výmenných kurzov sú trochu zraniteľné voči hackingu a predstavujú najbežnejšie miesto pre krádež digitálnej meny. [5]



Obrázok 1 Grafické znázornenie peer-to-peer siete
(zdroj: https://www.digitalcitizen.life/sites/default/files/gdrive/p2p/p2p__1.png)

VÝVOJ KRYPTOMENY

Všetko, čo na svete existuje prešlo svojím vývojom. Tak ako sa vyvíjal človek, tak isto sa vyvíjali aj peniaze. Ľudia vždy hľadali spôsob ako veci zdokonaľovať a tak sa aj zdokonaľoval a stále sa zdokonaľuje spôsob platby za tovary a služby. V minulosti sa najskôr využíval barterový obchod, kedy si obchodníci vymieňali tovar alebo služby za iné tovary alebo služby, tento spôsob nemusel vždy vyhovovať každému, kedy obchodník nemusel mať v ponuke takú službu alebo tovar, po akej sa opačná strana práve dopytovala. Preto sa ľudia snažili vymyslieť iný spôsob, ktorý by vyhovoval všetkým a tak sa neskôr prešlo ku obchodom, kedy sa platilo drahými kovmi, avšak nad tými nemusel disponovať každý, a tak aj tie ešte neskôr v rôznych formách vystriedali dnešné peniaze. Spolu s modernými technológiami prišlo, samozrejme, aj na to, že ľudia začali uvažovať aj o tom, ako prepojiť peniaze s internetom alebo teda ako lepšie, efektívnejšie pracovať s peniazmi alebo ako si privyrobiť.[5]

Základom kryptomien je šifrovanie, ktoré je zabezpečené vďaka príslušným algoritmom. Tento „oslepujúci“ algoritmus vznikol na začiatku osemdesiatych rokov minulého storočia, keď ho americký kryptograf David Chaum vynašiel. Dodnes sa tento algoritmus používa ako ústredný bod moderného šifrovania na webe. Vďaka tomuto algortimu sú možné bezpečné, nezameniteľné výmeny informácií medzi stranami a položil základ pre budúce elektronické menové prevody = známe aj ako „zaslepené peniaze“. [5]

Podľa Leeho celá história digitálnych peňazí začala prostredníctvom DigiCash-u, ktorého základ je tvorený už vyššie spomenutým algoritmom. DigiCash vznikol v roku 1990 v Holandsku vďaka Davidovi Chaumovi, kedy ponúkal svojim užívateľom možnosť virtuálnych peňazí, ktoré bolo možné posielať online alebo offline prostredníctvom kryptografických protokolov (zabezpečeniu) tak, aby chránili pred zdvojnásobnením výdavkov a takisto, aby chránili bezpečnosť užívateľa. Táto mena bola prístupná v bankách niektorých štátov ako napríklad Spojené štáty americké alebo vo Fínsku. Vzhľadom na to, že táto mena bola dostupná hlavne vďaka bankám, bol tento systém centralizovaný a regulovaný štátom. [4]

Svoju činnosť DigiCash sústreďoval priamo na jednotlivcov, ale Holandská centrálna banka sa proti tomu postavila a túto myšlienku ihneď zavrhla. DigiCash čelila ultimátu a tak súhlasila s predajom len licencovaným bankám, vďaka čomu vážne obmedzila svoj trhový potenciál. Avšak nádej

pre kryptomenu svitla, keď spoločnosť Microsoft oslovila DigiCash s ponukou o potenciálnom lukratívnom partnerstve medzi týmito spoločnosťami, ktorá by pre umožňovala skorým používateľom Windowsu nakupovať v tejto mene (konkrétne išlo o žiadosť Microsoftu, aby Digicash umiestnil svoj produkt na každý počítač so systémom Windows, začo spoločnosti bolo ponúknutých 180 miliónov dolárov)[13], no firmy sa nedokázali dohodnúť na spoločných podmienkach a tak od tejto myšlienky bolo upustené. Približne v tom istom čase dokonalý softvérový inžinier Wei Dai zverejnil bielu knihu o B-peniazoch, virtuálnej menovej architektúre, ktorá zahŕňala mnohé zo základných zložiek moderných kryptomien, ako sú komplexná ochrana anonymity a decentralizácia. B-peniaze však nikdy neboli rozmiestnené ako prostriedok výmeny. [5]

Chaumov, spolupracovník krátko na situáciu s Microsoftom vyvinul a vydal novú kryptomenu Bit Gold. Jej spomenutie stojí za zmienku, pretože táto mena začala využívať blockchain systém, ktorý sa stal základom pre väčšinu moderných kryptomien. Bit Gold však nikdy nezískal populárnu trakciu a už sa nepoužíva ako prostriedok výmeny. [5]

Čo je blockchain systém?

„Najväčšou devízou blockchain je však transparentnosť – aj preto sa nazýva „technológia pravdy“. Dáta sa ukladajú do samostatných úložných celkov zvaných „block“. Tieto bloky sa ukladajú do reťazca jeden za druhým, preto „chain“. Blockchain je distribuovaná databáza chránená šifrovaním tak, že zaručuje bezpečnosť informácií a chráni pred prístupom a úpravami od nevyžiadaných tretích strán.“ [1]

Možno konštatovať, že ide o databázu, kde sa „skladujú“ informácie, ktoré prejdú internetom. V tomto prípade môžeme hovoriť o centralizovanej a decentralizovanej blockchain siete. Centralizovaná databáza je databáza, ktorá je miestom, kde sa nachádza dátové centrum s veľkým počtom pevných diskov, rýchlym pripojením a s pocitom, že ak sa zničí toto dátové centrum, dôjde aj ku zničeniu dát. Decentralizovaná databáza na rozdiel od tej centralizovanej sa „stará sama o seba“. Nemala by mať žiadne slabé miesto, na ktoré by sa dalo zaútočiť, jednoducho neexistuje žiadna konkrétna lokalizácia, kde by sa informácie skladovali. Decentralizovaná blockchain databáza funguje na veľkom počte počítačov obyčajných ľudí, ktorí ťažia kryptomenu = mineri. [11]

William Mougayar vysvetľuje fungovanie tradičný spôsob zdieľania dát a decentralizovanej blockchainovej siete na príklade Google Docs verzus Microsoft Word. Oba programy sú známe a slúžia na písanie textov, prípadne textové úpravy, otvorenie textových dokumentov. V tomto príklade tradičný spôsob zdieľania dát predstavuje Microsoft Word. Mougayar píše, že na to, aby sme mohli zdieľať s inými ľuďmi Microsoft Word dokument, je potrebné ho najskôr uložiť do počítača a poslať, napríklad e-mailom, dotyčnej osobe, ktorá dostane dokument na upravovanie. V tomto momente, ak je dokument u druhej osoby na úprave textu, nemá k tomuto dokumentu prístup autor dokumentu a nedokáže ho v tomto momente modifikovať a pracovať s ním. Musí čakať na moment, kedy mu daný dokument druhá strana vráti. Podobným spôsobom pracujú aj banky a peňažné transfery, ak prebieha na strane banky práca s peniazmi, druhá strana má zablokovaný prístup k nim a účet otvoria ak je prevod dokončený a účet aktualizovaný. Avšak, ak si zoberieme dokument, ktorý bol vytvorený v Google Docs (blockchain sieť), na to aby mal k nemu prístup niekto druhý, je potrebné mu poslať internetový odkaz naň a prístup k tomuto dokumentu majú všetky osoby, ktoré naň dostali odkaz a zároveň ho môžu naraz modifikovať a inak s ním narábať v rovnakom čase a stále existuje len jedna verzia daného dokumentu. [7]

Po vývoji DigiCash-u sa transportovalo veľa finančných prostriedkov na podporu konvenčných digitálnych sprostredkovateľov, ako je napríklad PayPal, čo predstavuje online platobný systém, ktorý je možné využívať vďaka e-mailovým adresám, pod ktorými sú účty vedené. V tejto vlne vývoja nových systémov sa vývojári poučili z chýb na predchádzajúcich platformách a tak boli vytvorené nové platformy s vylepšeniami tu a tam, avšak PayPal sa stal absolútnym víťazom, vzhľadom na to, že ľuďom ponúkol to, čo vlastne chceli: peniaze na už známom webovom prehliadači. Služba PayPal ponúkla bezproblémový mechanizmus prenosu peer-to-peer a úhľadný spôsob akceptovania platieb pre obchodníkov. [13]

DigiCash bol takisto inšpiráciou pre mnohé ďalšie spoločnosti, ktoré vďaka imitácii DigiCashu naimitovali vlastné systémy v rôznych častiach sveta. Čo sa týka Spojených štátov amerických, na konci 90. rokov bola najvýznamnejšou virtuálnou menou mena známa ako e-gold. Spoločnosť, ktorá túto menu vyvinula, fungovala ako kupec digitálneho zlata. Zákazníci a používatelia mohli poslať svoje staré šperky zo zlata, mince alebo iné drobnosti do skladu a na oplátku dostali digitálne e-goldové jednotky denominované v unciach zlata. Používatelia mohli potom s týmito jednotkami obchodovať s inými používateľmi, vyberať zisk z fyzického zlata alebo vymieňať e-goldy za doláre. V polovici roku 2000 bolo e-gold na vrchole svojej existencie, malo niekoľko miliónov aktívnych užívateľov a každoročne spracovávalo transakcie vo výške niekoľko miliárd dolárov. E-gold vďaka svojím relatívne laxným bezpečnostným protokolom bolo populárnym cieľom pre hackerov a podvodníkov s phishingom a tak boli užívatelia vystavení finančným stratám. Platforma začala čeliť právnemu nátlaku, e-gold sa stal obľúbeným nástrojom pri praní špinavých peňazí a iným nezákonným aktivitám a tak v roku 2009 ukončila svoju činnosť. [5]

Záver

Rýchlosť a jednoduchosť platby je hlavnou výhodou kryptomien. Je potrebný len jeden platobný údaj a platba môže prebehnúť v poriadku v priebehu pár sekúnd až desiatok minút. Na uchovanie meny slúži peňaženka, ktorá môže byť v počítači, ale i napríklad v telefóne - platba pomocou QR kódu. Kryptomeny je možné využívať pre obchodovanie, zábavu, alebo zisk. Predávať ich možno v zmenárňach, keď je ich kurz vyšší a naopak. Prevodom na iné meny a využitím ich nárastov a prepadov potom je možné zostatok v peňaženke navršovať a mať na viac mikrotransakcií a platieb za drobnosti. Pri takomto konaní je dôležité sa riadiť predovšetkým platnými zákonmi a vlastným úsudkom. Obrovské objemy peňazí sa totiž stratili po napadnutí bezpečnosti zmenární, kedy boli pravdepodobne falošnými transakciami reprodukované a realizovali obrovské výbery. Užívateľom už asi nikdy ich Bitcoiny nebudú vrátené. Ďalším budúcim prínosom Bitcoinu môže byť schopnosť bezpečného zašifrovaného prenosu, kedy sa v budúcnosti veľa očakáva od prenosov ďalších mien, alebo dokumentov, povedzme prilepených k transakcii prenosu Bitcoinu. Tieto všetky aktivity je možné realizovať aj v rámci podnikateľského prostredia.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] Blockchain technológie na Slovensku 2017 [online]. Dostupné z: http://blockchainslovakia.sk/blockchain-ako-technologia-pravdy/
[2] Cryptocurrency [online]. Dostupné z: https://en.oxforddictionaries.com/definition/us/cryptocurrency
[3] Grafické znázornenie peer-to-peer siete [online]. Dostupné z: https://www.digitalcitizen.life/sites/default/files/gdrive/p2p/p2p__1.png
[4] Lee D., Kuo Chuen. 2015 Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Academic Press, ISBN 978-0-12-802117-0
[5] Martucci, B., What Is Cryptocurrency – How It Works, History & Bitcoin Alternatives [online]. Dostupné z: https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives
[6] Mougayar, W., Buterin, V. : 2016. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology , ebook, 208 pages Published April 26th 2016 by Wiley
[7] Mougayar, W., Explaining the Blockchain via a Google Docs Analogy [online]. Dostupné z: 7http://startupmanagement.org/2017/09/06/explaining-the-blockchain-via-a-google-docs-analogy/
[8] Pilkington, M.: Blockchain technology: principles and applications. In: Olleros, F.X., Zhegu, M. (eds.) Research Handbook on Digital Transformations. Edward Elgar, Northampton (2016)

[9] Satoshi : 2017. [online]. Dostupné z: https://www.investopedia.com/terms/s/satoshi.asp
[10] Scott, B.: Bitcoin Academic Research. The Heretic's Guide to Global Finance: Hacking the Future of Money, 30 December 2014
[11] Slavkovský, S.: 2017. Čo je Blockchain? [online]. Dostupné z: https://kryptomagazin.sk/co-je-blockchain
[12] Slavkovský, S. Ďalšie 3 kryptomeny do ktorých sa oplatí investovať, [online]. Dostupné z: https://kryptomagazin.sk/dalsie-3-kryptomeny-oplati-investovat/
[13] Team Koinex: A brief history of cryptocurrency [online]. Dostupné z: https://medium.com/koinex-crunch/a-brief-history-of-cryptocurrency-889fed168555
[14] University of Nicosia: Academic Certificates on the Blockchain, M.Sc. in Digital Currency - University of Nicosia (2014). [online]. Dostupné z: http://digitalcurrency.unic.ac.cy/certificates.

ADRESY AUTOROV

doc. Ing. Anton KORAUŠ, PhD., LL.M., MBA
Paneurópska vysoká škola Bratislava, Fakulta ekonómie a podnikania, Tematinská 10, 851 05 Bratislava
e-mail: akoraus@gmail.com

JUDr. Stanislav BACKA
Paneurópska vysoká škola Bratislava, Fakulta ekonómie a podnikania, Tematinská 10, 851 05 Bratislava
e-mail: stanislav.backa@gmail.com

RECENZIA TEXTOV V ZBORNÍKU
Recenzované dvomi recenzentmi, členmi vedeckej rady konferencie. Za textovú a jazykovú úpravu príspevku zodpovedajú autori.

REVIEW TEXT IN THE CONFERENCE PROCEEDINGS
Contributions published in proceedings were reviewed by two members of scientific committee of the conference. For text editing and linguistic contribution corresponding authors.