Kriptovalute, bitcoin, blockchain i slične čudnovatosti

„Ako ne mislite o budućnosti, ne možete ju ni imati."
John Galsworthy, engleski spisatelj i Nobelovac

„Budući čovjek – to je čovjek kojemu se ništa ne može obećati."
Vlado Gotovac, Rječnik o djelu

Kad bi u, recimo Slavoniji, danas stavili osobu u vremenski stroj i poslali ju sto godina unazad da svojim precima na selu kaže što učiti i za što se pripremati da im potomci ne bi bili nezaposleni i ne bi morali u Irsku, bio bi to fijasko. Naši preci nemaju taj vokabular, nemaju dostatan pojmovnik da bi razumjeli praunuka iz budućnosti. Prvo, u to doba posao nema samo lijenčina. Kakva „*nezaposlenost*", što je to uopće? Eto ti motike! Drugo, kako im objasniti Internet, programiranje računala, aplikacije za Android, 3D printere i slično kad oni ni struje ni telefona nikad vidjeli nisu?

Kad bi u, recimo Slavoniji, ljudi iz 2117. godine stavili osobu u vremenski stroj i poslali ju da nam danas kaže što činiti da bismo imali posao u budućnosti, i to bi vjerojatno bio fijasko. Došljak iz futura zasigurno bi imao čudnovati rječnik i brbljao neke fraze koje bi nam bile posvema apstraktne. No, možda je udar industrijsko-tehnološke revolucije XX. stoljeća neponovljiv, možda će se pokazati da je skok od 1917. do 2017. bitno veći nego od 2017. do 2117., možda svijet više neće doživljavati takve radikalne promjene u tako kratko vrijeme. A možda i hoće? Možda će budući čovjek govoriti o *blockchain* arhitekturi…?

Kriptovalute su izum novog doba. Prva i daleko najpoznatija je bitcoin, ali ima i drugih, ponešto drugačijih, bitcoinu nalik. Tu su već „dugih" osam godina, ali još su novost. Vrlo ih je teško pojmiti, zahtjevno objasniti, i većina ne razumije njihovo funkcioniranje. To je zato što se dizajn oslanja na informatiku, Internet i programiranje, a većina nâs ne zna objasniti što se u toj crnoj kutiji doista događa: jednostavno ju upalimo, odemo na Internet, upišemo par slova u Google, on vidovito predvidi što mi zapravo hoćemo i ponudi nam rezultat; i eto nas začas u virtualnoj šetnji australskim parkom Uluru-Kata Tjuta. Kažu da su sve to samo nule i jedinice; ako jesu Uluru-Kata Tjuta ima ih u izobilju.

Da bi se bar donekle pojasnile kriptovalute čitatelj treba imati neku predodžbu, predznanje i osnovni (engleski) rječnik (jer je engleski jezik računala) iz područja informatike. Valja zagrebati površinu po nekima.

Peer-to-peer mreža je koncept povezivanja računala bez središnje točke, bez poslužitelja (centralnog servera). Ondje svako računalo pronalazi i izravno komunicira s drugim računalima. Nema nekog središnjeg „autoriteta". Osim toga, peer-to-peer je i koncept dijeljenja datoteka između računala, također bez središnjeg poslužitelja. Stariji čitatelji sjetit će se Napstera – peer-to-peer mreže putem koje su korisnici dijelili glazbu. (Počivao u miru.)

Nadalje, *open-source* softver je računalni program čiji je programski kôd javno objavljen na Internetu i svatko ga može i vidjeti i mijenjati. Windowsi – primjerice, su sušta suprotnost; „prozori" nisu open-source i Microsoft ima ekskluzivno pravo i na taj softver i na zaradu od njega. Razotkrivanjem kôda Windowsi bi razotkrili i svoje slabe točke. Open-source temelji se na „internetskom zadrugarstvu" – dobrovoljnoj suradnji većeg broja ljudi koji, bez naknade, zajedno unaprjeđuju određeni softver na dobro svih korisnika. Namjernim razotkrivanjem kôda i slabih točaka želi se ojačati sustav: bez kritike nema razvoja. Ali nije svaka izmjena kôda promjena nabolje – kako osigurati da, premda svatko može uređivati sadržaj, samo dobre izmjene budu implementirane? Tako što cijela zajednica nadgleda prijedloge promjena i odobrava samo one koje smatra kvalitetnima. Wikipedija kao otvorena enciklopedija može biti primjer kolaborativnog alata, no ondje zna biti problema jer različiti ljudi različito tumače određene društvene pojave, pa članak o npr. biseksualnosti jedni mogu smatrati korektnim, a drugi pristranim, jednostranim. Također, i nestručnjaci mogu uređivati sadržaj i unijeti pomutnju. Što se softvera tiče, u njegovu sadržaju mahom je riječ o tehničkim konceptima oko kojih najčešće nema kontroverzi jer tu uglavnom nema prostora za privatne subjektivnosti.

Ciljevi su stabilnost, uporabljivost, sigurnost i slično, i tu dilema nema, a izmjena prolazi samo ako ju odobri zajednica.

Peer-to-peer i open-source temeljni su koncepti cijele jedne filozofije i svjetonazora kojega formiraju ljudi ucijepljeni u Internet. Oni su i temeljni građevni elementi dizajna kriptovaluta. Kriptovaluta je digitalni novac stvoren na Internetu za Internet, i to digitalni u punom smislu riječi. Kad osoba uplati novac u banku i potom plaća karticom ona zapravo koristi digitalizirani klasični novac; to nije digitalni novac u punom smislu jer je stvoren i koristi se kao naličje papirnog novca. Otprilike, to je poput digitalne fotografije koja je nastala skeniranjem klasične; ona se može slati putem interneta ali nije u potpunosti digitalna jer svijet u početku oslikava kroz klasičnu, tradicionalnu optiku. Digitalizirani novac u klasičnoj banci ima bitno drugačije karakteristike u odnosu na kriptovalute; on je dug. Polaganjem novca u banku (i posljedično njegovom digitalizacijom) stvara se dužničko-vjerovnički odnos: banka postaje dužnik – ona je taj novac dužna vratiti na zahtjev vlasnika. Kriptovaluta je posebna priča, odvojena od klasičnog monetarnog sustava. Kod kriptovaluta nitko nikome ništa ne duguje; imati jednu je otprilike kao imati zrno zlata u ruci. Zlato može imati veću ili manju vrijednost, ali kao takvo ne predstavlja dug.

Prije par tjedana druga najmnogoljudnija zemlja na svijetu – Indija – odlučila je legalizirati bitcoin. Kineski korisnici čine gotovo polovicu Bitcoin mreže (Bitcoin je mreža, a bitcoin jedinica valute), a i kineska središnja banka stavila ga je pod povećalo. K tome, kriptovaluta pod nazivom *Ethereum* vrlo naglo raste i mnogi joj predviđaju svijetlu budućnost. Početkom lipnja ruski se predsjednik Putin sastao s utemeljiteljem Ethereuma i iskazao otvorenost ruske vlade prema digitalnoj ekonomiji koja, mudro zbori Putin: „*nije zasebna industrija, nego temelj za stvaranje novih poslovnih modela*“. Čak se govori i o tome da bi Ethereum postao ruska nacionalna virtualna valuta.

Orijaški je entuzijazam zastupnika, korisnika i promotora kriptovaluta. Oni tvrde da uvođenje i razvoj kriptovaluta za financijsku industriju znače isto što i uvođenje i razvoj interneta za komunikaciju. Potpuni obrat. Treba se zato upoznati s njihovim osnovama.

GLAVNI TEKST

Usred Pacifika, usred ničega, nalazi se otok Yap i na njemu intrigantni kameni diskovi s rupom u sredini; neki i preko 3,5 metara visoki; zovu se *rai*. Na Yapu nema ni srebra ni zlata, a ni kamena od kojega su rai isklesani. Vapnenac za rai mukotrpno se iskapa i obrađuje na najbližem susjednom otoku (udaljenom svega 430 km), i odande prevozi na Yap. Zajednica na otoku Yapu u nekom je povijesnom trenutku uvidjela da im je potrebno nešto trajno što bi konzerviralo vrijednost tijekom generacija. U nedostatku plemenitih metala rai je preuzeo funkcije novca. No, on je pretežak da bi ga se prenosilo. Stoga kamen stoji na mjestu, a samo se vlasništvo izmjenjuje; cijela zajednica zna tko je vlasnik kojega kamena. Njegova fizička lokacija uopće nije važna. Primjerice, kad djevojka u miraz donosi rai svi znaju da je vlasništvo nad tim kamenom promijenjeno.

Jednom prilikom grupa je japljana isklesala rai, no putem nazad snašla ih je oluja i havarija: golemi je disk potonuo. Po povratku su preživjeli ispričali što im se dogodilo. To što je kamen na dnu oceana nije ih spriječilo da on i dalje obavlja funkcije novca. Svi vjeruju da je rai dolje među ribama, te se vlasništvo i nad oku nevidljivim kamenom i danas izmjenjuje.

Od kamenog diska na dnu oceana do virtualnog bitcoina i nije tako velik korak. Obje su valute apstraktne, nedodirljive, a počivaju na uzajamnom povjerenju i na dijeljenom znanju u zajednici. Ne postoji nikakva nadređena središnja institucija, vlada, agencija, banka ili korporacija koja izdaje ili vodi račune o tim valutama. Valuta je oskudna i ne raste na grani. Kreiranje nove jedinice i unos nove jedinice u sustav vrlo je zahtjevno i obavlja se pod budnim okom zajednice.

Bitcoin je i specifična pod-mreža na internetu, i jedinica najpoznatije kriptovalute. To je sustav elektroničkog plaćanja koji se zasniva na kriptografiji (šifriranju) – odatle „*kripto*valuta". Kriptografija se tisućljećima primjenjuje za osiguravanje tajnosti diplomatske, vojne i preljubničke komunikacije. Šifriranje se čini zato da bi komunikacija između dvije osobe ostala privatna i nekompromitirana, iako u komunikacijskom kanalu postoje treće osobe koje tu komunikaciju mogu pratiti. Budući da proces šifriranja i dešifriranja nije jednostavan, ni kriptovalute nisu jednostavne.

Ako tko želi poslati novac putem interneta potrebna mu je pouzdana treća osoba, institucija u koju ima povjerenja da će novac prenijeti od A do B. Kako internetom primiti novac bez posrednika, a biti siguran da ga nitko putem neće ukrasti ili kompromitirati (npr. umanjiti iznos), i također biti siguran da onaj tko je novac poslao doista ima taj novac? Moguće je rješenje u dijeljenom znanju u zajednici, u peer-to-peer mreži koja se temelji na open-source softveru, pri čemu je komunikacija vrlo snažno šifrirana. Povjerenje – temelj svakog financijskog sustava, i virtualnog i klasičnog – ne izvire iz povijesti institucije, stručnosti menadžmenta, vrlina čelnih osoba i sličnog, nego izvire iz povjerenja u matematiku, odnosno kriptografiju. Kad bi se sva računala na Bitcoin mreži udružila da zajedničkim radom probiju šifru samo jedne transakcije za to bi im trebalo preko 7.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000 godina. Izgleda impresivno, ali… nisu li računala impresivno snažna? Nemaju li, recimo CIA ili Kina (ili CIA i Kina zajedno) nešto što bi moglo probiti takvu šifru (tzv. SHA-256 enkripciju)? Ne, jer računalo koje bi to bilo u stanju učiniti ne može postojati u prostor-vremenu kakvog poznajemo, a osim kršenja zakona fizike suprotstavlja se i zakonima termodinamike; za kalkulaciju u kratkom vremenu bila bi potrebna energija koja zrači toplinu veće supernove, eksplozije veće zvijezde (iz B. Schneier, Primijenjena kriptografija, Wiley, 1996.). Moćno! A čak i ako se bude smatralo potrebnim, a zasad nije, kriptovalute se mogu prebaciti na još viši standard šifriranja. Kad se povjeruje u neprobojnost šifre više nije nužno vjerovati osobi ili instituciji. Ipak, svejedno je potrebno imati povjerenje u sustav u cjelini.

Iako je u srcu kriptovaluta kriptografija, samo šifriranje nije nikakva novost. Transakcija kriptovalutama putem Interneta temelji se na kriptografskom sustavu dva ključa: privatnog i javnog. To je poznat izum i postoje brojne aplikacije za sigurno komuniciranje putem Interneta koje se temelje na korištenju javnog i privatnog ključa. I u Hrvatskoj se elektroničko, e-potpisivanje dokumenata također zasniva na sustavu dva ključa. Javni se ključ matematički izvodi (šifrira) iz privatnog ključa, i to tako da je praktično nemoguće iz javnog ključa (unazad) doći do privatnog. Bitcoin mrežom ne šalju se šifrirane ni ljubavne ni vojne poruke, nego transakcije. Prostor jednog članka odveć je ograničen da bi se detaljno opisao proces transakcije bitcoina, stoga će se skratiti i pojednostaviti.

Za transakciju je potrebno da pošiljatelj i primatelj kriptovalute imaju tzv. bitcoin novčanike. Bitcoin novčanik je softver kojega korisnik može sam besplatno instalirati na svoje računalo ili mobitel, ili ga može otvoriti na Internetu. Za otvaranje novčanika nije potrebno dopuštenje niti ikakav formalni proces kod bilo koje institucije, i može se otvoriti potpuno anonimno. Vlasnik bitcoin novčanika ima privatni ključ (šifru) koji je samo njemu poznat i kojeg mora držati u apsolutnoj tajnosti jer svaki posjednik privatnog ključa može raspolagati bitcoinima u njegovu novčaniku. Izgubi li tko svoj privatni ključ ili bude nedovoljno oprezan s njime pa mu ga ukradu, zauvijek se može pozdraviti sa svojim novcem, a budući da je sustav decentraliziran nema nikakve središnje institucije kojoj bi se mogao obratiti za zaštitu prava ili za obeštećenje. Privatni ključevi nisu isto što i lozinke koje se uobičajeno koriste na Internetu jer su bitno duži i složeniji (primjer privatnog ključa je 5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF). Pošiljatelj bitcoina šalje transakciju u mrežu i čeka potvrdu transakcije. Bitcoin mrežu čine računala koja verificiraju transakcije, a kao nagradu za verifikaciju plaćeni su u bitcoinima što se naziva „rudarenje" (mining). Osoba može steći bitcoin tako da ga kupi (zamijeni kune za bitcoin), stekne u transakciji (npr. proda neku robu za bitcoin), ili ga zaradi „rudareći" u mreži. Za steći zlato potrebno je rudariti, a nagrada za računalno rudarenje su novi bitcoini u sustavu. Rudarenje je proces potvrđivanja i dodavanja novih transakcija u „glavnu knjigu" koja se naziva lanac blokova.

Bitcoin sustav osmišljen je imajući na umu zlato kao novac. Zlato je vrlo rijetko, i među ostalim zato se smatra vrijednim. I bitcoin je osmišljen tako da bude oskudan: zahtjevno ga je rudariti, i jednako kao što s vremenom zlatni rudnik postaje sve više iscrpljen, sve je manje zlata u njemu i sve je više truda potrebno

da se do zlata dođe, i „rudarenje“ bitcoina s vremenom donosi sve manje nagrade. Svake četiri godine nagrada za „rudarenje“ postaje dvostruko manja, te će 2140. godine (doduše, ako sustav do tada opstane) svi bitcoini – njih ukupno 21 milijun – biti „izrudareni“ i više neće biti novih jedinica. Predviđa se da će do tada biti osmišljeni procesori (čipovi) koji će biti toliko snažni i energetski efikasni da će se troškovi mreže pokrivati iz naknada za transakcije.

Sustav je tako usmjeren da kriptovaluta s vremenom dobiva na vrijednosti i da *nikada* ne bude inflacije; prvo jer nema središnje institucije koja bi upumpala valutu u sustav, a drugo jer je softver tako programiran. (Netko može reći: pa ako je to open-source softver, onda se on može drukčije programirati! Da, mogao bi kad bi se svi članovi bitcoin zajednice oko toga složili, ali to bi bila odluka o samouništenju jer bi se sustav urušio. Nijedan vlasnik bitcoina nije za takvo što motiviran jer bi rušenjem sustava izgubio bitcoine, odnosno novac. Tu se otvara prostor za alternativne kriptovalute – drugačije koncepcije softvera – koje koriste osnovne ideje bitcoina, ali ležernije i velikodušnije isplaćuju nagrade za rudarenje. Vrijeme će pokazati koliko su održive i stabilne.)

Eto još jedne bitne razlike između klasičnog monetarnog sustava i kriptovaluta: premda ni jedno ni drugo nemaju nikakvo realno pokriće kriptovalute nisu osmišljene za makroekonomiju. Države se zadužuju računajući da će inflacija pojesti dio tog duga, i to smatraju pozitivnim. No, na razini građana-pojedinca, inflacija ga osiromašuje jer izjeda vrijednost njegova novca (doduše, neki se sjećaju da se u vrijeme Jugoslavije, kad krediti nisu bili na neki način vezani uz stopu inflacije, kredit nakon nekoliko godina vraćao u mizernim mjesečnim iznosima, ali to je daleka prošlost i banke su se odonda opametile). Građani žele valutu u kojoj mogu trajno konzervirati vrijednost. Ovdje leži dio otpora tradicionalnih monetarista prema kriptovalutama: osim što idejno utemeljenje na zlatu smatraju barbarskim, kod kriptovaluta nemaju nikakvu kontrolu nad ponudom novca, nemoguće su devalvacija i inflacija, a devalvacija i inflacija mogu biti saveznici papirnih sustava.

U početku je bilo tko mogao na kućnom računalu „rudariti“ bitcoine, ali širenjem mreže „rudara“ i zbog smanjenja nagrada potrebno je imati sve jače računalo da bi se na taj način moglo zaraditi. Danas je u praksi manja zarada na rudarenju nego što je trošak cijene električne energije za pogon računala, tako da se rudarenjem bave samo oni koji imaju pristup iznimno jeftinoj struji.

Glavno pitanje na koje kriptovalute imaju odgovor glasi: kako u decentraliziranoj, *peer-to-peer* mreži znati da pošiljatelj doista ima novac kojega može proslijediti drugome? Ako nema nijedne banke, nikakvog autoriteta, kako znati ima li tko novca na raspolaganju za potrošiti? Odgovor je u kompletnom popisu svih transakcija iz cijele povijesti kojega ima svaki član mreže, popisu iz kojeg se može vidjeti da je pošiljatelj nekad prije stekao kriptovalutu. Osoba ne može potrošiti jedinicu kriptovalute ako ju nije prethodno nekako stekla, a činjenica da ju jest stekla nalazi se u „glavnoj knjizi“. Ovo je središnja inovacija: „glavna knjiga“ kao popis svih transakcija (tzv. blockchain). Transakcije u tijeku grupiraju se u blokove, a verifikacija jednog bloka uobičajeno traje desetak minuta. Nakon obrade blok verificiranih transakcija se pridodaje lancu prethodnih blokova: svaki je blok šifrirano vezan na prethodni, i svaki je označen jedinstvenim vremenskim žigom tako da se kasnije ne može mijenjati. Cjelokupan lanac blokova je „glavna knjiga“ – popis svih transakcija ikad učinjenih. Nema jedne „glavne knjige“, ona je u cijelosti umnožena i podijeljena svim elementima mreže tako da svatko ima cjelokupnu „glavnu knjigu“. Ako tko i pokuša manipulirati svojim primjerkom on se više neće savršeno podudarati s ostalima, te će ga ostali odbaciti. Čak i ako se većina sudionika mreže u nekom trenutku udruži i pokuša zajedno manipulirati „glavnom knjigom“ ona se i dalje neće kriptografski (matematički) podudarati s posljednjom ispravnom verzijom.

Prednosti ovakvog sustava su goleme. Svi detalji sustava su javni, i tkogod želi (i razumije se u to) može vidjeti svaku liniju programskog kôda, odnosno svaku transakciju u „glavnoj knjizi“. Nestaje potrebe za višestrukim knjigovodstvom: nema potrebe da svatko vodi svoj pojedinačni račun (ili da to za njega čini neka banka ili druga institucija) jer je povijest svih verificiranih transakcija, na jednom, zajedničkom mjestu. Sustav osigurava privatnost i tajnost podataka što nasušno nedostaje suvremenom Internetu.

Većina bankara, ekonomista, financijaša ne razumiju kriptovalute, i to s pravom; njih ne stvaraju ekonomisti nego računalni programeri. Čini se da je tu i najveća prepreka: teško će široki krug ljudi prihvatiti kriptovalute ako ne mogu razumjeti osnove funkcioniranja uistinu digitalnog novca. Kad se uđe u fine detalje malo tko doista razumije kako to zapravo funkcionira. No, većina ljudi i pametne mobitele (i štošta drugo) koristi a da ne zna u detalje kako to mikroračunalo doista funkcionira. Financijski se sustav uvijek na kraju svodi na povjerenje.

OKVIRI

Glavna knjiga - blokchain

Sve potvrđene i verificirane transakcije od početka povijesti kriptovalute zapisane su u „glavnoj knjizi" koja se naziva „lanac blokova" (blockchain). Pojedinačne se transakcije agregiraju u blokove i zajedno se verificira jedan blok transakcija što uobičajeno traje desetak minuta. Nakon potvrde transakcije blok se veže na prethodne blokove. Budući da su blokovi kriptografski vezani ne može se promijeniti neki prethodni blok, a da se ne promijene i svi blokovi poslije njega. Identitet osoba u transakcijama je šifriran, stoga se kaže da je sustav pseudoniman, a ne anoniman. Netko može konstantno koristiti samo jednu šifru, samo jednu adresu (što se nikako ne preporučuje), a na taj se način može razotkriti njegov identitet. Lanac blokova ne nalazi se na samo jednom mjestu nego je distribuiran: svatko ima svoj primjerak koji se redovito ažurira.

Upravo je lanac blokova kao zasebni koncept koji je proizišao iz Bitcoin mreže okupirao najviše pozornosti i financijske i ne-financijske industrije. Klasična financijska industrija intenzivno razmatra uvođenje lanca blokova u svoje poslovanje. Najveće svjetske banke već su se udružile kako bi zajedno napravile industrijski standard (to ne znači da će se prebaciti na kriptovalute, nego da će koristiti tehnologiju lanca blokova u nekom segmentu svoga poslovanja). Ne-financijska industrija priprema ih u izradi dokumenata (putovnica, potvrda, i sl.), zdravstvenim kartonima, distribuciji glazbe, logistici dostavnog lanca, zemljišnim knjigama, tzv. pametnim ugovorima, javnom bilježništvu itd., jer predstavlja siguran, jeftin i trajan sustav vođenja podataka. Bilo kako bilo, mnogi zagriženi simpatizeri blockchaina uvjeravaju da je to koncept koji će promijeniti budućnost u brojnim segmentima društva.

Primjer transakcije kriptovalutom

Jedan bitcoin je lanac digitalnih potpisa. Pretpostavimo da pošiljatelj želi uplatiti tisućinku bitcoina (jedan se bitcoin dijeli na sto milijuna jedinica koje se zovu *satoshi*) nekom primatelju. Pošiljatelju treba primateljeva bitcoin adresa. Primatelj u svom novčaniku (softveru) generira novu adresu (npr. 1HsjKqfDzFJiGkvkYMyLPMk1ZpVsi5s9yu) te adresu da pošiljatelju. Adrese nisu fiksne (iako mogu biti) i snažno se preporučuje za svaku novu transakciju koristiti novu adresu. Adresu nikako ne treba promatrati kao bankovni račun (npr. kao IBAN), jer Bitcoin mreža ne funkcionira po načelu računa i stanja na računima. Glavna knjiga (lanac blokova) nije popis računa (i stanja na njima) nego popis svih transakcija. Apsolutno svaku jedinicu kriptovalute u početku je zaradio neki „rudar", potom ju je potrošio (učinio neku transakciju), te time kreće povijest i lanac transakcija tom jedinicom. Tako se za svaku jedinicu može pratiti povijest verificiranih transakcija od njenog nastanka, što je za klasične valute apsolutno nemoguće.

Adresa i javni ključ nisu isto, ali jesu matematički povezani; bitcoin adresa je šifrirana verzija javnog ključa. Kad primatelj novca pošalje svoju adresu pošiljatelju siguran je da samo on (primatelj) može „otključati" i kasnije potrošiti taj novac. Kasnije će primatelj potrošiti digitalni novac koristeći svoj privatni ključ: upravo onaj s kojim je šifrirao svoju adresu prije nego ju je poslao pošiljatelju.

Imajući adresu primatelja pošiljatelj šalje zahtjev za transakciju u Bitcoin mrežu. Transakcija se „potpisuje" pošiljateljevim potpisom, odnosno njegovim privatnim ključem, što predstavlja matematički dokaz da je pošiljatelj vlasnik novčanika. Nitko u mreži ne vidi privatni ključ, ali vidi da je samo onaj tko doista ima privatni ključ mogao poslati transakciju. Pošiljateljev potpis također osigurava da nitko ne može kompromitirati sadržaj transakcije.

Pitanje: ako je adresa nasumični niz znakova bez identifikacijskih elemenata, svaki put drugačija, kako primatelj na adresi može dobiti novac? Stvar je u načinu dostave. Kad poštar nosi pismo treba mu fiksna adresa, kućni broj primatelja na koju će dostaviti pošiljku. Kod kriptovaluta „pismo" (transakcija) je digitalni zapis koji se peer-to-peer mrežom dostavlja na apsolutno sve „kućne brojeve" koji postoje. Svaki element mreže dobiva svako „pismo" (zapis o svakoj transakciji), ali samo vlasnik privatnog ključa može „otključati" (dešifrirati) njegov sadržaj i zatim koristiti novac u „pismu". Zato kad vlasnik izgubi (ili mu ukradu) privatni ključ bilo tko u mreži može koristiti njegov novčanik. Stoga se savjetuje privatne ključeve držati izvan mreže, na sigurnom. Postoji tvrtka koja za naknadu čuva privatne ključeve korisnika na offline serveru u sefu koji je smješten u srcu jedne planine u Švicarskoj…

Korištenje u nezakonite svrhe

Pranje novca, izbjegavanje poreza, trgovina protuzakonitom robom – sve su to aktivnosti koje se mogu osmisliti i naplaćivati kriptovalutama. Protivnici kriptovaluta često ističu da su najvjerniji korisnici kriptovaluta kriminalci. S druge strane, mnogi programeri žele otvoreni dijalog s organima vlasti u pogledu reguliranja (dijela) ovih sustava, no kod institucija najčešće nailaze na nerazumijevanje i nevoljnost. Također tvrde da su kriptovalute samo jedna vrsta tehnologije, alat koji sam po sebi ne može biti ni dobar ni loš: ovisi za što se koristi.

Problemi odrastanja

Potpuno suprotno osnovnoj ideji otvorenosti i slobodnog pristupa, zbog naglog rasta Bitcoin mreže mnogi servisi koji pružaju usluge plaćanja bitcoinima uveli su naknade za plaćanje. Nedostatak stihijskog rasta je i zagušenje mreže: ponekad je potrebno i nekoliko sati (umjesto očekivanih desetak minuta) za obradu transakcije i prijenos bitcoina. Te su kritike na mjestu, ali malko je ipak deplasirano kad dolaze od bankara koji za iste usluge odavna naplaćuju masne naknade i kojima za međunarodni prijenos novca treba nekoliko dana.

Misteriozni osnivač

Idejni utemeljitelj prve kriptovalute, bitcoina, je Satoshi Nakamoto. Nitko ne zna tko je to, a špekulira se i da to nije jedna, nego grupa osoba. U svakom slučaju zna se da to nije njegovo pravo ime nego pseudonim: u istinskoj maniri prvoga kripto-rudara nije razotkrio svoj identitet. Također se zna da je (bio) zagriženi liberal. Budući da je bio prvi kripto-rudar on je i najveći imatelj bitcoina u svijetu. Smatra se da ima oko milijun bitcoina koji danas imaju vrijednost preko dvije milijarde dolara. Veo misterija oko njegova identiteta otvara prostor za prekobrojne teorije o tome tko je to zapravo, koji su motivi osnivača, i tko stoji iza svega. Zasad su sve to samo priče bez pravog pokrića.

Deset najznačajnijih kriptovaluta u svijetu (krajem lipnja 2017.)			
	Naziv	Ukupna tržišna vrijednost	Količina jedinica u ponudi
1	Bitcoin	36.688.417.728 €	16.418.800 BTC
2	Ethereum	25.415.820.211 €	92.910.252 ETH
3	Ripple	8.957.504.099 €	38.291.387.790 XRP *
4	Litecoin	1.876.630.907 €	51.778.407 LTC
5	Ethereum Classic	1.578.724.331 €	93.097.273 ETC
6	NEM	1.317.288.744 €	8.999.999.999 XEM *
7	Dash	1.180.218.141 €	7.393.399 DASH
8	IOTA	1.070.288.334 €	2.779.530.283 MIOTA *
9	BitShares	587.438.644 €	2.596.460.000 BTS *
10	Monero	583.501.994 €	14.708.605 XMR
* Kriptovaluta koja se ne rudari Izvor: coinmarketcap.com			