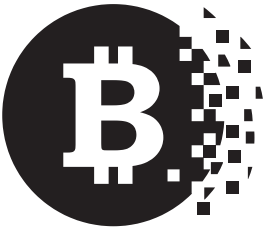
Natanijel Poper



DIGITALNO ZLATO

Prevela
Nevena Andrić

Laguna

Naslov originala

Nathaniel Popper
Digital Gold

Mami i tati

UVOD

Ponoć je prošla i mnogi gosti su već otišli na spavanje; za njima su ostale čaše sa zlatnožutim tragovima skupog viskija. Pokerska krupije-dama, čije su usluge za tu priliku iznajmljene od lokalnog kazina, otišla je pola sata ranije, ali preostali igrači su je ubedili da im ostavi sto i karte kako bi mogli igrati dalje. Grupa se još naginjala nad čoju, a iznad čipova, tri sprata više, protezala se zasvođena tavanica na drvenim gredama. Preko puta stola, velik zid, ceo u prozorima, gledao je na dugačak drveni mol, koji se ljuljuškao na svetlucavoj površini jezera Taho.

Za jednim krajem stola, leđima okrenut jezeru, sedeo je dvadesetdevetogodišnji Erik Vorhis; nije ličio na čoveka koji je tri godine ranije bio nezaposlen, do guše u dugovima zbog kreditnih kartica, i koji je radio kojekakve posliće kako bi platio kiriju u Nju Hempširu. Ove večeri Erik se, u svojim oksford cipelama od jelenske kože i po meri šivenim farmerkama, sjajno uklapao u društvo, i lagodno se zavitlavao sa investicionim menadžerom hedž fonda* koji je sedeo pored

* Posebna vrsta investicionog fonda za ograničen broj ulagača. (Prim. prev.)

njega. Zalisci su mu već bili uočljivi, ali još je bio mladolik i zračio je nekakvom svežinom. S rupicama na obrazima, Erik se šalio kako se prethodne večeri loše pokazao u partiji pokera, i rekao da je sve to deo njegove „dugoročne igre".

„Pripremao sam teren za večeras", reče, pa se široko iskezi i gurnu gomilu čipova na sredinu stola.

Erik je mogao da priušti gubitak. Nedavno je prodao kockarski veb-sajt koji je radio pomoću bitkoina – zagonetnog digitalnog novca i platne mreže. Taj kockarski sajt je kupio još 2012. godine za dvesta dvadeset i pet dolara, dao mu novo ime, *Satošidajs* (*SatoshiDice*), i godinu dana kasnije ga prodao za oko jedanaest miliona. Takođe je imao i zalihu bitkoina, koje je počeo da prikuplja nekoliko godina ranije, kada je svaki bitkoin vredeo svega nekoliko dolara. Bitkoini su sada koštali oko petsto dolara po komadu, te je njegov imetak trenutno vredeo više miliona. Iako su ga investitori i ozbiljni biznismeni isprva izbegavali, mnogi moćni ljudi sada su se zanimali za Erika. Na jezero Taho pozvao ga je Den Morhed, menadžer hedž fonda, sada na stolici pored njega, jer je želeo da se raspita o svemu i da popriča s ljudima koji su se obogatili u bitkoinskoj zlatnoj groznici.

Vorhisovi porivi za učešće u zlatnoj groznici, kao i porivi mnogih drugih u Morhedovoj kući, imali su u isto vreme i vrlo mnogo i vrlo malo veze s bogaćenjem. Nakon što je preko posta na *Fejsbuku* saznao za bitkoinsku tehnologiju, Erik je uskoro predvideo da će vrednost svakog bitkoina astronomski narasti. Ipak, dugo je verovao da će rast biti posledica višeslojnog bitkoinskog računarskog koda koji će korenito izmeniti preovlađujuće ustrojstvo moći u svetu, uključujući i banke Volstrita i vlade mnogih država – jednom rečju, imaće isto dejstvo na novac kao internet na poštu i medijsku industriju. Kako je Erik smatrao, neće njegovo lično bogaćenje biti jedina

posledica porasta vrednosti bitkoina. Ovaj porast dovešće i do jednog pravednijeg i mirnijeg sveta, u kom vlade neće moći da finansiraju ratove a pojedinci će imati kontrolu nad sopstvenim novcem i sopstvenom sudbinom.

Nije ni čudo što je, sa ovakvim ambicijama, Erik prošao buran put od vremena kada je bio nezaposlen u Nju Hempširu. Posle selidbe u Njujork, zajedno s još nekolicinom ubedio je blizance Vinklvos, Tajlera i Kamerona, čuvene po slučaju *Fejsbuka**, da ulože skoro milion dolara u startap preduzeće osnovano uz njegovu pomoć, a zvano *Bitinstant* (*BitInstant*). Ipak, saradnja se završila žestokom i dugotrajnom svađom, posle koje je Erik dao ostavku u kompaniji i s devojkom se preselio u Panamu.

U poslednje vreme Erik je vreme pretežno provodio u kancelariji u Panami, gde je morao da se nosi sa istražiteljima iz Komisije za berzu i hartije od vrednosti Sjedinjenih Američkih Država, koja spada među glavne agencije za finansijsku kontrolu; istražitelji su preispitivali uslove ugovora pod kojima je on prodao akcije svog startap preduzeća za bitkoine. Akcije su investitorima donele veliku dobit. A kontrolori, po Erikovoj proceni, nisu čak ni razumeli samu tehnologiju. Ipak, bili su u pravu utoliko što nije prijavio svoj udeo nadležnom regulatornom telu. Ova istraga je u svakom slučaju bila bolja od okolnosti u kojima se našao Erikov nekadašnji partner iz *Bitinstanta*, uhapšen po optužbi za pranje novca dva meseca ranije, u januaru 2014.

Sad već nije bilo lako uzdrmati Erika. Nije smetalo ni što je, za razliku od mnogih strastvenih pobornika bitkoina,

* Blizanci su tužili Marka Zakerberga da im je ukrao ideju za *Fejsbuk*. Ovaj slučaj detaljnije je objašnjen dalje u knjizi. (Prim. prev.)

umeo da se našali na svoj račun i na račun donkihotskog pokreta u čijem se središtu obreo.

„Stalno podsećam sebe da će bitkoin verovatno doživeti krah", rekao je on. „Ma koliko ja bio tvrdoglav po pitanju bitkoina, obuzdavam se i podsećam sebe da nove, novonastale stvari uglavnom ne uspeju da se probiju. Čisto da ne bih poludeo."

Ipak, nije odustajao, i to ne samo zato što mu se na bankovnom računu gomilalo bogatstvo. Ustrajavao je i zbog novog novca, projekta na kom su radili on i drugi trenutno prisutni na jezeru Taho – jer ovaj novi novac će, kako je verovao, promeniti svet.

Koncept bitkoina nastao je pod skromnijim okolnostima, pet godina ranije, kada ga je tajanstveni idejni tvorac, koji je koristio ime Satoši Nakamoto, pomenuo na jednoj malo poznatoj mejling listi.

Od samog početka Satoši je zamišljao digitalni pandan starinskom zlatu: novi, univerzalni novac, koji bi svako mogao posedovati i koji bi se svuda mogao trošiti. Kao zlato, ovi novi digitalni novčići vredeli su samo koliko je neko voljan da plati za njih – u početku ništa. Ali sistem je bio zamišljen tako da ni bitkoina, kao ni zlata, nikad ne bude u velikim količinama – samo dvadeset i jedan milion bi bio pušten u promet – i bilo bi teško falsifikovati ih. Kao što je slučaj i sa zlatom, da bi se proizveli novi bitkoini, bio je potreban rad – u ovom slučaju, kompjuterski rad.

Bitkoini su, kao novi nosilac vrednosti, takođe imali izvesnu uočljivu prednost u odnosu na zlato. Ne treba vam brod da biste prebacili bitkoine iz Londona u Njujork – treba vam samo privatni digitalni ključ i klik miša. Kao obezbeđenje,

Satoši je umesto naoružanih stražara upotrebljavao nerešive matematičke formule.

Ipak, poređenje sa zlatom ne može sasvim objasniti zašto je bitkoin privukao toliku pažnju. Svaka zlatna poluga uvek je postojala nezavisno od svake druge zlatne poluge. Bitkoini su, s druge strane, bili zamišljeni tako da postoje u domišljato načinjenoj, decentralizovanoj mreži, baš kao što i svi veb-sajtovi na svetu postoje samo na decentralizovanoj mreži poznatoj kao internet. Kao ni internetom, bitkoinskom mrežom nisu upravljale centralne vlasti. Nju su načinili i održavali svi ljudi koji bi joj pristupili putem računara, a to je mogao svako na svetu. Na internetu sve učesnike povezuje skup softverskih pravila poznatih kao internet protokoli, koji upravljaju protokom informacija. Bitkoin je imao sopstvene softverske protokole – pravila koja su upravljala funkcionisanjem sistema.

Tehničke pojedinosti mogle su biti toliko zamršene da vam pamet stane; podrazumevale bi komplikovanu matematiku i kriptografiju. Ali od najranijih dana, jedna grupa posvećenika uvidela je da je, u suštini, bitkoin naprosto novi način stvaranja, čuvanja i slanja novca. Bitkoini nisu bili kao dolari i evri, koje stvaraju centralne banke, a čuvaju ih velike i moćne finansijske institucije. Ovu valutu stvarali su i održavali korisnici, a novi novac lagano je deljen ljudima koji su podržavali mrežu.

Pošto je cilj bitkoinske mreže bio da se suprotstavi možda najmoćnijim institucijama našeg društva, pristalice su je od samog početka opisivale utopijskim rečima. Baš kao što je internet oduzeo moć velikim medijskim kućama i dao je u ruke blogerima i disidentima, bitkoin je pružao nadu da će moć biti oduzeta od banaka i vlasti i data narodu koji koristi novac.

Sve ovo je zvučalo prilično arogantno i izazivalo je mnogo prezira; kada bi čuli, obični ljudi su uglavnom zamišljali da je bitkoin nešto otprilike između Tamagočija – digitalnog ljubimca – i Ponzijeve prevare*.

Ipak, bitkoin je bio te sreće da stupi u svet u utopijskom trenutku, nakon finansijske krize koja je ukazala na mnoge mane postojećeg finansijskog i političkog sistema; ljudi su priželjkivali drugačija rešenja.

Pokret „Čajanka", pokret „Okupirajmo Volstrit" i *Vikiliks* – pored ostalih – imali su vrlo različite ciljeve, ali ih je krasila zajednička želja da oduzmu moć povlašćenoj eliti i vrate je pojedincima. Koliki je odziv bitkoin postigao kod svojih pobornika videlo se po tome koliko je različitih ljudi ostavilo dotadašnji život i pojurilo za onim što im je ova tehnologija obećavala – bili su to poklonici poput Erika Vorhisa i njegovih brojnih novih prijatelja. Nije bilo naodmet ni što će se, ako se bitkoin probije, rani korisnici veoma obogatiti. Kao što je Erik rado govorio: „Prvi put, koliko ja znam, da ste se mogli i bogatiti i istovremeno menjati svet."

Pošto je nudio i priliku za zaradu, bitkoin nije privlačio samo nezadovoljne revolucionare. Erikov domaćin Den Morhed bio je prinstonski đak i radio je za grupu *Goldman Saks* pre nego što je osnovao sopstveni hedž fond. Morhed je bio vodeći među imućnim ulagačima koji su nedavno ulili desetine miliona dolara u ekosistem bitkoina u nadi da će dobici biti veliki. U Silicijumskoj dolini, investitori i preduzetnici su se takmičili kako da pomoću bitkoina poboljšaju postojeće platne sisteme poput *Pejpala, Vize* i *Vestern juniona*, i tako preotmu posao Volstritu.

* Čuvena piramidalna šema. (Prim. prev.)

Čak i protivnici pokreta „Okupirajmo Volstrit“ ili „Čajanka“ shvatali su vrline univerzalnijeg novca, koji se ne mora menjati na svakom graničnom prelazu; prednosti digitalnog plaćanja prilikom kog ne morate davati lične podatke; pravednost jedne valute koju čak i najsiromašniji mogu da drže na digitalnom računu bez plaćanja velikih dažbina, umesto da koriste isključivo gotovinu; i pogodnosti platnog sistema koji omogućava servisima na internetu da naplate peni ili deset centi – kako biste vi pogledali jedan novinski članak ili preskočili reklamu – čime bi se zaobišla trenutna ograničenja, jer najmanja moguća transakcija pomoću kreditne kartice iznosi dvadeset ili trideset centi.

Na kraju su, ipak, mnogi koje je zanimala praktičnija primena bitkoina svejedno govorili o ovoj tehnologiji revolucionarnim jezikom: nazivali su je prilikom da se zaradi novac i istovremeno uzdrma status kvo. Za večerom, nekoliko sati pre kasnonoćne partije pokera, Morhed se našalio kako u tom trenutku svi bitkoini na svetu, uzeti zajedno, vrede koliko kompanija *Urban autfiters*, koja snabdeva svet iscepanim farmerkama i ukrasima za studentske spavaonice – dakle oko pet milijardi dolara.

„Baš je sumanuto, jelda?“, rekao je Morhed. „Kada za nekoliko vekova iskopaju ostatke našeg društva, kao u *Planeti majmuna*, verovatno će se ispostaviti da je bitkoin imao veći upliv u svetu od *Urban autfitersa*. Ovo je tek početak.“

Mnogi bankari, ekonomisti i državni zvaničnici smatrali su da su zaluđenici za bitkoin nevažni, da su to samo naivni pobornici nekakve zamišljene buduće groznice, pomalo nalik na holandsku pomamu za lalama četiri veka ranije. U nekoliko navrata, istorija bitkoina pokazala je da su protivnici s pravom upozoravali na opasnosti koje sa sobom nosi iskorak ka jednom digitalizovanom svetu bez centralne vlasti. Samo

nedelju dana pre Morhedovog okupljanja, najveća svetska kompanija zadužena za bitkoinske transakcije, firma poznata kao *Mt. Goks* (*Mt. Gox*), objavila je da je izgubila bitkoine korisnika u vrednosti od četiristo miliona dolara i da se povlači iz posla – bio je to tek najnoviji od mnogih takvih skandala koji su snašli korisnike bitkoina.

Ipak, nijedna kriza nije uspela da uništi polet pristalica bitkoina, i broj korisnika samo je rastao, i u dobru i u zlu. U vreme Morhedovog okupljanja, na raznim veb-sajtovima bilo je otvoreno više od pet miliona bitkoinskih novčanika, mahom van Sjedinjenih Država. Ljudi u Morhedovoj kući predstavljali su širok spektar persona koje su se našle u ovoj priči: bio je tu i jedan nekadašnji rukovodilac *Volmarta*, koji je doleteo iz Kine, pa nedavno diplomirani slovenački student, londonski bankar i dva stara člana studentskog bratstva sa Džordžijskog instituta za tehnologiju. Neke je pokretalo nepoverenje prema vladi, druge mržnja prema velikim bankama, a treći su imali ličnije razloge. Kineskog rukovodioca *Volmarta*, na primer, odgajili su baba i deda, begunci pred komunističkom revolucijom, koji su od sveg imetka sa sobom poneli samo zlato. Po njegovom mišljenju, u ovom nesigurnom svetu, bitkoini bi se mnogo lakše transportovali.

Upravo ovi ljudi, ljudi različitih životnih priča i različitih motivacija, stvorili su bitkoin i nastavili dalje u istom smeru; oni su predmet ove priče. Tvorac bitkoina, Satoši, nestao je još 2011. godine; za sobom je ostavio softver otvorenog koda*, koji korisnici mogu ažurirati i poboljšavati. Pet godina kasnije, po izvesnim procenama samo petnaest posto[1]

* Besplatan softver koji korisnici mogu menjati, pošto je uz njega dostupan i izvorni kod, što nije slučaj s plaćenim, licenciranim softverom. (Prim. prev.)

osnovnog kompjuterskog koda bitkoina ostalo je nepromenjeno u odnosu na Satošijev. Nevezano za rad na softveru, korist i moć bitkoina direktno su proporcionalne broju njegovih korisnika, kao što je i inače slučaj s novcem. Kad god se neka nova osoba pridruži, povećava se i verovatnoća opstanka bitkoina.

Ovo stoga nije obična priča o startap preduzeću, priča o usamljenom geniju koji je od sveta načinio šta je hteo i zaradio pozamašnu svotu novca. Ne, ovo je priča o grupnom izumu koji je iskoristio mnoga dominantna strujanja našeg doba: bes na vladu i Volstrit; bitke između Silicijumske doline i finansijske industrije; i nadu da će nas tehnologija spasti od naše sopstvene ljudske krhkosti, baš kao i strah od moći iste te tehnologije. Svaki čovek o kome govorimo u knjizi iz sopstvenih razloga se posvetio ovoj novoj ideji, ali sve njihove živote uobličili su ambicija, pohlepa, idealizam i ljudska krhkost, koji su pretvorili bitkoin iz opskurnog akademskog rada u industriju vrednu više milijardi dolara.

Za pojedine učesnike ishod je bilo bogatstvo, kakvo se moglo videti i u Morhedovoj kući, gde je na kamenom ulazu visio Morhedov lični grb. Za druge, sve se završilo siromaštvom, pa čak i zatvorom. Sam bitkoin je večito nadomak potpune propasti, ali ga uvek spase neko domišljato rešenje. Ipak, čak i ako na kraju propadne, već nam je na izuzetno zanimljiv način pokazao kako novac funkcioniše, ko iz njega izvlači korist i kako se on može poboljšati. Bitkoin verovatno neće u roku od pet godina zameniti dolar, ali nam daje nekakav mali uvid u to šta bi nas moglo snaći kada vlade neizbežno prestanu štampati lica mrtvih predsednika na skupom papiru.

Ujutru nakon velike pokeraške partije, dok su se gosti pakovali, Vorhis je sedeo iza Morhedove kuće, na kraju mola, visoko iznad vode pošto je te zime palo vrlo malo snega.

Sinoćno ushićenje, iskazano za pokeraškim stolom, beše nestalo. Zabrinutog lica govorio je o nedavnoj odluci da dâ ostavku na položaj glavnog izvršnog direktora bitkoinskog startap preduzeća u Panami. Radno mesto ga je sprečavalo da govori o revolucionarnom potencijalu bitkoina iz straha da će naškoditi kompaniji.

„Ne privlači me da vodim biznis, moja strast je da stvorim bitkoinski svet", objasnio je.

Povrh toga, njegovoj devojci se život u Panami smučio, a i Eriku je nedostajala porodica u Sjedinjenim Državama. Planirao je da se za nekoliko nedelja vrati u Kolorado, gde je odrastao. Zbog bitkoina, međutim, vratiće se kući kao bitno drugačiji čovek od onog koji je otišao. Sa ovim su se mogli poistovetiti i mnogi drugi pobornici bitkoina.

PRVI DEO

INIT: 85E655D6 417A1795 3363376A 624CDE5C 76E09589 CAC5F811 CC4B32C1 F20E533A
T = 0 7C20C838 85E655D6 417A1795 3363376A 4670AE6E 76E09589 CAC5F811 CC4B32C1
T = 1 7C3C0F86 7C20C838 85E655D6 417A1795 8C51BE64 4670AE6E 76E09589 CAC5F811
T = 2 FD1EEBDC 7C3C0F86 7C20C838 85E655D6 AF71B9EA 8C51BE64 4670AE6E 76E09589
T = 3 F268FAA9 FD1EEBDC 7C3C0F86 7C20C838 E20362EF AF71B9EA 8C51BE64 4670AE6E
T = 4 185A5D79 F268FAA9 FD1EEBDC 7C3C0F86 8DFF3001 E20362EF AF71B9EA 8C51BE64
T = 5 3EEB6C06 185A5D79 F268FAA9 FD1EEBDC FE20CDA6 8DFF3001 E20362EF AF71B9EA
T = 6 89BBA3F1 3EEB6C06 185A5D79 F268FAA9 0A34DF03 FE20CDA6 8DFF3001 E20362EF
T = 7 BF9A93A0 89BBA3F1 3EEB6C06 185A5D79 059ABDD1 0A34DF03 FE20CDA6 8DFF3001
T = 8 2C096744 BF9A93A0 89BBA3F1 3EEB6C06 ABFA465B 059ABDD1 0A34DF03 FE20CDA6
T = 9 2D964E86 2C096744 BF9A93A0 89BBA3F1 AA27ED82 ABFA465B 059ABDD1 0A34DF03
T = 10 5B35025B 2D964E86 2C096744 BF9A93A0 10E77723 AA27ED82 ABFA465B 059ABDD1
T = 11 5EB4EC40 5B35025B 2D964E86 2C096744 E11B4548 10E77723 AA27ED82 ABFA465B
T = 12 35EE996D 5EB4EC40 5B35025B 2D964E86 5C24E2A2 E11B4548 10E77723 AA27ED82
T = 13 D74080FA 35EE996D 5EB4EC40 5B35025B 68AA893F 5C24E2A2 E11B4548 10E77723
T = 14 0CEA5CBC D74080FA 35EE996D 5EB4EC40 60356548 68AA893F 5C24E2A2 E11B4548
T = 15 16A8CC79 0CEA5CBC D74080FA 35EE996D 0FCB1F6F 60356548 68AA893F 5C24E2A2
T = 16 F16F634E 16A8CC79 0CEA5CBC D74080FA 8B21CDC1 0FCB1F6F 60356548 68AA893F
T = 17 23DCB6C2 F16F634E 16A8CC79 0CEA5CBC CA9182D3 8B21CDC1 0FCB1F6F 60356548
T = 18 DCFF40FD 23DCB6C2 F16F634E 16A8CC79 69BF7B95 CA9182D3 8B21CDC1 0FCB1F6F
T = 19 76F1A2BC DCFF40FD 23DCB6C2 F16F634E 0DC84BB1 69BF7B95 CA9182D3 8B21CDC1
T = 20 20AAD899 76F1A2BC DCFF40FD 23DCB6C2 CC4769F2 0DC84BB1 69BF7B95 CA9182D3
T = 21 D44DC81A 20AAD899 76F1A2BC DCFF40FD 5BACE62D CC4769F2 0DC84BB1 69BF7B95
T = 22 F13AE55B D44DC81A 20AAD899 76F1A2BC 966AA287 5BACE62D CC4769F2 0DC84BB1
T = 23 A4195B91 F13AE55B D44DC81A 20AAD899 EDDBD6ED 966AA287 5BACE62D CC4769F2
T = 24 4984FA79 A4195B91 F13AE55B D44DC81A A530D939 EDDBD6ED 966AA287 5BACE62D
T = 25 AA6CB982 4984FA79 A4195B91 F13AE55B 0B5EEEA4 A530D939 EDDBD6ED 966AA287
T = 26 9450FBBC AA6CB982 4984FA79 A4195B91 09166DDA 0B5EEEA4 A530D939 EDDBD6ED
T = 27 0D936BAB 9450FBBC AA6CB982 4984FA79 6E495D4B 09166DDA 0B5EEEA4 A530D939
T = 28 D958B529 0D936BAB 9450FBBC AA6CB982 C2FA99B1 6E495D4B 09166DDA 0B5EEEA4
T = 29 1CFA5EB0 D958B529 0D936BAB 9450FBBC 6C49DB9F C2FA99B1 6E495D4B 09166DDA
T = 30 02EF3A5F 1CFA5EB0 D958B529 0D936BAB 5DA10665 6C49DB9F C2FA99B1 6E495D4B
T = 31 B0EAB1C5 02EF3A5F 1CFA5EB0 D958B529 F6D93952 5DA10665 6C49DB9F C2FA99B1
INIT: 85E655D6 417A1795 3363376A 624CDE5C 76E09589 CAC5F811 CC4B32C1 F20E533A
T = 0 7C20C838 85E655D6 417A1795 3363376A 4670AE6E 76E09589 CAC5F811 CC4B32C1
T = 1 7C3C0F86 7C20C838 85E655D6 417A1795 8C51BE64 4670AE6E 76E09589 CAC5F811
T = 2 FD1EEBDC 7C3C0F86 7C20C838 85E655D6 AF71B9EA 8C51BE64 4670AE6E 76E09589
T = 3 F268FAA9 FD1EEBDC 7C3C0F86 7C20C838 E20362EF AF71B9EA 8C51BE64 4670AE6E
T = 4 185A5D79 F268FAA9 FD1EEBDC 7C3C0F86 8DFF3001 E20362EF AF71B9EA 8C51BE64
T = 5 3EEB6C06 185A5D79 F268FAA9 FD1EEBDC FE20CDA6 8DFF3001 E20362EF AF71B9EA
T = 6 89BBA3F1 3EEB6C06 185A5D79 F268FAA9 0A34DF03 FE20CDA6 8DFF3001 E20362EF
T = 7 BF9A93A0 89BBA3F1 3EEB6C06 185A5D79 059ABDD1 0A34DF03 FE20CDA6 8DFF3001
T = 8 2C096744 BF9A93A0 89BBA3F1 3EEB6C06 ABFA465B 059ABDD1 0A34DF03 FE20CDA6
T = 9 2D964E86 2C096744 BF9A93A0 89BBA3F1 AA27ED82 ABFA465B 059ABDD1 0A34DF03
T = 10 5B35025B 2D964E86 2C096744 BF9A93A0 10E77723 AA27ED82 ABFA465B 059ABDD1
T = 11 5EB4EC40 5B35025B 2D964E86 2C096744 E11B4548 10E77723 AA27ED82 ABFA465B
T = 12 35EE996D 5EB4EC40 5B35025B 2D964E86 5C24E2A2 E11B4548 10E77723 AA27ED82
T = 13 D74080FA 35EE996D 5EB4EC40 5B35025B 68AA893F 5C24E2A2 E11B4548 10E77723
T = 14 0CEA5CBC D74080FA 35EE996D 5EB4EC40 60356548 68AA893F 5C24E2A2 E11B4548
T = 15 16A8CC79 0CEA5CBC D74080FA 35EE996D 0FCB1F6F 60356548 68AA893F 5C24E2A2
T = 16 F16F634E 16A8CC79 0CEA5CBC D74080FA 8B21CDC1 0FCB1F6F 60356548 68AA893F
T = 17 23DCB6C2 F16F634E 16A8CC79 0CEA5CBC CA9182D3 8B21CDC1 0FCB1F6F 60356548
T = 18 DCFF40FD 23DCB6C2 F16F634E 16A8CC79 69BF7B95 CA9182D3 8B21CDC1 0FCB1F6F
T = 19 76F1A2BC DCFF40FD 23DCB6C2 F16F634E 0DC84BB1 69BF7B95 CA9182D3 8B21CDC1
T = 20 20AAD899 76F1A2BC DCFF40FD 23DCB6C2 CC4769F2 0DC84BB1 69BF7B95 CA9182D3
T = 21 D44DC81A 20AAD899 76F1A2BC DCFF40FD 5BACE62D CC4769F2 0DC84BB1 69BF7B95
T = 22 F13AE55B D44DC81A 20AAD899 76F1A2BC 966AA287 5BACE62D CC4769F2 0DC84BB1
T = 23 A4195B91 F13AE55B D44DC81A 20AAD899 EDDBD6ED 966AA287 5BACE62D CC4769F2
T = 24 4984FA79 A4195B91 F13AE55B D44DC81A A530D939 EDDBD6ED 966AA287 5BACE62D
T = 25 AA6CB982 4984FA79 A4195B91 F13AE55B 0B5EEEA4 A530D939 EDDBD6ED 966AA287
T = 26 9450FBBC AA6CB982 4984FA79 A4195B91 09166DDA 0B5EEEA4 A530D939 EDDBD6ED
T = 27 0D936BAB 9450FBBC AA6CB982 4984FA79 6E495D4B 09166DDA 0B5EEEA4 A530D939
T = 28 D958B529 0D936BAB 9450FBBC AA6CB982 C2FA99B1 6E495D4B 09166DDA 0B5EEEA4
T = 29 1CFA5EB0 D958B529 0D936BAB 9450FBBC 6C49DB9F C2FA99B1 6E495D4B 09166DDA
T = 30 02EF3A5F 1CFA5EB0 D958B529 0D936BAB 5DA10665 6C49DB9F C2FA99B1 6E495D4B
T = 31 B0EAB1C5 02EF3A5F 1CFA5EB0 D958B529 F6D93952 5DA10665 6C49DB9F C2FA99B1
INIT: 85E655D6 417A1795 3363376A 624CDE5C 76E09589 CAC5F811 CC4B32C1 F20E533A
T = 0 7C20C838 85E655D6 417A1795 3363376A 4670AE6E 76E09589 CAC5F811 CC4B32C1
T = 1 7C3C0F86 7C20C838 85E655D6 417A1795 8C51BE64 4670AE6E 76E09589 CAC5F811
T = 2 FD1EEBDC 7C3C0F86 7C20C838 85E655D6 AF71B9EA 8C51BE64 4670AE6E 76E09589
T = 3 F268FAA9 FD1EEBDC 7C3C0F86 7C20C838 E20362EF AF71B9EA 8C51BE64 4670AE6E
T = 4 185A5D79 F268FAA9 FD1EEBDC 7C3C0F86 8DFF3001 E20362EF AF71B9EA 8C51BE64
T = 5 3EEB6C06 185A5D79 F268FAA9 FD1EEBDC FE20CDA6 8DFF3001 E20362EF AF71B9EA
T = 6 89BBA3F1 3EEB6C06 185A5D79 F268FAA9 0A34DF03 FE20CDA6 8DFF3001 E20362EF
T = 7 BF9A93A0 89BBA3F1 3EEB6C06 185A5D79 059ABDD1 0A34DF03 FE20CDA6 8DFF3001
T = 8 2C096744 BF9A93A0 89BBA3F1 3EEB6C06 ABFA465B 059ABDD1 0A34DF03 FE20CDA6
T = 9 2D964E86 2C096744 BF9A93A0 89BBA3F1 AA27ED82 ABFA465B 059ABDD1 0A34DF03
T = 10 5B35025B 2D964E86 2C096744 BF9A93A0 10E77723 AA27ED82 ABFA465B 059ABDD1
T = 11 5EB4EC40 5B35025B 2D964E86 2C096744 E11B4548 10E77723 AA27ED82 ABFA465B
T = 12 35EE996D 5EB4EC40 5B35025B 2D964E86 5C24E2A2 E11B4548 10E77723 AA27ED82
T = 13 D74080FA 35EE996D 5EB4EC40 5B35025B 68AA893F 5C24E2A2 E11B4548 10E77723
T = 14 0CEA5CBC D74080FA 35EE996D 5EB4EC40 60356548 68AA893F 5C24E2A2 E11B4548
T = 15 16A8CC79 0CEA5CBC D74080FA 35EE996D 0FCB1F6F 60356548 68AA893F 5C24E2A2
T = 16 F16F634E 16A8CC79 0CEA5CBC D74080FA 8B21CDC1 0FCB1F6F 60356548 68AA893F
T = 17 23DCB6C2 F16F634E 16A8CC79 0CEA5CBC CA9182D3 8B21CDC1 0FCB1F6F 60356548
T = 18 DCFF40FD 23DCB6C2 F16F634E 16A8CC79 69BF7B95 CA9182D3 8B21CDC1 0FCB1F6F
T = 19 76F1A2BC DCFF40FD 23DCB6C2 F16F634E 0DC84BB1 69BF7B95 CA9182D3 8B21CDC1
T = 20 20AAD899 76F1A2BC DCFF40FD 23DCB6C2 CC4769F2 0DC84BB1 69BF7B95 CA9182D3

PRVO POGLAVLJE

10. januar 2009.

Bila je subota. Njegovom sinu je bio rođendan. Vreme u Santa Barbari bilo je divno. Snaja mu je upravo stigla iz Francuske. Ipak, Hal Fini je morao da bude za kompjuterom. Ovaj dan je čekao već mesecima i, u izvesnom smislu, decenijama.

Hal nije ni pokušao da objasni supruzi Fren čime se bavi. Bila je fizioterapeutkinja i slabo je razumela šta on to radi na kompjuteru. A odakle bi uopšte i počeo? Dušo, pokušavam da napravim novu vrstu novca.

Upravo to mu je, u suštini, bila namera kada je, posle dugog jutarnjeg trčanja, seo u svoju skromnu kućnu kancelariju: jedan ugao dnevne sobe s velikim starim pisaćim stolom, koji su uglavnom zauzimala četiri kompjuterska monitora različitih oblika i marke, svi priključeni na različite računare, namenjene za rad i u lične svrhe. Prostor koji nije zauzimala kompjuterska oprema bio je prekriven rusvajem papira, svezaka i starih programerskih priručnika. Naoko i nije bilo ništa posebno. Ali sedeći tu, Hal je video trem na drugoj strani dnevne sobe, okupan kalifornijskim suncem

čak i sredinom januara. Levo od njega na tepihu je ležao Arki, njegov verni rodezijski ridžbek, nazvan po zvezdi u sazvežđu Volar. Ovde se osećao kao svoj na svome, i ovde se uglavnom bavio kreativnim programerskim radom.

Uključio je ogromni *IBM ThinkCentre*, smestio se, i kliknuo na link koji je prethodnog dana, dok je radio, dobio u imejlu: www.bitcoin.org.

Prvi put je ugledao reč „bitkoin" nekoliko meseci pre toga, u poruci poslatoj na jednu od mnogih mejling lista kojima je pripadao. Prepiska se uglavnom vodila između dugogodišnjih poznanika i sagovornika, zainteresovanih za prilično usko polje kodiranja, kojim se i sam bavio. Ipak, ovaj imejl došao je od nepoznatog čoveka pod imenom Satoši Nakamoto – a unutra je bilo opisana izvesna elektronska gotovina, zvučno nazvana „bitkoin".[2] Hal je već dugo eksperimentisao s digitalnim novcem – dovoljno dugo da bude sumnjičav i zapita se bi li tako nešto uopšte moglo uspeti. Ipak, nešto u ovom imejlu zapalo mu je za oko. Satoši je obećavao pare kojima se ne bi moralo raspolagati putem banke ili preko nekog trećeg. Sistem bi u potpunosti postojao u kolektivnoj kompjuterskoj memoriji korisnika. Na Hala je najveći utisak ostavila Satošijeva tvrdnja da bi korisnici mogli posedovati i razmenjivati bitkoine bez davanja ličnih podataka centralnim vlastima. Hal je dobar deo karijere proveo u radu na programima koji omogućuju ljudima da izvrdaju budnu prismotru vlasti.

Pošto je pročitao opis na devet strana,[3] u okviru, kako se činilo, nekakvog akademskog rada, Hal je poletno odgovorio.

„Kad je osnovana *Vikipedija*, nisam mislio da će uspeti, ali se odlično pokazala iz donekle sličnih razloga", napisao je grupi.

Zbog sumnjičavosti drugih članova mejling liste, Hal je nagovarao Satošija da zapravo napiše deo koda za opisani

sistem. Nekoliko meseci kasnije, ove januarske subote, Hal je skinuo Satošijev kod s bitkoinskog veb-sajta. Prost egzekutivni fajl instalirao je bitkoinski program i automatski na desktopu otvorio jasan i uredan prozor.

Kada se program prvi put otvorio, automatski je napravio listu bitkoinskih adresa koje će predstavljati brojeve Halovih računa u sistemu, kao i lozinku, odnosno privatni ključ, koji mu je omogućavao pristup svakoj od ovih adresa. Pored toga, program je imao samo nekoliko funkcija. Glavna, „pošalji novac", nije naročito zanimala Hala pošto nije imao novca za slanje. Ali pre nego što je stigao da pročačka dalje, program se zakočio.

Ovo nije odbilo Hala. Pošto je pregledao logove svog računara, pisao je Satošiju i objasnio mu šta se desilo kada je kompjuter pokušao da mu se poveže s drugim računarima na mreži. Prema logovima, pored Halovog na mreži su bila još samo dva računara, i to oba na istoj IP adresi – verovatno Satošijevoj – povezana preko internet provajdera iz Kalifornije.[4]

U roku od sat vremena Satoši je odgovorio; bio je razočaran zbog neuspeha. Rekao je da je dobro testirao sve[5] i da nije naišao na probleme. Ipak, rekao je Halu da jeste smanjio program kako bi se lakše skidao sa interneta, što je sigurno izazvalo problem.

„Biće da sam pogrešno procenio", pisao je Satoši s gotovo opipljivom frustracijom.

Satoši je poslao Halu novu verziju programa, u koju je vratio deo starog materijala, i zahvalio mu na pomoći. Kada se program opet ukočio, Hal se nije dao. Konačno ga je naterao da proradi pomoću programa pokrenutog van *Majkrosoft Vindousa*. Kada je proradio, Hal je na meniju kliknuo funkciju koja mu je delovala najzanimljivije: „Napravi novčiće."

Kada je ovo uradio, procesor njegovog računara čujno se dao u naporan rad.

Pošto je sve radilo, Hal je mogao da napravi pauzu i posveti se porodičnim dužnostima, između ostalog zajedničkoj večeri u obližnjem kineskom restoranu i maloj rođendanskoj proslavi za sina. Satošijeva priložena uputstva tvrdila su da bi stvaranje novca moglo potrajati „danima ili mesecima, zavisno od brzine vašeg računara i konkurencije na mreži".

Hal je na brzinu naškrabao poruku Satošiju da sve radi: „Moram da idem, ali ću ostaviti ovu verziju uključenu neko vreme."

Hal je već dovoljno iščitao da bi razumeo osnove onoga što mu je kompjuter sada radio. Kada se bitkoinski program uključi, ulogovao bi se u određen čet-kanal i našao druge računare na kojima je isti softver pušten u pogon – u suštini, trenutno samo Satošijeve kompjutere. Svi kompjuteri su pokušavali da uhvate nove bitkoine, puštene u sistem u grupama, svežnjevima, od po pedeset novčića. Svaka nova grupacija bitkoina bila bi dodeljena adresi jednog korisnika koji bi se povezao na mrežu i pobedio u nekoj vrsti trke u rešavanju kompjuterske zagonetke. Kada bi računar pobedio u jednoj etapi trke i uhvatio nove novčiće, sve ostale mašine na mreži bi ažurirale zajedničku evidenciju o broju bitkoina na bitkoinskoj adresi tog računara. Onda bi računari na mreži automatski počeli da se trkaju u rešavanju novog problema kako bi otključali sledeću grupu od pedeset novčića.

Te večeri, kada se Hal vratio za kompjuter, odmah je video da je već zaradio pedeset bitkoina, koji su sada stajali ubeleženi pored jedne njegove bitkoinske adrese,[6] i takođe bili uneti u javnu knjigu finansija, gde se vodila evidencija o svim bitkoinima. Ovih sedamdeset osam grupa tek proizvedenih novčića bile su među prve četiri hiljade bitkoina

puštenih u svet. U to doba nisu vredeli ama baš ništa, ali to nije umanjilo Halov polet. U imejlu je čestitao Satošiju i poslao je imejl čitavoj mejling listi; dopustio je sebi da se upusti u maštarije.

„Zamislite da bitkoin bude uspešan i postane glavni sistem plaćanja širom sveta", pisao je on. „Onda bi ukupna vrednost ove valute trebalo da je jednaka ukupnom svetskom bogatstvu."

Po njegovim proračunima, to bi značilo da svaki bitkoin vredi desetak miliona dolara.

„Iako su mali izgledi da bitkoin uspe do te mere, zar su zaista baš jedan prema sto miliona? Vredi razmisliti o tome", napisao je pre nego što se izlogovao.

Hal Fini je dugo razmatrao kako će se budućnost, po izgledu i teksturi, razlikovati od sadašnjice.

Kao jedno od četvoro dece naftnog inženjera koji je mnogo putovao, Hal je iščitao naučnofantastične klasike, ali je takođe iz zabave čitao knjige o aritmetici i kasnije je pohađao Kalifornijski tehnološki institut. Nikad nije posustajao pred intelektualnim izazovima. Na prvoj godini fakulteta pohađao je kurs o teoriji gravitacionog polja predviđen za postdiplomce.

Ipak, nije bio tipičan zaluđenik za nauku. Bio je krupan, atletski građen, voleo je da se skija u kalifornijskim planinama i, za razliku od većine studenata Kalifornijskog instituta, nije bio stidljiv i nezgrapan u društvu. Sportski duh je prenosio i na intelektualno polje. Posle čitanja romana Larija Nivena, koji raspravlja o mogućnosti kriogenskog zamrzavanja i kasnijeg oživljavanja ljudi, Hal nije samo u spavaonici razmišljao šta bi to sve omogućilo. Našao je fondaciju posvećenu ostvarivanju ove ideje i prijavio se da prima časopis Fondacije

za produženje života *Alkor*. Na kraju je platio da se njegovo telo i tela njegove porodice posle smrti stave u hladnjače blizu Los Anđelesa.

Pojava interneta dobro je došla Halu; sada je mogao stupiti u vezu s drugim, udaljenim ljudima koji su razmišljali o slično opskurnim ali radikalnim idejama. Čak i pre nego što je osmišljen prvi brauzer, Hal se pridružio najranijim internet zajednicama, grupama s nazivima kao *Sajferpankeri* i *Ekstropijanci*, gde se bacio u rasprave o tome kako bi se nova tehnologija dala upotrebiti za stvaranje budućnosti iz snova.

Ove grupe su bile izuzetno opsednute pitanjem kako će tehnologija promeniti ravnotežu moći između korporacija i vlada s jedne i pojedinaca s druge strane. Tehnologija je očito davala pojedincima više moći nego ikad ranije. Internet u povoju omogućio je ovim ljudima da razgovaraju sa srodnim dušama i šire svoje ideje na dotad nemoguće načine. Ali neprestano se diskutovalo o tome kako nadolazeća digitalizacija života takođe daje vladama i kompanijama veću kontrolu nad možda najvrednijom i najopasnijom robom informacionog doba: samim informacijama.

U danima pre kompjutera, vlade su svakako imale dosijee građana, ali o većini je bilo nemoguće pronaći baš mnogo podataka. Devedesetih godina dvadesetog veka, međutim – mnogo pre nego što je otkriveno da Državna bezbednosna agencija (NSA) njuška po mobilnim telefonima običnih građana i pre nego što se čitava nacija upustila u raspravu o pravilima privatnosti na *Fejsbuku* – sajferpankeri su uvideli da digitalizacija života veoma olakšava vlastima da prikupljaju podatke o građanima, zbog čega je lakše i da ti isti podaci padnu u zločinačke ruke. Sajferpankeri su postali opsednuti zaštitom ličnih podataka i čuvanjem privatnosti. Sajferpankerski manifest, koji je Erik Hjuz, matematičar s

Berklija, poslao na mejling listu 1993. godine, počinjao je rečima: „U elektronsko doba, privatnost je neophodan uslov za postojanje otvorenog društva."

Ovaj način razmišljanja delimično je proistekao iz libertarijanske politike, popularne u Kaliforniji još od sedamdesetih i osamdesetih godina dvadesetog veka. Sumnjičavost prema vladi bila je prirodna za programere poput Hala, koji su se trudili da programiranjem stvore novi svet i nisu bili primorani da se oslanjaju ni na koga drugog. Hal je posisao ove ideje na Kalifornijskom tehničkom institutu, kao i iz romana Ajn Rand. Ipak, pitanje privatnosti u doba interneta bilo je popularno i van libertarijanskih krugova, među borcima za ljudska prava i drugim protestnim pokretima.

Niko među sajferpankerima nije smatrao da rešenje problema leži u bekstvu od tehnologije. Umesto toga, Hal i ostali nameravali su da odgovore pronađu upravo u tehnologiji, i naročito u nauci koja se bavi enkripcijom, šifrovanjem podataka. Enkripcione tehnologije su, istorijski gledano, prvenstveno bile povlastica najmoćnijih institucija. Pojedinci su mogli pokušavati da zaštite svoje razgovore i poruke šiframa, ali vlada i oružane snage gotovo uvek su posedovale moć da tako nešto dešifruju. Sedamdesetih i osamdesetih godina dvadesetog veka, međutim, matematičari sa Stanforda i Masačusetskog tehnološkog instituta došli su do niza revolucionarnih otkrića koja su sada prvi put omogućila običnim ljudima da šifruju ili skrembluju poruke tako da ih može dešifrovati samo primalac, a ne može ih odgonetnuti čak ni najjači superkompjuter.

Svaki korisnik ove nove tehnologije, poznate kao asimetrična kriptografija ili kriptografija s javnim ključem, dobio bi javni ključ – jedinstvenu kombinaciju slova i brojeva, neku vrstu adrese koja se sme podeliti javno – i privatni ključ za

nju, koji treba da je poznat samo dotičnom korisniku. Dva ključa su matematički povezana na način koji obezbeđuje da samo korisnik, ili recimo korisnica – nazovimo ovu korisnicu Alis, kao što su kriptografi imali običaj – koji poseduje privatni ključ može otključati poruku poslatu na svoj javni ključ, svoju javnu adresu. Jedinstvenu vezu između svakog javnog i privatnog ključa određivale su složene matematičke jednačine, tako oštroumno osmišljene da samo pomoću javnog ključa niko nikad ne bi obrnutim postupkom mogao doći do odgovarajućeg privatnog ključa – čak ni najjači superkompjuter. Svi ovi činioci kasnije će odigrati ključnu ulogu u radu bitkoinskog softvera.

Godine 1991. Hal se upoznao s mogućnostima kriptografije s javnim ključem posredstvom revolucionarnog kriptografa Dejvida Čoma, koji je eksperimentisao ne bi li ustanovio kako se kriptografija s javnim ključem može upotrebiti za zaštitu privatnosti pojedinca.

„Meni ovo deluje vrlo očigledno", rekao je Hal ostalim sajferpankerima kad se prvi put susreo sa Čomovim delima. „Suočeni smo s problemom gubitka privatnosti, nadolazeće kompjuterizacije, ogromnih baza podataka, dalje centralizacije – a Čom nam nudi jedan potpuno nov pravac, pravac koji će dati moć u ruke pojedincu, a ne vladi ili korporacijama."

Kao i obično kad naiđe na nešto uzbudljivo, Hal nije samo pasivno čitao o tome. Noću i vikendom, posle posla – radio je kao softverski developer – počeo je da pomaže u dobrovoljnom projektu zvanom „Dosta dobra privatnost" (*Pretty Good Privacy* ili PGP), koji je omogućavao ljudima da jedni drugima šalju poruke šifrovane pomoću kriptografije s javnim ključem. Osnivač projekta Fil Zimerman bio je antinuklearni aktivista i želeo je disidentima da omogući

komunikaciju bez prismotre vlasti. Uskoro je Zimerman primio Hala u PGP kao svog prvog zaposlenog.

Idealistički projekti poput PGP-a uglavnom nemaju veliku publiku. Ipak, postalo je jasno koliko je ova tehnologija možda značajna kada je savezno tužilaštvo pokrenulo krivičnu istragu protiv PGP-a i Zimermana. Vlada je klasifikovala enkripcione tehnologije poput PGP-a kao ratnu opremu ravnu oružju, i zbog ove oznake ju je bilo nezakonito izvoziti. Iako se od tužbe naposletku odustalo, Hal je morao godinama da pauzira sa učešćem u PGP-u i nikad nije smeo da prizna kako je zaslužan za pojedine važne doprinose projektu.

Ekstropijanci i sajferpankeri su sprovodili u delo nekoliko različitih eksperimenata, s namerom da pruže pojedincu više moći u odnosu na tradicionalne predstavnike vlasti. Ipak, u središtu njihovih napora da zamisle i ostvare drugačiju budućnost, od samog početka je ležao novac.

Za svaku tržišnu ekonomiju novac je isto ono što su voda, vatra ili krv za ljudski ekosistem – osnovna supstanca neophodna da bi sve ostalo funkcionisalo. Postojeće valute, važeće samo unutar granica jedne zemlje i podložne uticaju tehnološki nepotkovanih banaka, programerima su se činile kao bespotrebno ograničenje. U naučnoj fantastici uz koju su Hal i ostali odrastali gotovo uvek se širom galaksija koristi univerzalni novac – u *Zvezdanim ratovima* to su standardni galaktički krediti. U trilogiji *Zora noći* Pitera F. Hamiltona to su jupiterski krediti.

Nisu u pitanju bile samo ambicije iz mašte; sajferpankeri su postojeći finansijski sistem posmatrali kao jednu od najvećih pretnji privatnosti pojedinca. Retko koji tip podataka otkriva toliko o osobi poput Alis, miljenice kriptografa,

kao njene novčane transakcije. Ako se njuškala domognu njenih bankovnih izveštaja o korišćenju kreditnih kartica, mogu da prate kuda se kretala nekog određenog dana. Nije slučajno što su bankovni izveštaji jedan od glavnih načina za praćenje begunaca pred zakonom. Sajferpankerski manifest Erika Hjuza ovim se pozabavio nadugačko i naširoko. „Kada mehanizam koji omogućava transakciju razotkrije ko sam ja, više nemam privatnost. Ne mogu da se razotkrijem samo delimično; uvek moram u potpunosti da pokažem ko sam", pisao je Hjuz.

„Privatnost u otvorenom društvu zahtevala bi sisteme anonimne transakcije", dodao je on.

Gotovina je uvek omogućavala anonimno plaćanje, ali gotovina se nije prenela u digitalni svet. Čim je novac postao digitalan, neka treća strana, recimo banka, uvek je bila umešana i mogla je da prati transakciju. Hal, Čom i sajferpankeri želeli su gotovinu digitalnog doba, gotovinu bezbednu za upotrebu bez žrtvovanja privatnosti korisnika, gotovinu koju bi bilo nemoguće krivotvoriti. Iste one godine kada je Hjuz napisao manifest, Hal je poslao imejl grupi koja je zamislila neku vrstu digitalne gotovine, prilikom čijeg korišćenja se „ne evidentira gde trošim sopstveni novac. Banka samo zna koliko podižem svakog meseca".

Mesec dana kasnije, Hal je čak smislio drzak naziv: „Danas sam smislio novo ime za digitalnu gotovinu: KREŠ, kao KRipto kEŠ."

Još pre nego što su sajferpankeri počeli da se zanimaju za ovo, Čom je već bio smislio svoju verziju. Sa instituta u Amsterdamu, gde je radio, napravio je digikeš (*DigiCash*), internet novac koji se mogao trošiti svuda u svetu a da korisnici ne moraju odati privatne podatke. Sistem je koristio kriptografiju s javnim ključem i dozvoljavao je nešto što

je Čom nazivao slepim digitalnim potpisima; oni su omogućavali ljudima transakcije bez davanja informacija o sebi. Kada je banka *Mark Tven* u Sjedinjenim Državama počela da eksperimentiše s digikešom, Hal je otvorio račun u njoj.

Ipak, Čomov postupak neće se dopasti Halu i ostalima.[7] Kod digikeša, centralna organizacija, to jest Čomova kompanija, morala je da potvrdi svaki digitalni potpis. Ovo je značilo da se do izvesne mere moralo ukazati poverenje toj centralnoj organizaciji da neće dirati bilans, kao i da neće propasti u poslu. I zaista, kada je Čomova kompanija bankrotirala 1998. godine, digikeš je propao s njom.[8] Ovo je brinulo Hala i ostale, te su se trudili da naprave digitalnu gotovinu koja se neće oslanjati na nekakvu centralnu instituciju. Problem je, naravno, bio to što bi neko morao paziti da ljudi prosto ne iskopiraju svoj digitalni novac i ne potroše ga dvaput. Neki sajferpankeri jednostavno su odustali od projekta, ali Hal se nije tako lako predavao.

Ironično je što, iako je Hal bio toliko oran da napravi novi novac, njegovo zanimanje nije bilo prvenstveno finansijske prirode. Programi koje je pisao, poput PGP-a, bili su izričito predviđeni da budu dostupni svakom, besplatno. Njegovo političko nepoverenje prema vladi pak nije vuklo korene iz sebičnog ogorčenja što mora da plaća porez. Devedesetih godina dvadesetog veka Hal je imao običaj da izračuna najveću moguću svotu za svoju poresku klasu i poslao bi ček tog iznosa kako ne bi morao da se gnjavi i popunjava formulare o ličnom dohotku radi procene poreza.[9] Kupio je skromnu kuću na obodu Santa Barbare i ostao tu godinama. Kao da mu nije smetalo što radi u dnevnoj sobi ili što su se plave fotelje ispred njegovog pisaćeg stola izlizale. Umesto sebičnosti, činilo se da ga pokreće radoznalost intelektualne

prirode, jasno vidljiva u svakom njegovom imejlu, kao i ideje o tome koliko drugi ljudi zaslužuju.

„Uopšteno govoreći, sve što sada radimo, radimo da bi Veliki Brat postao bespotreban. Naš posao je važan“,[10] pisao je Hal sadruzima. „Ako sve prođe kako treba, možda ćemo se jednog dana osvrnuti i shvatiti kako je ovo nešto najvažnije što smo ikad uradili.“

DRUGO POGLAVLJE

1997.

Pomisao na stvaranje nove vrste novca mnogima će izgledati vrlo čudna, pa čak i besmislena. Za brojne savremene ljude, novac naprosto čine papirne novčanice i kovanice koje izdaju pojedine zemlje. Pravo na kovanje novca spada u stavke koje definišu naciju, čak i male nacije kao što su Vatikan ili Mikronezija.

Ipak, to je tako tek manje-više odnedavno. Do Američkog građanskog rata, većinu novca u upotrebi u Sjedinjenim Državama izdavale su privatne banke; vladao je potpun rusvaj suparničkih novčanica, koje su postajale bezvredne ako im matična banka propadne. Mnoge države u to doba upotrebljavale su inostrane novčiće.

Ovo se samo nastavljalo na mnogo dugotrajnije stanje; ljudi su se gotovo odvajkada trudili da nađu bolji oblik novca, pa su usput isprobali zlato, školjke, kamene diskove i dudovu koru.

U potrazi za boljim oblikom novca, suština je uvek bila pronaći neki pouzdaniji i jednoobrazniji način da se ustanovi vrednost svega što nas okružuje – nekakvo zajedničko merilo,

zahvaljujući kom bismo mogli pouzdano uporediti vrednost drvene grede, jednog časa stolarskog rada i slike šume. Kako se izrazio sociolog Najdžel Dod,[11] valjan novac nam „omogućava da pretvorimo kvalitativne razlike između predmeta u kvantitativne razlike, koje nam onda omogućavaju razmenu".

Valuta kakvu su zamišljali sajferpankeri oterala bi standardizaciju koju nam novac pruža u logičku krajnost i donela nam univerzalni novac koji se može trošiti bilo gde; ne bismo bili ograničeni državnim valutama, ne bismo ih morali nositi sa sobom i razmenjivati na svakoj granici, ovako kao sada.

Dok su se trudili da osmisle novu valutu, sajferpankeri nisu gubili iz vida odlike uspešnog novca. Dobar novac obično je trajan (zamislite novčanicu od jednog dolara odštampanu na toalet-papiru), lako prenosiv (zamislite novčić od četvrt dolara težak deset kilograma), razmenjiv (zamislite da imamo samo novčanice od sto dolara i nemamo sitninu), jednoobrazan (zamislite da sve novčanice od jednog dolara izgledaju različito), i teško dostupan (zamislite novčanice koje svako može iskopirati).

Ipak, pored svih ovih odlika, novac uvek zahteva i nešto mnogo manje opipljivo, a to je vera ljudi. Ako će farmer da prihvati novčanicu od dolar u zamenu za žito oko kog se marljivo trudio, mora verovati da će taj dolar vredeti nešto u budućnosti, svejedno što je u pitanju samo zeleno parče papira. Ključna odlika uspešnog novca, vremenski gledano, nije ko ga je izdao – pa čak ni koliko je lako prenosiv ili izdržljiv – već broj ljudi voljnih da ga upotrebljavaju.

U dvadesetom veku dolar je služio kao globalna valuta, uglavnom zato što je većina ljudi verovala da Sjedinjene Države i njihov monetarni sistem imaju praktično najveće izglede za preživljavanje. Ovo objašnjava zašto su ljudi prodavali lokalne valute i štedeli u dolarima.

Veza između novca i vere već dugo pretvara pojedince koji uspevaju da stvore i zaštite novac u kvazireligijske ličnosti. Engleska reč *money*, novac, potiče od imena starorimske boginje Junone Monete, u čijim se hramovima kovao novac. U Sjedinjenim Državama, prema guvernerima centralne banke – Saveznih rezervi, koji imaju zadatak da nadziru snabdevanje novcem, odnose se kao prema nekakvim prorocima; njihove objave se analiziraju kao kozje iznutrice u stara vremena. Predstavnicima Saveznih rezervi podarene su moć i nezavisnost kakve nema gotovo nijedan drugi državni zvaničnik, a zadatak zaštite državne valute poveren je naročitoj agenciji, Tajnoj službi, koja je tek kasnije dobila i dodatnu odgovornost da štiti predsednikov život.

Alan Grinspen, možda najčuveniji prorok Saveznih rezervi – premda je i on imao svoje mane – znao je da novac nije nešto što samo bankari centralne banke mogu stvarati. U svom govoru 1996. godine, baš kada su sajferpankeri uznapredovali u ogledima, Grinspen je izjavio da zamišlja kako bi tehnološka revolucija mogla ponovo otvoriti mogućnost postojanja privatnog novca, i da bi to u stvari moglo biti korisno:

„Zamislivo je da će, u bliskoj budućnosti, posrednici u elektronskom plaćanju, koji posreduju na primer putem pretplatnih kartica ili 'digitalne gotovine', osnovati specijalizovane korporacije za pružanje ove usluge – korporacije dobrog finansijskog stanja i dobrog kreditnog rejtinga."[12]

U godinama koje su usledile za Grinspenovim govorom, sajferpankerski svet sav je vrveo od uposlenosti. Godine 1997. britanski naučnik po imenu Adam Bak[13] poslao je na sajferpankersku mejling listu plan za nešto što je nazvao

heškeš (*hashcash*), i to je rešilo jedan od najosnovnijih problema koji su usporavali projekat digitalne gotovine: navodnu nemogućnost da se napravi bilo kakav digitalni fajl koji se ne može bezbroj puta iskopirati.

Bak je, radi rešenja ovog problema, došao na pametnu ideju, koja će se kasnije ispostaviti kao važan činilac za stvaranje bitkoinskog softvera. U svom konceptu, Bak je kreativno iskoristio jedan od glavnih elemenata kriptografije s javnim ključem: kriptografske funkcije za sažimanje ili heš funkcije. To su matematičke jednačine koje je lako rešiti, ali je teško na njih primeniti obrnuti inženjering, baš kao što je manje-više lako pomoću papira i olovke pomnožiti 2.903 sa 3.571, ali je daleko teže ustanoviti koja dva broja treba pomnožiti da bi se dobilo 10.366.613. U suštini, kod heškeša, kompjuteri su morali da dokuče koja dva broja se mogu pomnožiti da bi se dobio rezultat 10.366.613, premda su posredi bili znatno teži matematički problemi. Zapravo su bili toliko teški da je računar mogao samo više puta da nagađa s ciljem da naposletku nađe pravi odgovor. Kada bi kompjuter došao do odgovora, zaradio bi heškeš.

Stvaranje heškeša ovim metodom bilo je korisno u kontekstu digitalnog novca jer je postizalo cilj: da heškeš bude redak i teško dostupan – a to je odlika valjanog novca, ali ne i digitalnih fajlova, koji se uglavnom lako daju umnožiti. Računaru je bio potreban velik trud da bi stvorio svaku novu jedinicu heškeša, i stoga je sam taj proces zadobio ime *proof-of-work* (dokaz o radu)* – što će kasnije postati glavna inovacija na kojoj će se zasnivati bitkoin. Glavni problem s Bakovim sistemom, ako ga posmatramo kao neku vrstu

* Dokaz o radu je podatak koji je teško ili skupo proizvesti, ali ga je lako proveriti. (Prim. prev.)

digitalnog novca, bio je što se svaka jedinica heškeša mogla upotrebiti samo jednom i svako u sistemu bi morao da stvara nove jedinice kad god poželi da ih koristi. Još jedan problem bio je što osoba s beskrajno dobrim kompjuterom može da proizvodi sve više i više heškeša i tako smanjuje vrednost svake jedinice.

Godinu dana nakon što je Bak učinio svoj program dostupnim, još dva člana sajferpankerske liste osmislila su sopstvene sisteme, i u njima ispravila pojedine mane heškeša; ishod su bili digitalni žetoni koji su zahtevali „dokaz o radu", ali su se mogli koristiti višekratno. Jedan je bio koncept nazvan bit-zlato[14]; njegov izumitelj Nik Sabo, stručnjak za računarsku bezbednost, predstavio je ovu ideju bliskim saradnicima poput Hala Finija 1998, ali nikad je zapravo nije upotrebio u praksi. Drugi, poznat kao b-novac, potekao je od Amerikanca po imenu Vej Dej.[15] Hal je napravio sopstvenu varijantu, manje privlačnog naziva[16]: dokazi o radu za višekratnu upotrebu (*reusable proofs of work*, RPOW).

Razgovor o ovim idejama na sajferpankerskoj listi i u srodnim grupama ponekad je ličio na prepucavanje suparničke braće koja se nadmeću. Sabo se brecao na druge predloge, govorio da se svi previše oslanjaju na specijalizovan računarski hardver umesto na softver. Ipak, ovi muškarci – a svi su bili muškarci – takođe su stekli veliko međusobno poštovanje. Premda su im ogledi bili neuspešni, ambicije su im rasle i više se nisu svodile samo na anonimni novac. Između ostalog, Bak, Sabo i Fini su pokušavali da savladaju problem dažbina i prepreka trenutnog finansijskog sistema, u kom banke naplaćuju takse na svaku transakciju i otežavaju vam slanje novca preko državnih granica.

„Želimo potpuno anonimne, prenosive jedinice za razmenu, i transakcije po izuzetno niskim cenama. Ako nam to

pođe za rukom (a očito pojedini ljudi oprobavaju digikeš i još ponešto slično), banke će postati zastareli fosili, baš kao što i zaslužuju", izjavio je Bak na sajferpankerskoj listi uskoro nakon što je pustio heškeš u promet.

Kada je pisac naučne fantastike Nil Stivenson 1999. objavio knjigu *Kriptonomikon*, istraživači sa sajferpankerske liste dobili su platonski ideal ka kom su mogli stremiti. U romanu, koji je u hakerskim krugovima postao legendaran, zamišljen je podzemni svet; ovaj svet funkcioniše zahvaljujući digitalnom zlatu, pri čijoj upotrebi ljudi ne moraju odavati ko su i šta su. U romanu je nadugačko opisana kriptografija koja je sve to omogućila.

Ipak, ogledi sajferpankera u stvarnom svetu i dalje su nailazili na praktične prepreke. Niko nije mogao smisliti kako da se stvori novac bez oslanjanja na centralnu instituciju, a mane takve institucije bile su moguća propast ili nadzor vlade. Ogledi su takođe nailazili i na suštinskije poteškoće, to jest kako naterati ljude da koriste nove digitalne žetone i da im pripišu vrednost. Pre nego što je na scenu stupio Satoši Nakamoto, a pošto je projekat za sobom imao ovakvu istoriju, mnogi ljudi koji bi vrlo verovatno bili pobornici bitkoina postali su krajnje blazirani. Stvaranje digitalnog novca delovalo je kao običan san, isto kao pretvaranje uglja u dijamante.

U avgustu 2008. godine Satoši je stupio u svet putem imejla koji je poslao tvorcu heškeša Adamu Baku; zamolio ga je da pogleda kratak rad u kom je opisao nešto po imenu bitkoin. Bak nije čuo ni za bitkoin niti za Satošija, i nije se naročito pozabavio imejlom osim što je usmerio Satošija na druge sajferpankerske oglede koji su mu možda promakli.

Šest nedelja kasnije, na Noć veštica, Satoši je poslao detaljniji predlog na specijalizovanu i veoma akademski orijentisanu mejling listu posvećenu prvenstveno kriptografiji – bila je jedan od brojnih naslednika sajferpankerske liste, koja je izašla iz upotrebe. Kao što je uobičajeno u ovim krugovima, Satoši nije rekao ko je ni odakle je, i niko nije pitao. Bila je važna ideja, ne osoba. Preciznim, suvoparnim jezikom Satoši je započeo razgovor smelom tvrdnjom da je rešio mnoge probleme duge potrage za svetim gralom univerzalnog novca.

„Radim na novom sistemu elektronske gotovine, koji bi potpuno radio po principu *peer-to-peer**, bez oslanjanja na treću stranku", počinjao je imejl.

Iz devet strana dugog PDF dokumenta[17] u prilogu imejla jasno se videlo da je Satoši vrlo dobro upoznat sa svim prethodnim pokušajima da se stvori samoodrživ digitalni novac. Satoši je u svom radu citirao Baka i Veja Deja, kao i nekoliko manje poznatih časopisa o kriptografiji. Ipak, Satoši je iskombinovao sve ove ranije izume i stvorio je sistem različit od svih prethodnih.

Umesto da se oslanja na centralnu banku ili kompaniju koja će izdavati novac i pratiti njegovo korišćenje – kao što je slučaj s postojećim finansijskim sistemom i Čomovim digikešom – ovaj sistem bio je zamišljen tako da o svakoj bitkoinskoj transakciji i imovini svakog korisnika evidenciju vode računari svih korisnika digitalnog novca, u zajedničkoj bazi podataka koja će postati poznata pod nazivom blok-lanac.

Ovaj proces je složen; čak i stručnjacima bi trebalo više meseci da shvate kako sve to radi. Ipak, osnovni elementi

* *Peer-to-peer* mreža podrazumeva neposredno povezivanje sa računarom drugog korisnika. (Prim. prev.)

sistema mogu se otprilike skicirati, kao što je Satoši i učinio u svom radu, kasnije poznatom kao Bitkoinski izveštaj.

Kako se navodi u dotičnom radu, svaki korisnik sistema mogao bi imati jednu javnu bitkoinsku adresu ili više njih – to je nešto slično bankovnim računima – i privatni ključ za svaku adresu. Novčiće povezane sa određenom adresom mogla bi da troši samo osoba koja ima odgovarajući privatni ključ za tu adresu. Privatni ključ bio je malo drugačiji od uobičajene lozinke, koju mora da čuva neki centralni autoritet kako bi proverio unosi li korisnik tačnu lozinku. Kod bitkoina, Satoši je primenio čudo kriptografije s javnim ključem, i sada je korisnica – nazovimo je opet Alis – mogla da potvrdi transakciju i dokaže da ima privatni ključ bez potrebe da iko drugi vidi ili zna njen privatni ključ*.

Kada Alis pomoću privatnog ključa potvrdi transakciju, ona bi obavestila o ovome sve ostale kompjutere na bitkoinskoj mreži. Ovi kompjuteri bi proverili poseduje li Alis novčiće koje pokušava da potroši. Ovo bi uradili proverom u javnoj evidenciji svih bitkoinskih transakcija – svi kompjuteri na mreži imali bi primerak ove evidencije. Kada kompjuteri potvrde da se na Alisinoj adresi stvarno nalazi novac koji ona pokušava da potroši, podaci o Alisinoj transakciji bili bi upisani na spisak svih skorašnjih transakcija – takav spisak naziva se blok – u blok-lancu.

Tačna metoda kojom se blokovi dodaju u blok-lanac možda je najsloženiji deo sistema. Najjednostavnije rečeno, ovo podrazumeva neku vrstu računarske trke između svih kompjutera na mreži, po modelu koji je Adam Bak[18] osmislio za heškeš. Kompjuter koji pobedi u trci zadužen je

* Za više detalja o ovom i ostalim osnovnim elementima funkcionisanja bitkoinske mreže vidi Tehnički dodatak na strani 377.

da zabeleži najnoviji transakcioni blok u blok-lanac. Što je podjednako važno, pobednik takođe dobija svežanj novih bitkoina – pedeset bitkoina u vreme kada je mreža konačno proradila. Ovo je zaista bio jedini način da se novi bitkoini donesu na svet. Nagrada u vidu novih novčića podsticala je korisnike bitkoina da podese kompjutere za učestvovanje u zajedničkom vođenju evidencije.

Ako bi bilo sporno koji je računar dobio lutriju, prevagnula bi ona transakciona evidencija koju je već prihvatila većina kompjutera na mreži. Ako, na primer, većina računara na mreži veruje da je u prošloj trci pobedila Alis, ali nekoliko računara veruje da je pobedio Bob, većina kompjutera na mreži bi prenebregavala kompjutere koji koriste Bobovu evidenciju sve dok se ovi ne bi priključili većini. Demokratski način odlučivanja bio je važan jer je sprečavao da se nekoliko rđavih kompjutera odmetne i počne da dodeljuje sebi mnogo novih bitkoina; ovakvi prestupnici morali bi da preuzmu većinu kompjutera na mreži kako bi ovo postigli.

Po demokratskom modelu odlučivalo bi se i o izmenama u bitkoinskom softveru, instaliranom na računaru svakog korisnika. Svaki korisnik mogao bi da unese izmenu u bitkoinski softver otvorenog koda, ali izmene bi stupile na snagu tek kada većina kompjutera na mreži prihvati izmenjenu verziju softvera. Ako samo jedan kompjuter počne da koristi različitu verziju bitkoinskog softvera, ostali računari bi ga u suštini ignorisali i on više ne bi pripadao bitkoinskoj mreži.

Da ponovimo, ovako je glasilo pet osnovnih koraka korišćenja bitkoina:

- Alis započinje prenos bitkoina sa svog računa tako što potvrdi ovaj transfer privatnim ključem i pošalje informacije o transakciji ostalim korisnicima.

- Drugi korisnici mreže provere ima li na Alisinoj bitkoinskoj adresi dovoljno sredstava, a onda dodaju Alisinu transakciju na spisak skorašnjih transakcija, poznat kao blok.
- Kompjuteri se utrkuju u rešavanju problema da se vidi čiji će se spisak transakcija, to jest blok, pridodati blok-lancu.
- Kompjuter čiji je blok dodat blok-lancu dobija svežanj novih bitkoina
- Računari na mreži počinju da prave nov spisak nedavnih, još nepotvrđenih transakcija u pokušaju da osvoje sledeći svežanj bitkoina.

Ishod ovog složenog postupka bio je varljivo jednostavan, ali nikad ranije nije bio moguć; bila je to finansijska mreža koja može da stvara i premešta novac bez pomoći centralnog autoriteta. Bez banaka, bez kompanija koje se bave kreditnim karticama, bez regulatornih tela. Sistem je bio osmišljen tako da niko osim vlasnika privatnog ključa ne može trošiti ili uzimati novac sa određene bitkoinske adrese. Što je još važnije, svaki korisnik sistema mogao je biti siguran da će u svakom trenutku postojati samo jedna javna, nepromenljiva evidencija o imetku svakog člana sistema. Radi ovoga, korisnici nisu morali pokloniti poverenje Satošiju onako kako su korisnici digikeša morali da se oslone na Dejvida Čoma, ili korisnici dolara na Savezne rezerve. Morali su samo da veruju sopstvenim računarima sa instaliranim bitkoinskim softverom, i Satošijevom kodu, a to je bio otvoreni kod i stoga je svako mogao da ga pregleda. Ako se korisnicima ne bi dopadalo nešto u pravilima koja je Satošijev softver propisivao, mogli su da izmene pravila. Ljudi koji bi se priključili bitkoinskoj mreži bili su bukvalno i klijenti i vlasnici, i banke i kovnice.