

BITCOIN – VIRTUÁLNA PEŇAŽNÁ MENA

Anton KORAUŠ

BITCOIN – VIRTUAL CASH CURRENCY

ABSTRAKT

Bitcoin je virtuálna open-source peňažná mena, ktorou je možné vykonávať peňažné prevody kedykoľvek a kdekoľvek na svete bez čakania a za bezkonkurenčne nízke poplatky prostredníctvom úplne decentralizovanej P2P siete. Bitcoin pracuje na princípe vzájomne klientskych aplikácií, ktoré sa starajú o bezpečné prevody a predvídateľnú tvorbu nových peňazí. Na fungovanie systému nemusí dohliadať banka, ani žiadna iná inštitúcia.

KLúčové slová: Bitcoin, virtuálna mena, peňažná mena, peňažné prevody

ABSTRACT

Bitcoin is an open-source virtual cash currency, which can perform money transfers anytime, anywhere in the world and without waiting for unbeatably low fees through a fully decentralized P2P network. Bitcoin works by each client applications that care about safe and predictable transfers creation of new money. To run the system does not oversee the Bank nor any other institution.

Keywords: Bitcoin, virtual currency, cash currency, money transfers

Jel Classification: E42, E49, E58

Úvod

Virtuálna mena Bitcoin a jej odvodené alternatívy sú v súčasnosti jednou z najaktuálnejších tém vo finančnom svete. Bitcoin je virtuálna mena a zároveň decentralizovaná sieť, prostredníctvom ktorej je možné vykonávať požadované peňažné prevody bez ohľadu na miesto a čas.

So zvýšením záujmu verejnosti o obchodovanie s virtuálnou menou bitcoin sa dostali do popredia aj mnohé jej ekonomické a právne otázky.

1. Predstavenie Bitcoinu

Bitcoin je decentralizované digitálne platidlo označované aj ako „virtuálna mena“, ktoré nie je kryté zlatom a mechanizmus jeho obehu zabezpečuje vysokú mieru anonymitu platiteľa a príjemcu. Bitcoin má podobu počítačového súboru. Prvkom zabezpečujúcim anonymitu používateľov a úplnosť transakcií je asymetrické šifrovanie, ktorým sa potvrdzuje autenticita prevodu platidla a tým sa umožňuje stranám transakcie, aby mohli obchodovať navzájom bez dodatočnej autorizácie treťou stranou.¹ Práve decentralizovanosť a anonymný beh platidla je dôvodom jeho rastúcej popularity. Bitcoin je deliteľný na osem desatinných miest umožňujúcich jeho jednoduché použitie pri platobných transakciách. Výmenný kurz sa určuje na základe ponuky a dopytu.

Hlavnou unikátnosťou Bitcoinu je jeho plná decentralizácia, ktorá je navrhnutá tak, aby nikto, vrátane autorov, skupín alebo vlád, nemohol menu nijako ovplyvňovať, falšovať, zabavovať účty, kontrolovať peňažné toky alebo spôsobovať infláciu. V sieti neexistuje žiadny centrálny bod, ani nikto, kto by mohol o sieť rozhodovať.

Bitcoin je deflačná mena. Celkové množstvo peňazí je konečné a je dopredu známe, a jeho uvoľňovanie do obehu je definované iba matematickými zákonmi. V sieti prebiehajú platby za minimálne alebo žiadne náklady.

V roku 2008 jednotlivcov, alebo skupina jednotlivcov pod pseudonymom Satoshi Nakamoto (neexistujú žiadne informácie o jeho identite alebo pôvode) publikoval správu popisujúcu digitálnu menu Bitcoin, stalo sa tak v Cryptography Mailing listu na metzdowd.com. Na internetovom fóre v roku 2009 uvádzal, že na Bitcoine pracoval od roku 2007. Nadviazal na článok³ z roku 1998 autora Wei Dai, absolventa Washingtonskej univerzity, ktorý predstavil víziu vytvorenia takeého prostriedku výmeny, ktorý nebude prechádzať cez zúčtovacie systémy finančných inštitúcií a do ktorého nebude možné zasahovať najmä zo strany vlády, resp. centrálnych bánk. Bitcoin nie je absolútnou novinkou, pretože v nedávnej minulosti už fungovali, resp. fungujú rôzne iné digitálne platidlá, napr. DigiCash, GoldMoney, Pecunix, Web-Money. Bitcoin je však doposiaľ zďaleka najprepracovanejším digitálnym platidlom.

Sieť funguje od roku 2009, kedy Satoshi Nakamoto predstavil kryptografickú štúdiu. V nej navrhol a vysvetlil princíp siete typu peer-to-peer, v ktorej zúčastnené systémy produkovali komplikované matematické výpočty na niečo čo sa nazýva

¹ Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System (2009), dostupné na <http://bitcoin.org/bitcoin.pdf>

² Deflácia je, v ekonomike, pokles všeobecnej cenovej hladiny tovaru a služieb (opak inflácie). Deflácia nastane, keď miera inflácie klesne pod 0 % (záporná miera inflácie). Inflácia znižuje reálnu hodnotu peňazí a naopak deflácia zvýši reálnu hodnotu peňazí či už v makroekonomike alebo mikroekonomike. Tým je možné nakupovať viac tovaru s rovnakým množstvom peňazí

³ Dai, W.: „b-money“, dostupné na <http://www.weidai.com/bmoney.txt>, 1998

„blockchain“. Výsledkom malo byť vytvorenie úplne novej, v tomto prípade virtuálnej meny: kryptomeny. Meny, ktorej základom je matematika. Názov štúdie znel: „Bitcoin: Peer-to-Peer Electronic Cash System“.

Nakamoto aktívne vyvíjal Bitcoin softvér aj po publikácii prvej verejnej verzie, ale v priebehu roka 2010 odovzdal svoj Bitcoin SourceForge projekt nástupcovi sa menom Gavin Andresen.

Keď sa Bitcoin stal cenným, ľudia sa čoraz viac zaujímali o Satoshiho Nakamotu. Ten poskytol niekoľko interview prostredníctvom e-mailov, ale potom úplne zastavil korešpondenciu, až nakoniec zmizol. Keď sa ho niektorí snažili vypátrať, uvedomili si, že Satoshi Nakamoto zrejme vôbec neexistuje. Takže dodnes nikto nevie, kto v skutočnosti vynašiel Bitcoin.

Zrejme kvôli povahe projektu autor nikdy neuvybral svoju skutočnú identitu a krátko po väčšom rozšírení Bitcoinu v roku 2010 sa odmlčal úplne. O projekt sa začali zaujímať ďalší vývojári a technologickí nadšenci. Dnes pre platby existuje oficiálny softvérový klient, o ktorý sa starajú dobrovoľníci z celého sveta a niekoľko alternatívnych klientov.

Od roku 2011 sa o Bitcoine, ekonomike, možnostiach a dôsledkoch tejto meny usporiadávajú konferencie, a to v New Yorku, v Prahe a v Londýne.

V septembri 2012 vznikla Bitcoin Foundation starajúca sa o infraštruktúru Bitcoinu, vrátane hlavného klienta, sledovanie hrozieb a prípadné vylepšovanie protokolu, zabezpečovanie konferencií a propagáciu meny. Vzhľadom k decentralizovanej povahe siete nadácia nemá žiadne zvláštne právomoci, v sieti vždy rozhodne väčšina, bez ohľadu na Bitcoin Foundation. Dnes sa okrem vývojárov a technologických nadšencov o Bitcoin zaujímajú aj obchodníci a investori.

2. Právna povaha bitcoinov

Moderné ekonomiky v súčasnosti používajú tzv. peniaze s núteným obehom (fiat money), ktoré sú síce podobné peniazom krytým určitou komoditou (napr. zlatom počas tzv. zlatého štandardu), ich koncept je však úplne odlišný a to tým, že nie sú naviazané na žiadnu komoditu. Vynútenie tu má formu právnej normy, ktorou orgán verejnej moci ustanovuje a zavádza konkrétnu sústavu peňazí a systematicky upravuje svojim právnym poriadkom jednotlivé aspekty jej obehu a ochrany⁴, čím zakotvuje menu ako právnu formu peňazí.

Ustanovenie meny je vždy právnym aktom a mena je jedným z atribútov suverenity štátu. Štát požíva takzvanú menovú suverenitu, ktorá v zmysle medzinárodnoprávnej zásady *lex monetae*⁵ znamená, že každý štát má výlučné právo vytvoriť si vlastnú menu (a disponovať s ňou), ktorú musia iné štáty a ich orgány rešpektovať. V podmienkach Európskej únie sa jej členské štáty na základe medzinárodnoprávného záväzku, ktorý je súčasťou ich prístupovej zmluvy, dobrovoľne vzdávajú vlastnej meny.

Peniaze s núteným obehom sú najčastejšie v právnom predpise určitého štátu uzákonené ako zákonné platidlo a vydáva ich ústredná autorita, čo je vo väčšine prípadov centrálna banka.

Z ekonomického hľadiska je potrebné zdôrazniť, že celý tento systém je založený na dôvere, teda na dôvere v to, že peniaze, ktorými osoba disponuje, bude schopná v ktoromkoľvek okamihu vymeniť za tovar alebo službu a osoba poskytujúca tovar alebo službu bude ochotná tieto peniaze prijať ako protihodnotu.

Vzhľadom na to, že bitcoin nespĺňa atribúty meny v právnom zmysle (jeho platnosť na určitom území nie je mocensky ustanovená, právny poriadok neupravuje jej obeh ani ochranu), zastávame názor, že ho nie je možné označovať za menu. Na účely tohto článku budeme používať označenie „virtuálna mena“ alebo „platidlo“.

Bitcoin, resp. iné elektronické platidlá, napriek ich novej podobnosti treba odlišovať aj od elektronických peňazí. Týmto problémom sa zaoberala aj Európska centrálna banka. Predpisy európskeho práva⁶ definujú elektronické peniaze ako „peňažnú hodnotu uchovávanú elektronicky vrátane magnetického záznamu, predstavujúcu záväzok vydávateľa vystavený pri prijatí peňazí na účel vykonávania platobných transakcií v zmysle definície v článku 4 bode 5 smernice 2007/64/ES⁷, prijímanú aj inými fyzickými alebo právnickými osobami, než je vydavateľ elektronických peňazí.“

Podľa ECB, aj keď bitcoin splňuje niektoré prvky tejto definície, elektronické peniaze sú aj v elektronickej podobe vyjadrené v mene príslušného štátu, čo neplatí pre bitcoin, keďže tie sa vyjadrujú len vo forme bitcoinov.⁸ Elektronické peniaze sú práve regulované a finančné inštitúcie, ktoré pracujú s elektronickými peniazmi, podliehajú dohľadu príslušných vnútroštátnych orgánov, čo však neplatí pre Bitcoin.

Napokon bitcoin nemá ani povahu finančného nástroja. Ustanovenie § 5 zákona č. 556/2001 Z. z. o cenných papieroch a investičných službách obsahuje taxatívny výpočet finančných nástrojov, ktorý neumožňuje bitcoin subsumovať bitcoin pod žiadny z existujúcich finančných nástrojov, a to ani pri použití extenzívneho výkladu.

3. Vydávanie a obeh bitcoinov

Vydávanie bitcoinov a ich uvádzanie do obehu je decentralizované. Prvý bitcoin bol uvedený do obehu v roku 2009. Objem platidla v obehu sa zvyšuje automatickým generovaním nových bitcoinov v počte 25 ks každých približne 10 minút. Tento proces sa nazýva dolovanie bitcoinov (Bitcoin mining). Môže ho realizovať každý, kto si stiahne a spustí program na

⁴ Mankiw, G.: Zásady ekonómie. Grada Publishing, Praha, 2009, s. 573

⁵ K tomu pozri TOMAŠEK, M.: Pojetí zásady *lex monetae* v právu ES. In *Evropské a mezinárodní právo*, 3/1998, s. 12–15

⁶ Smernica Európskeho parlamentu a Rady 2009/110/ES zo 16. Septembra 2009 o začatí a vykonávaní činnosti a dohľade nad obozretným podnikaním inštitúcií elektronického peňažníctva, ktorou sa menia a dopĺňajú smernice 2005/60/ES a 2006/48/ES a zrušuje smernica 2000/46/ES.

⁷ Smernica Európskeho parlamentu a Rady 2007/64/ES z 13. Novembra 2007 o platobných službách na vnútornom trhu, ktorou sa menia a dopĺňajú smernice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a ktorou sa zrušuje smernica 97/5/ES, U. v. EU L 319, 5.12.2007, s. 1–36

⁸ European Central Bank, Virtual Currency Schemes (Oktober 2012) dostupné na <http://www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, s. 16

získavanie bitcoinov (Bitcoin's mining program). Celkové množstvo bitcoinov v obehu je fixne limitované na 21 miliónov a tento počet by mal byť dosiahnutý v roku 2040.

Obeh Bitcoinov sa realizuje prostredníctvom internetu na princípe priamej komunikácie, ktorá je prevádzkovaná bez centrálného servera (peer-to-peer) a spolieha sa na výpočtovú silu počítačov jednotlivých užívateľov.⁹ Platiteľ aj príjemca musia mať pridelenú špecifickú adresu – alfanumerický reťazec, ktorý predstavuje tzv. verejný kľúč na šifrovanie odosielaných platieb a overenie autentickosti prichádzajúcich platieb. Platiteľ môže platbu realizovať, len ak má súkromný kľúč, ktorým podpíše odchádzajúcu platbu. Odosielanie a prijímanie platieb sa uskutočňuje prostredníctvom online alebo offline programu, tzv. digitálnej peňaženky. Súkromný kľúč sa uschováva v peňaženke alebo na dátovom nosiči, ktorý môže mať podobu napr. mince.

V súčasnosti pomerne rýchlo vzrastá počet subjektov, ktoré sú ochotné akceptovať bitcoin ako platobný prostriedok, pričom najväčší počet týchto subjektov predstavujú internetové obchody.

Cena tovarov a služieb sa určuje na základe výmenného kurzu bitcoinu k inej mene. Bitcoin sa síce prevádzajú online, avšak rovnako ako pri hotovosti môžu byť zničené alebo stratené. Digitálna peňaženka umožňuje jednoduché uloženie bitcoinov na svoj online účet, ktorý je však pod správou tretej strany, z čoho môže vzniknúť nebezpečenstvo straty bitcoinov alebo môže dôjsť k ich krádeži hackermi. Výhodou ich úschovy prostredníctvom online peňaženky je prístup k vlastným bitcoinom z ktoréhokoľvek počítača.

Ako alternatíva môže slúžiť uloženie bitcoinov vo vlastnom osobnom počítači. Aj v tomto prípade však hrozí riziko ich straty, pretože osobný počítač môže byť nainfikovaný vírusom alebo môže dôjsť k jeho poškodeniu, čím môžu byť všetky bitcoiny vymazané.

Pokiaľ ide o výmenu bitcoinov za oficiálne meny, možno ju realizovať podobne ako pri tradičnej zmene jednej meny za inú, teda prostredníctvom online výmeny. Na tento účel vzniklo niekoľko online zmenární, z ktorých najväčšia a najznámejšia je Mt. Gox.¹⁰ Popri online zmenárňach sa dajú Bitcoin vykonať aj priamou výmenou, ak sa nájde niekto, kto ich je ochotný vymeniť za hotovosť.

4. Bezpečnosť Bitcoin

Skutočnosť, že táto mena nie je krytá žiadnou reálnou komoditou, rieši verejná história transakcií, vďaka ktorej sa je možné dopátrať, že konkrétne Bitcoin boli vytvorené. Takto sa vlastne overuje, odkiaľ a kam sa presúvajú a aký je ich objem, aby nevznikla double-spending¹¹. Napriek tomu, že sieť je decentralizovaná, transakcie sa musia niekde spracovávať a overovať. Z hľadiska bezpečnosti sa na verifikáciu vlastníctva Bitcoinov využívajú digitálne podpisy.

Na ukládanie a overovanie transakcií sa používa verejne dostupná distribuovaná databáza transakcií. Distribuovaný databázový systém je množina uzlov počítačovej siete, navzájom prepojených v komunikačnej sieti. Tieto uzly navzájom spolupracujú tak, že z každého uzla je možné sprístupniť údaje uložené na inom uzle presne tak, akoby boli umiestnené na vlastnom uzle.

V prípade plnohodnotného klienta je možné sa na obsah databázy pýtať iného dôveryhodného uzla, poprípade si udržovať len jej časť. Tak každý uzol vie, ktorý Bitcoin v sieti patrí ktorej virtuálnej peňaženke.

Všetky transakcie používateľov sú zaznamenané v histórii a uložené v blokoch, ktoré na seba nadväzujú. Tieto bloky sa nevytvárajú automaticky. Na rad prichádzajú takzvaní mineri¹², ktorí zabezpečujú chod siete poskytovaním výpočtovej sily. Aby mohli používatelia bezpečne platiť menou, mineri riešia matematický problém vo forme silnej šifry.

5. Ťažba a pohyb kurzu Bitcoin

Ťažiť Bitcoin môže každý, kto vlastní počítač. Stačí k tomu špecializovaný softvér, pre Windows napríklad GUIMiner. Zarobiť sa na tom dá, ale dnes už veľmi zložito. V začiatkoch sa Bitcoin ťažil čisto pomocou procesora (CPU) počítača. Tento spôsob je dnes už neefektívny.

Ďalším krokom bola ťažba pomocou grafickej karty v PC. Čím je grafická karta výkonnejšia, tým samozrejme lepšie.

V dnešnej dobe sa ťažba Bitcoin opláť iba pomocou špecializovaných zariadení, tzv. ASIC jednotiek. V podstate jediná cesta, ako nejaké Bitcoin vykopat' je teda ASIC alebo mnoho výkonných grafických kariet.

Dnes sú známe veľké počítačové siete, ktoré ťazia Bitcoin, prípadne konkurenčné kryptografické meny (napr. Litecoin). Základná myšlienka ťažby je jednoduchá: ak niekto vlastní výkonný počítač, môže si zarobiť peniaze. Bohužiaľ, tieto počítače nemusia byť vlastné. Je možné nainfikovať počítač niekoho iného, ktorý má systém Windows XP. Pri jeho 100% využití ťaží po celý deň mince v hodnote desiatok tisíc dolárov – možno pre jednotlivca, možno pre počítačové gangy. Je možné predpokladať, že aj v budúcnosti bude podobná ťažba v kruhoch online kriminálnikov veľmi populárna.

Ešte dôležitejšie je, že vyššie popísaný útok si na to, aby mohol zarábať peniaze, nevyžaduje od používateľa počítača nič. Väčšina tradičných mechanizmov si vyžadovala účasť používateľa. Napríklad, keyloggre kreditných kariet potrebujú aby majiteľ karty sám zadal svoje platobné údaje. Iba tak môžu získať prístup k jeho dátam. Na ťažbu kybernetických mien však stačí len výkon procesora a pripojenie počítača k sieti.

Niektoré z nových kryptomien nepotrebujú na to, aby vykonávali ťažbu, vysokovýkonné GPU¹³: postačí obyčajné CPU¹⁴. Ak sa k tomu pridá fakt, že dnes je v každej domácnosti čoraz viac procesorov je možné predikovať zaujímavý vývoj: budú

⁹ Podobnou sieťou je známa Bit-Torrent, prostredníctvom ktorej sa zdieľajú rôzne súbory ako filmy, hry alebo hudba

¹⁰ Mt. Gox, <http://mtgox.com/>. V auguste 2013 sa 1 bitcoin predával, resp. kupoval v priemere za necelých 136 dolárov.

¹¹ Minutie tých istých peňazí dva krát

¹² baníci

¹³ Grafický procesor (ang. graphics processing unit, skráteno GPU alebo novšie aj visual processing unit, skráteno VPU) je procesorslužiaci na výpočet grafických informácií pre zobrazenie údajov z počítača (alebo iného zariadenia spracovávajúceho digitálne dáta) na viditeľný

existovať botnety¹⁵, vyrábajúce peniaze ťažbou na sieťach, ktoré sa vytvoria so zapnutých elektronicky ovládaných zariadení. Môžu to byť napríklad infikované elektrické rúry, varné konvice, mikrovlnky, tlačiarne, TV, mobily a pod.

Mikrovlnky, práčky, tlačiarne s vloženými počítačmi a pripojením na internet môžu byť v budúcnosti realitou. Predtým ako existovali kryptomeny, by bolo ťažké pochopiť, prečo by sa niekto snažil vymyslieť spôsob, ako infikovať práčku. Ťažobný botnet, ktorý nainfikuje tisíce práčok, však môže zarobiť dosť peňazí na to, aby odôvodnil takéto zmysľovanie.

Algoritmus, na ktorom stojí Bitcoin, rieši dva hlavné problémy kryptomien: ako potvrdiť transakciu a ako implementovať nové jednotky meny do systému bez toho, aby dochádzalo k inflácii. Neexistuje tu žiadny centrálny bankový systém, ale transakcia musí byť nejakým potvrdená. V opačnom prípade by sa dali vyrobiť falošné peniaze. V bitcoinovom systéme preto potvrdenie vystavuje nejaký iný člen peer-to-peer siete. Najmenej šesť členov siete musí potvrdiť transakciu predtým, ako sa vykoná. Otázka znie: Prečo by niekto potvrdzoval transakcie pre ostatných? Odpoveď je jednoduchá: Pre zisk. Bitcoin odmeňuje členov, ktorí potvrdzujú transakcie. Toto sa nazýva „mining“, čiže ťažba. V začiatkoch Bitcoinu bola ťažba ľahká a ľahko sa dali zarobiť desiatky Bitcoinov pomocou svojho osobného počítača. Ako hodnota Bitcoinu rástla, rástla aj ťažba a bolo čoraz náročnejšie sa k Bitcoinom dostať, keďže záujemcov bolo čoraz viac. Aj keď kurz dolára k Bitcoinu kolísal, trend bol rastúci. Na začiatku roka 2013 bol výmenný kurz Bitcoinu asi 8 USD, v lete už 130 USD, t. z. že Bitcoin má veľmi reálnu hodnotu v reálnom svete.

Vytvorenie platného bloku vyžaduje veľký výpočtový výkon. Miner, ktorému sa podarilo vygenerovať blok, dostane za výpočtovú prácu zaslúženú odmenu. Sú ňou úplne nové Bitcoin. Aktuálna výška odmeny za spracovanie jedného bloku transakcií je 25 BTC. Tá sa mení v závislosti od počtu vytvorených blokov. Po každých 210-tisíc blokoch sa táto odmena zníži na polovicu.

Pre minerov je vhodné zriadiť si účet v Bitcoin poole, čo je zoskupenie mnohých ťažiarov, ktorí "kopú" spoločne. Akonáhle jeden člen nájde nový blok a získa odmenu, je rozdelená medzi všetkých účastníkov poole podľa toho, koľko na člena pripadá čiastkových výsledkov.

Obťažnosť generovania blokov sa pravidelne aktualizuje podľa výpočtovej sily všetkých minerov. Počet vytvorených Bitcoinov bude stále klesať, až kým nebudú vyťažené všetky Bitcoin. Momentálne je vyťažovaných približne necelých 11 miliónov z celkového počtu 21 miliónov Bitcoinov.

Záver

Je názor, že Bitcoin je v relatívne skorej fáze v porovnaní s hypotetickým potenciálom, a teda je úplne normálne, že táto cesta je plná prekážok a rýchlych zmien.

V prospech udržateľnosti tohto peňažného systému hovorí, že má za sebou skoro päťročnú históriu, prekonal niekoľko technických kríz a už existuje niekoľko implementácií v rôznych programovacích jazykoch. V neposlednom rade Bitcoinu pomáha aj to, že sa zväčšuje jeho praktické využitie a vyjasňuje aj právna situácia. Napríklad Nemecko túto menu oficiálne uznalo. Takže ju môže potenciálne v budúcnosti zdaňovať.

Ďalšími výhodami sú rýchlosť platby, nízke náklady transakcie a anonymnosť, čo oceňuje určitá skupina ľudí.

Užívatelia tejto virtuálnej meny si tak na volatilitu musia zvyknúť alebo sa voči tomu poistiť. Sprostredkovatelia platobných systémov napríklad takéto služby bežne využívajú, takže obchodníci prijímajúci platbu Bitcoinom nemusia byť odborníkmi na finančné trhy.

Výhodou pri obchodovaní s bitcoinmi je zníženie transakčných nákladov na minimum. Transakcie sa môžu uskutočniť kedykoľvek, kdekoľvek a nevyžadujú si priamu interakciu medzi účastníkmi transakcie. To znamená výrazné úspory, pokiaľ ide o produkciu, prepravu a manipuláciu s fyzickými peniazmi. Odhadované ročne náklady pri manipulácii s americkým dolárom americkými maloobchodníkmi a bankami je 60 miliárd dolárov, pričom táto suma zahŕňa náklady na spracovanie a

grafický obraz zobraziteľný na monitore. Prevádza digitálne dáta do formy zobraziteľnej pomocou obrazových pixelov. Nachádza sa buď na grafickej karte alebo ako samostatný čip na matičnej doske počítača (vtedy hovoríme o integrovanej grafickej karte).

Úlohou grafického procesora nie je len jednoduché zobrazenie dát, ale aj prepočty virtuálnych trojrozmerných obrazových scén v reálnom čase. Vtedy hovoríme o 3D akcelerátoroch. GPU vykonáva všetky grafické inštrukcie čím šetrí strojový čas mikroprocesora počítača, a zrýchľuje dostupnosť údajov. Tieto nemusia pri spracovaní v CPU putovať prostredníctvom zbernice do operačnej pamäte a odtiaľ do grafickej karty. V praxi to znamená že v keď sa v programe vyskytne inštrukcia pre spracovanie obrazu, tú nevykoná CPU, ale GPU. GPU je skutočným procesorom s klasickou architektúrou disponujúcou výkonovými jednotkami (jednotka transformácií, osvetlenia, nastavenia a renderovania). Hlavnou činnosťou moderného GPU je rendering, čiže vizualizácia, tvorba reálneho obrazu na základe počítačového modelu so zohľadnením charakteristík scény a jej okolia. Model (zobrazovaný objekt) je charakterizovaný sieťou alebo drôtovej konštrukciou a je mu priradený definovaný povrch a vzťah k dopadajúcemu svetlu. Scénu charakterizuje umiestnenie svetiel a kamery, okolie farba resp. obraz v pozadí, hmla, vodné a svetelné efekty. Program na základe matematických algoritmov skonštruje bitmapový obrázok simulujúci resp. napodobujúci reálnu sceneriu. GPU potrebuje nielen dostatočne širokú zbernicu, ale aj podporu rýchlejšie pamäte umožňujúcej zápis a čítanie údajov. http://sk.wikipedia.org/wiki/Grafick%C3%BD_processor

¹⁴ CPU (skr. z angl. central processing unit, často prekladané ako centrálna procesorová jednotka) je hlavný procesor počítača. Interpretuje, vykonáva alebo spracúva inštrukcie alebo dáta programu vo forme strojového kódu. Dnes sú centrálny procesorové jednotky takmer vždy realizované vo forme mikroprocesora. CPU sa v slovenčine oficiálne označuje ako procesor základnej jednotky alebo skrátené základná jednotka alebo procesor (tiež: procesor ústrednej jednotky, centrálny procesor, ústredný procesor). Osobný počítač (PC) obsahuje obvykle len jednu CPU. V minulosti sa objavili aj riešenia s viacerými CPU, dnes sa dáva prednosť jedinému, ale viacjadrovému CPU. Existujú superpočítače s viacerými integrovanými procesormi, ktoré vzájomne spolupracujú. <http://sk.wikipedia.org/wiki/CPU>

¹⁵ **Botnet** je sieť softvérových robotov, ktoré ovláda hacker. Hacker spojí počítače infikované podvrhnutým kódom do jedného botnetu. Tisíce infikovaných počítačov vykonáva bez vedomia používateľov počítača naprogramovanú úlohu, napríklad zahŕňa a zablokujú koordinovaným útokom zvolenú webovú stránku, hromadne zasielajú spam, phishing a podobne.

počítanie peňazí, ich uloženie, prepravu a ich zabezpečenie.¹⁶ Transakcie sú anonymné, účty nie sú nikde zaregistrované a bitcoiny sa posielajú priamo z jedného účtu na druhý.

Na druhej strane jedným z často zmieňovaných negatív je vysoká volatilita výmenného kurzu bitcoinov vo vzťahu k oficiálnym menám. Neexistuje žiadny pevne stanovený výmenný kurz medzi bitcoinmi a bežnými menami. V máji 2010 sa jeden bitcoin predával, resp. kupoval za 50 centov. V júni 2011 jeho hodnota prudko vzrástla až na 30 dolárov, no v októbri 2011 spadla na úroveň dvoch dolárov. Veľké výkyvy zaznamenala hodnota bitcoinu aj počas cyperskej krízy v marci 2013.

Jedným z najnovších prípadom je zastavenie činnosti internetového trhoviska Silk Road, kde sa obchodovalo aj s bitcoinmi. Ako reakcia na túto udalosť spadla hodnota bitcoinu o 8,6 % na úroveň 128 dolárov za jeden bitcoin. Toto všetko poukazuje na citlivosť bitcoinov na množstvo vonkajších udalostí.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

- [1] Bollen, Rhys, The Legal Status of Online Currencies: Are Bitcoins the Future? (May 1, 2013). Journal of Banking and Finance Law and Practice (2013). - [on-line] Available on - URL: <http://ssrn.com/abstract=2285247>
- [2] Kaplanov, Nikolei M., Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation (March 31, 2012). Temple University Legal Studies Research Paper. - [on-line] Available on - URL: <http://ssrn.com/abstract=2115203> or <http://dx.doi.org/10.2139/ssrn.2115203>
- [3] Plassaras, Nicholas, Regulating Digital Currencies: Bringing Bitcoin with in the Reach of the IMF (April 7, 2013). Chicago Journal of International Law, 14 Chi J Intl L (2013) Forthcoming. - [on-line] Available on - URL: <http://ssrn.com/abstract=2248419>
- [4] Robert J. Barro and Vittorio Grilli (1994), European Macroeconomics, chap. 8, p. 142. ISBN 0-333-57764-7
- [5] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2009) - [on-line] Available on - URL: <http://bitcoin.org/bitcoin.pdf>
- [6] Selgin, George, Synthetic Commodity Money (April 10, 2013). - [on-line] Available on - URL: <http://ssrn.com/abstract=2000118> or <http://dx.doi.org/10.2139/ssrn.2000118>
- [7] Tomašek, M.: Pojeti zásady lex monetae v právu ES. In Evropske a mezinárodní právo, 3/1998.

ADRESA AUTORA:

Ing. Anton Korauš, PhD., LL.M., MBA, Národná rada SR, Bratislava

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.

¹⁶ David G.Hayes et al.: An introduction to Electronic Money Issues (unpublished report prepared for the US Dept. Of Treasury, 1996), dostupne na <http://www.occ.gov/topics/bank-operations/bit/intro-to-electronic-money-issues.pdf>