Andrej Ivanuša

RUDARJENJE BITCOINOV

Rudarimo lahko tudi s pomočjo računalnikov

Denar je menjalno sredstvo. Na začetku so se veliko uporabljali kosci kovine, a tudi morski polžek kavri. Kitajci so izumili papirnati denar. S prihodom računalnikov je denar pričel spreminjati obliko iz resnične v namišljeno. Postal je samo dolg niz številk v elektronski obliki. S prihodom interneta dajemo denarju še novo značilnost.

RUDARJENJE »BITKOJNOV«

Ob moji pisarni je pisarna prijatelja, ki sestavlja in servisira računalnike. Pred kakšnim mesecem dni je k njemu prišel naročnik, ki je zahteval, da mu sestavi računalnik s štirimi grafičnimi karticami. Vendar ni zahteval najcenejših, temveč najbolj zmogljive in najdražje, ki jih je mogoče dobiti na tržišču. Prijatelj ga je presenečeno vprašal, zakaj jih potrebuje. Ta pa je odgovoril: »Uporabil jih bom za pridobivanje bitkojnov! Pravzaprav za njihovo rudarjenje!«

Jasno je, da nama ni bilo nič jasno. Prijatelj je zmignil z rameni in sprejel naročilo, naročnik pa je odšel. Moj sosed se je lotil sestavljanja računalnika s štirimi zmogljivimi grafičnimi karticami, ki je vsaka vredna vsaj 450€, sam pa sem na računalniku povprašal strička Googla in se posvetoval s teto Wikipedijo o rudarjeju bitkojnov. Kmalu je postalo jasno, da zadeva nima ničesar opraviti z bitnimi konji, temveč z internetnim denarjem imenovanim bitcoin. A tudi tisto rudarjenje sem kmalu razumel. Ob tem pa še, da je to trenutno konj za katerim se najbolj praši.

NASTANEK BITCOINA IN DELOVANJE SISTEMA

O zgodovini denarja sem pisal že večkrat v prejšnjih člankih. Na začetku so začeli izmenjevati blago za blago, potem so določili izdelke, ki so služili za menjalno sredstvo (komoditetni denar). Najbolj znan je morski polžek kavri. Še kasneje so uporabljali uporabne izdelke iz kovine, ki so se spremenili v kovani denar okrogle oblike. Od srednjega veka naprej se uporablja papirnati denar, ki so si ga najprej izmislili Kitajci. Od leta 2008 naprej imamo še virtualni, namišljeni ali internetni denar z imenom bitcoin.

Bitcoin (oznaka: BTC ali XBT) je kriptovaluta, pri kateri nastajanje in prenos bitcoinov temelji na odprtokodnem računalniškem, če hočete, na internetnem protokolu. Začetnik vsega je avtor ali skupina avtorjev s psevdonimom Satoshi Nakamoto, ki je 31. 10. 2008 oznanil projekt Bitcoin v dopisnem seznamu za kriptografijo in objavil belo knjigo. V začetku marca 2014 je Newsweek v ZDA objavil, da je odkril avtorja. To bi naj bil Dorian Satoshi Nakamoto, 64-letni ameriški državljan japonskega porekla, ki živi v Los Angelesu in bi se naj dejansko ljubiteljsko ukvarjal z matematiko in kriptografijo ter izdeloval modelno železnico. Vendar je Dorian kategorično zanikal, da ima karkoli opraviti z bitcoinom.

V osnovi je to računalniški program/protokol, ki rešuje problem izvedbe varne transakcije denarja/vrednosti skozi internet. Kdor se vključi v sistem, dobi poseben Bitcoin naslov v obliki javnega ključa (primer 120-bitnega ključa: 19VAVuupv9gbmySbKq9zUQzy6T297jsLoV) in ta se hrani v »denarnicah«, ki so lahko v obliki spletnih aplikacij, namiznih aplikacij ali na papirju. Ob tem si vsakdo s posebnim

programom sam izdela zasebni ključ ECDSA po postopku asimetrične kriptografije. Za pošiljanje denarja prejemniku je potrebno le poznavanje javnega ključa, medtem ko je za razpolaganje s stanjem na naslovu/denarnici Bitcoin potreben še zasebni ključ.

Slika 1 – Bitcoin logo in bitcoin kovanci
(obstaja več kakor 100 različic skovanih na različnih koncih sveta)

Denarnica Bitcoin je datoteka, ki vsebuje zbirko zasebnih ključev za naslove lastnika denarnice. Programska denarnica je nameščena na lastnikovem osebnem računalniku, spletna denarnica deluje kot storitev v internetu, mobilna denarnica pa je nameščena v lastnikovi mobilni napravi. Pri hrambi denarnice morajo biti izpolnjeni ukrepi za varovanje pred odtujitvijo ali razkritjem.

Sam prenos se opravi s pomočjo neke vrednosti, ki jo je avtor imenoval bitcoin. Verjetno v začetku ni bil mišljen kot valuta. Sčasoma pa se je enota za prenos prelevila v denar, torej v plačilno sredstvo. In posledica? Na začetku leta 2014 je bil 1 bitcoin vreden približno 650 €!

KAKO NASTANE DENAR?

V srednjem veku so izdajali denar vladarji. V sodobnem svetu to počnejo vlade držav, oz. njihove centralne banke. O načinu izdaj, emisiji denarja in o drugem je bilo že veliko rečenega in mnoge disertacije so napisane o tem. V bistvu pa vse skupaj običajno nima bistvene povezave s stanjem gospodarstva dežele. Denar je nekaj v kar verjamemo. Če vzamete v roke bankovec za 10€, je to zelo drago izdelan kos potiskanega papirja z deset in več zaščitami proti ponarejanju. Njegova vrednost je tista, ki je zapisana na njem in je v nekem sorazmerju z drugimi potiskanimi kosi papirja, ki so jih izdale druge centralne banke. Seveda je njegova izdelavna vrednost mnogo nižja. V kolikor tega kosca papirja nihče ne sprejme, torej ne verjame vanj, je to samo papir brez vrednosti.

V primeru bitcoina pa nastopi težava. Namreč nikjer ni centralne banke ali vlade, ki bi odobrilo emisijo internetnega denarja. Sistem je učinkovit zato, ker je popolnoma

decentraliziran in ne obstaja njegov upravnik. Skupina programerjev skrbi le zato, da programi in ves sistem gladko tečejo. Ne more pa izdajati novih kovancev!

Avtor je zato prišel na idejo o rudarjenju bitcoinov. Osnovo tvorijo transakcije, ki jih izvajajo uporabniki, ko kupujejo izdelke. Kdor želi in ima tehnične zmogljivosti ter priključek na internet, lahko zbira transakcije, ki do njega pridejo iz omrežja in preveri njihovo veljavnost. Neveljavne transakcije zavrže, nad preostalimi pa nato izvaja računsko zamudne operacije, ki požrejo ogromno procesorskega časa. Ob tem išče določeno vrednost, ki je del kriptografskega programa.

To delo je avtor poimenoval rudarjenje, oseba, ki ga izvaja, pa je rudar. Rudar, ki mu uspe najti takšno zgoščeno vrednost, je nagrajen z določenim fiksnim številom bitcoinov in s provizijami vseh transakcij v izračunanem bloku. Trenutna nagrada je 20 BTC za izračunan blok transakcij. Tako številni rudarji po vsem svetu predstavljajo ustanovo/sistem, ki opravlja emisijo bitcoinov, torej so neke vrste emisijska ali centralna svetovna banka. Nemogoče? Nenavadno? Niti ne! Ko je bil plačilno sredstvo polžek kavri, si potreboval čoln in nekaj znanja o potapljanju, da si bil emisijska banka!

Čisti matematični izračun kaže, da obstaja končno število tako izdanih bitcoinov. Ko bodo opravljeni vsi izračuni, bo v obtoku okrog 21 milijonov BTC, kar se bo predvidoma zgodilo do leta 2140. V tem trenutku je v obtoku okrog 12,5 milijonov BTC. Ob tem nastopi še dodatna težava! Čas za izračun novega števila, torej za rudarjenje novega bitcoina, se vse bolj povečuje in zato je potrebna vse bolj zmogljiva računalniška oprema.

Prav zato je naročnik zahteval pregrešno drage grafične kartice. Namreč, v vsakem osebnem računalniku se nahajata dva procesorja. Prvi je tisti na matični plošči, drugi pa je na grafični kartici. Vemo, da so za gladko tekoče računalniške igre potrebni hitri in zmogljivi procesorji, ki zmorejo preračunati na milijone točk in grafičnih trikotnikov. To pa je idealno tudi za izračun zgoščenih vrednosti transakcij v sistemu Bitcoin. Programi, ki so brezplačno na voljo na internetu, s pridom izkoriščajo procesorske moči grafične kartice. Tako več kartic sočasno preračunava vrednosti in na ta način skrajša čas za rudarjenje bitcoinov. Zdaj je jasno, zakaj je stranka potrebovala kar štiri drage grafične kartice v računalniku! A čas se še podaljšuje in v zadnjem času prijatelji skupno postavijo več računalnikov v grozd in rudarijo bitcoine skupinsko.

KJE LAHKO PLAČAMO Z BITCOINI?

Bitcoini se delijo na manjše enote, podobno kot vse običajne valute. A ker je njihova vrednost tako visoka in ker v internetu ni problem deliti denar na manjše enote kadarkoli, so ga razdelili na osem decimalnih mest. 0,00000001 BTC (deset-milijoninka) je najmanjša enota, ki se imenuje satoši. V začetku leta 2014 so se uporabniki odločili, da bodo enoto vpisovali s predpono mikro in kot osnovo vzeli tisočkrat manjšo enoto imenovano mBTC (http://bitcoinity.org/ in http://data.bitcoinity.org/). Torej 1 BTC = 1.000 mBTC.

Bitcoini so se pojavili tudi v fizični obliki. Kovanec ima na sebi hologramsko nalepko z 120-bitnim kriptografskim ključem. Tako ga lahko uporabimo na internetu. Ameriški podjetnik iz Los Angelesa je že napovedal, da namerava postaviti bankomat za izplačilo bitcoinov do konca aprila 2014.

Na začetku je bil bitcoin čista eksotika. Rudarjenje je bilo visoko dobičkonosno, ker si število lahko hitro izračunal. Zaradi nepoznavanja sistema se ga ni lotil skoraj nihče. Redki uporabniki so zapravljali velike količine za malovredne izdelke in storitve. En bitcoin je bil vreden vsega nekaj dolarskih centov. Spletni trgovci so jih počasi začeli sprejemati in konec leta 2010 je začela njegova vrednost rasti. Do sredine 2011 se je

vrednost povzpela na skoraj 30 dolarjev. Avgusta 2011 je sledil močan hekerski napad na omrežje in posledica je bil »borzni zlom«. Koda je napad preživela, vendar je padla vrednost na 5 dolarjev.

Slika 2 – Bitcoin (25 BTC) s hologramsko kodo

Slika 3 - Rast cene Bitcoina v dolarjih (© Vir: Bitcoinity.org)

Januarja 2013 je zrasla na 13 dolarjev, potem pa je do decembra 2013 poletela v nebo do 1216 dolarjev! Vrednost v začetku marca 2014 je bila 0,65 USD za 1 mBTC (1 BTC = 650 USD).

Najbolj odmeven nakup doslej je bilo plačilo električnega avtomobila Tesla v ZDA. Kupec je zanj plačal 91,4 BTC (91.400 mBTC) . Po svetu je že na tisoče trgovin, ki sprejemajo internetno valuto. Tudi v Sloveniji je vsaj 40 internetnih ponudnikov, na primer virtua-shop, eksotika, giga-shop, zabec.net, itn. V realnem svetu je mogoče kupiti kosilo v ljubljanski restavraciji Allegria in pico v sosednji piceriji Osmica, itd. Trgovanje z bitcoinom in drugimi valutami po vzoru sistema FOREX je možno na več elektronskih

borzah. Uporabniki borz so izpostavljeni velikim tveganjem zaradi valutnih nihanj in računalniških vdorov.

Slika 4 – Prodajno mesto, ki sprejema bitcoine.

URADNO PRIZNANJE IN SLOVENIJA O BITCOIN

Bitcoinov ne varuje nobena zakonodaja na svetu. Vendar je Ameriško zvezno sodišče v februarju 2014 potrdilo, da je bitcoin uradno priznana valuta in se lahko uporablja v ZDA. O posledicah te odločitve bo še govora.

Slika 5 – Kje je uporaba bitcoina v kakršnikoli obliki dovoljena (zeleno), kje je omejena (rumeno) in kje je bitcoin v celoti prepovedan (rdeče)?

Zemljevid sveta prikazuje v katerih deželah je bitcoin v kakršnikoli obliki legalen. Tudi Slovenija je označena z zeleno barvo. Slovensko finančno ministrstvo o uradnem priznavanju valute še ne razmišlja. O stališču Davčne uprave Republike Slovenije (DURS) smo prebrali v prejšnji številki revije.

Evropski bančni organ EBA je 12.12.2013 vsem uporabnikom na teritoriju Evropske unije izdal opozorilo glede virtualnih valut. Tako opozarja na tveganja (vključno z izgubo denarja), s katerimi se lahko srečajo uporabniki, če kupujejo, hranijo ali trgujejo z virtualnimi valutami (npr. bitcoin). Virtualne valute so oblika nereguliranega digitalnega denarja, ki ga ne izda centralna banka in zanj ne jamči. Opozarja tudi, da ne obstajajo nobeni regulativni zaščitni ukrepi, ki bi uporabnikom povrnili izgube, če platforma, na kateri se menja ali hrani virtualne valute, propade ali preneha poslovati. Medtem EBA

preučuje vsa pomembna vprašanja, povezana z virtualnimi valutami, da bi ugotovila, ali jih je mogoče regulirati in nadzorovati in ali je to potrebno storiti.

Vendar to vedno bolj razjarjenih Grkov in Ciprčanov (ter drugih) ne prepriča. Ker jim država legalno krade iz žepa, se je število transakcij s pomočjo bitcoinov zelo povečalo. Če ne moreš uporabljati legalnega menjalnega sredstva pač poiščeš nadomestno. Prav bitcoin je zaradi elektronskega plačevanja najbolj primerno novodobno menjalno sredstvo.

VSAK KOVANEC IMA DVE STRANI

Zlorabe dokazujejo, da je bitcoin »zaresna« valuta. Kar ni nič vredno, se ne splača ukrasti. V kratki zgodovini bitcoina smo videli načine kako pridobiti čim več namišljenih kovancev na nepošten način in tudi njegovo uporabo za financiranje nezakonite trgovine.

Mnogi so naivno verjeli, da je zaradi svojega sistema imun na zlorabe. A velja prav nasprotno! Transakcije so anonimne in nevračljive. Tako so idealne za tatvine. Z vdorom v elektronsko denarnico so junija 2011 lastniku 25.000 BTC odnesli vse do zadnjega satošija, kar je po takratnem tečaju predstavljalo okrog pol milijona evrov. Ker ne obstaja svetovna policija in se ne moreš nikomur pritožiti, se je lastnik obrisal pod nosom.

Nastala in razpadla je prva piramidna shema (Bitcoin Savings & Trust), ki je od leta 2012 ponujala sedem odstotkov obresti na mesec. Avgusta 2013 je organizator z zelo spodbudnim internetnim vzdevkom pirateat40 enostavno popihal s pol milijona bitcoinov naivnih vlagateljev.

Svoj lonček so pristavili klasični internetni pirati, ki so izdelali kopico trojancev za krajo bitcoinov. Ti v okuženih računalnikih poiščejo datoteke z denarnicami in jih skupaj z geslom izmaknejo. Zlikovci si potem iz denarnice zlahka nakažejo bitcoine. Lastnik ne more nikakor dokazati, da je resnični lastnik, niti ne more izpodbiti transakcije, saj ta ni zabeležena nikjer več potem, ko je opravljena. Ker ne obstaja centralna banka!

So pa vsem bitcoini pri srcu zaradi svoje anonimnosti. Z njimi je mogoče nakupovati, ne da bi to kdorkoli vedel. To pa je idealno tudi za mafijske nakupe! Aprila 2013 so FBI, Agencija za boj proti drogam (DEA) ter nizozemska in kolumbijska policija razbili mamilarsko družbo, ki je upravljala stran The Farmer's Market. Na njej je bilo mogoče naročiti vse vrste opojnih substanc, od marihuane do ketamina in kokaina. Plačevali so z Western Unionom, PayPalom in tudi z bitcoini.

Znotraj interneta deluje zelo skrit in anonimni sistem Tor. Je del tako imenovanega globokega interneta (deep web), ki ga najdemo ob uporabi ustreznih orodij in če vemo, kako ga poiščemo. Na strani Silk Road (svilna cesta) lahko kupimo vse vrste drog, orožje, ukradene številke kreditnih kartic, nadzor nad računalniki, najamemo hekerje, navodila in opremo za izdelavo eksplozivnih teles, osebne podatke, itd. Silk Road je organiziran in pregleden podobno kot Amazon ter enako zanesljiv. Kupljeno blago je skoraj stoodstotno skladno z obljubami v oglasih. Na leto obrnejo 20-30 milijonov dolarjev, plačila pa so seveda v bitcoinih.

Da je nekaj uspešno, vidimo tudi po številu posnemovalcev in kopij. Tako so si izmislili že celo kopico –coinov, na primer litecoin, zerocoin, dogecoin, primecoin, primecoin, ripple, itd. Potrebujete svoj lasten –coin? Ni problema! Pojdite na http://coingen.bluematt.me in si naredite svojega!

NEPRIJETNE NOVICE

V mesecu marcu 2014 so pričele prihajati neprijetne novice o bitcoinih. Iz Singapurja so sporočili, da je bankrotirala tokijska borza bitnih kovancev MT.Gox. Izvršni direktor Mark Karpeles se je na japonski televiziji najprej kar nekaj časa globoko priklanjal, nato pa pojasnil, da je ogromno izgubo povzročila tehnična napaka v sistemu. Opravičil se je za težave, ki jih je povzročil velikemu število ljudi. Kyodo News je poročala, da je Mt Gox zabeležil izgubo v višini 63,3 milijona dolarjev.

Prav tako poročajo, da so ameriško izvršno direktorico virtualne menjalnice First Meta našli mrtvo v njenem stanovanju v Singapurju. Prenehala je poslovati kanadska spletna stran Felxcoin, kjer so uporabniki lahko hranili svoje bitne kovance. Tako se mnogi sprašujejo in napovedujejo, da je zlom virtualne valute vse bližji. Morda!