Kion mi lernis falante la Bitmono-kuniklotruon

"Ho, vi malsaĝa Alicio!" ŝi diris denove, "kiel vi povas lerni lecionojn ĉi tie?
Nu, apenaŭ estas loko por vi, kaj tute ne estas loko por iuj lecionlibroj!"

La Blanka Kuniklo surmetis siajn okulvitrojn.
Kie mi komencu, bonvolu al via Moŝto? li demandis.
" Komencu de la komenco ," diris la Reĝo serioze,
"kaj daŭrigu ĝis vi venos al la fino: tiam ĉesu."

Ĉu vi pretas eniri Mirlandon?

Permesilo

Ĉi tiu libro laŭ la permesilo Krea Komunaĵo Atribuite-Samkondiĉe 4.0 Tutmonda (CC BY-SA 4.0), kio signifas, ke vi rajtas kunhavigi kaj adapti la materialon laŭplaĉe. La sola postulo estas, ke vi devas distribui viajn kontribuojn sub la sama permesilo.

Antaŭparolo

Eta Alicio falis el la truo, frapis sian kapon kaj kontuzis ŝian animon.

Fali en la Bitmono-kuniklotruon estas stranga sperto. Kiel multaj aliaj, mi sentas, ke mi lernis pli en la lastaj du jaroj studante Bitmono ol mi dum du jardekoj da formala edukado.

La sekvaj lecionoj estas distilado de tio, kion mi lernis. Unue eldonita kiel artikola serio titolita "Kion mi Lernis De Bitmono", kio sekvas povas esti vidita kiel dua eldono de la origina serio.

Kiel Bitmono, ĉi tiuj lecionoj ne estas senmova afero. Mi planas labori pri ili periode, publikigante ĝisdatigitajn versiojn kaj kroman materialon estonte.

Male al Bitmono, estontaj versioj de ĉi tiu projekto ne devas esti malantaŭen kongruaj. Iuj lecionoj povus esti plilongigitaj, aliaj povus esti reverkitaj aŭ anstataŭigitaj. Mi esperas, ke estonta versio estos io, kion vi povas teni en viaj manoj, sed mi ankoraŭ ne volas ion promesi.

Bitmono estas neelĉerpebla instruisto, tial mi ne asertas, ke ĉi tiuj lecionoj estas tute ampleksaj aŭ kompletaj. Ili estas spegulbildo de mia persona vojaĝo laŭ la kuniklotruo. Estas multaj pli da lecionoj por lerni, kaj ĉiu homo lernos ion malsaman ol eniri la mondon de Bitmono.

Mi esperas, ke vi trovos ĉi tiujn lecionojn utilaj kaj ke la procezo lerni ilin per legado ne estos tiel peniga kaj dolora kiel lerni ilin propraokula.

Gigi

"Ĉu vi dirus al mi, mi petas, kiun vojon mi devas iri de ĉi tie?"
"Tio dependas multe de kie vi volas atingi."
"Mi ne multe zorgas kien -"
"Do ne gravas kiun vojon vi iras."

Enhavtabelo

Antaŭparolo	3
Enhavtabelo	5
Enkonduko	7
Ĉapitro I: Filozofio	**9**
Leciono 1: Neŝanĝebleco kaj ŝanĝo	11
Leciono 2: La malabundeco de malabundeco	13
Leciono 3: Reproduktado kaj loko	14
Leciono 4: La problemo de identeco	16
Leciono 5: Senmakula koncepto	17
Leciono 6: La potenco de libera parolado	18
Leciono 7: La limoj de scio	19
Ĉapitro II: Ekonomio	**20**
Leciono 8: Financa nescio	22
Leciono 9: Inflacio	24
Leciono 10: Valoro	27
Leciono 11: Mono	28
Leciono 12: La historio kaj falo de mono	30
Leciono 13: Frakcia Rezerva Frenezo	35
Leciono 14: Sona mono	38
Ĉapitro III: Teknologio	**43**
Leciono 15: Forto en nombroj	45
Leciono 16: Interkonsiliĝoj pri "Ne Fidu, Kontrolu"	49
Leciono 17: Rakonti tempon postulas laboron	53
Leciono 18: Movu malrapide kaj ne rompu aferojn	55
Leciono 19: Privateco ne mortis	58
Leciono 20: Cypherpunks skribas kodon	60
Leciono 21: Metaforoj por la estonteco de bitmono	62
Konkludo	65
Rekonoj	68
Dank	69

Enkonduko

"Sed mi ne volas iri inter frenezuloj," Alicio komentis.
"Ho, vi ne povas helpi tion," diris la Kato: "ni ĉiuj estas frenezaj ĉi tie.
Mi estas freneza. Vi estas freneza."
"Kiel vi scias, ke mi estas freneza?" diris Alicio.
"Vi certe estas," diris la Kato, "alie vi ne estus veninta ĉi tien."

En oktobro 2018, Arjun Balaji demandis la senkulpan demandon, Kion vi lernis de Bitmono? Post provi respondi ĉi tiun demandon per mallonga ĉirpeto, kaj mizere malsukcesante, mi konstatis, ke la aferoj, kiujn mi lernis, estas multe tro multaj por respondi rapide, se entute.

La aferoj, kiujn mi lernis, estas, evidente, pri bitmono - aŭ almenaŭ rilataj al ĝi. Tamen, dum kelkaj el la internaj funkciadoj de bitmono estas klarigitaj, la sekvaj lecionoj ne estas klarigo pri kiel bitmono funkcias aŭ kio ĝi estas, ili tamen povus helpi esplori kelkajn el la aferoj, kiujn bitmono tuŝas: filozofiaj demandoj, ekonomiaj realaĵoj, kaj teknologiaj novigoj.

La 21 lecionoj estas strukturitaj en faskoj de sep, rezultigante tri ĉapitrojn. Ĉiu ĉapitro rigardas bitmonon per malsama lenso, ĉerpante kiajn lecionojn oni povas lerni inspektante ĉi tiun strangan reton de malsama angulo.

Ĉapitro 1 esploras la filozofiajn instruojn de bitmono. La interagado de neŝanĝebleco kaj ŝanĝo, la koncepto de vera malabundeco, la senmakula koncepto de bitmono, la problemo de identeco, la kontraŭdiro de reproduktado kaj loko, la potenco de libera sinesprimo, kaj la limoj de scio.

Ĉapitro 2 esploras la ekonomiajn instruojn de bitmono. Lecionoj pri financa nescio, inflacio, valoro, mono kaj la historio de mono, frakcia rezerva bankado, kaj kiel bitmono reenkondukas solidan monon en ruza, ĉirkaŭvojo.

Ĉapitro 3 esploras kelkajn el la lecionoj lernitaj ekzamenante la teknologion de bitmono. Kial estas forto en nombroj, pripensoj pri fido, kial rakonti tempon postulas laboron, kiel moviĝi malrapide kaj ne rompi aferojn estas trajto kaj ne cimo, kion la kreado de bitmono povas diri al ni pri privateco, kial kodo skribas

kodon (kaj ne leĝoj), kaj kiaj metaforoj povus esti utilaj por esplori la estontecon de bitmono.

Ĉiu leciono enhavas plurajn citaĵojn kaj ligilojn tra la teksto. Se mi esploris ideon pli detale, vi povas trovi ligilojn al miaj rilataj verkoj en la sekcio "Tra la Spegulo". Se vi ŝatas profundiĝi, ligiloj al la plej grava materialo estas listigitaj en la sekcio "Malsupren la Kuniklotruo". Ambaŭ troviĝas ĉe la fino de ĉiu leciono.

Kvankam iuj antaŭaj scio pri bitmono estas utila, mi esperas, ke ĉi tiuj lecionoj povas esti digestitaj de iu ajn scivolema leganto. Dum kelkaj rilatas unu al la alia, ĉiu leciono devus povi stari memstare kaj legeblas sendepende. Mi faris mian plejeblon por eviti teknikan ĵargonon, kvankam iu domajna specifa vortprovizo estas neevitebla.

Mi esperas, ke mia skribo servas kiel inspiro por aliaj fosi sub la surfaco kaj ekzameni iujn el la pli profundaj demandoj, kiujn bitmono levas. Mia propra inspiro venis de amaso da aŭtoroj kaj enhavaj kreintoj al ĉiuj el kiuj mi estas eterne dankema.

Laste sed ne malplej: mia celo skribante ĉi tion ne estas konvinki vin pri io ajn. Mia celo estas pensigi vin, kaj montri al vi, ke bitmono estas multe pli ol ŝajnas al vi. Mi eĉ ne povas diri al vi kio estas bitmono aŭ kion bitmono instruos al vi. Vi devos eltrovi tion mem.

"Post ĉi tio, ne eblas returni sin. Vi prenas la bluan pilolon — la rakonto finiĝas, vi vekiĝas en via lito kaj kredas kion ajn vi volas kredi. Vi prenu la ruĝan pilolon — vi restas en Mirlando, kaj mi montras al vi, kiom profundiĝas la kuniklotruo."

Morfeo

Ĉapitro I

Filozofio

La muso iom esplore rigardis ŝin, kaj ŝajnis al ŝi palpebrumi per unu el siaj etaj okuletoj, sed ĝi diris nenion.

Rigardante bitmonon supraĵe, oni povus konkludi, ke ĝi estas malrapida, malŝparema, nenecese superflua kaj tro paranoja. Rigardante bitmonon esplore, oni povus ekscii, ke aferoj ne estas kiel ili ŝajnas unuavide.

Bitmono havas manieron preni viajn supozojn kaj turni ilin sur siajn kapojn. Post iom da tempo, ĝuste kiam vi denove komfortiĝos, bitmono frakasos tra la muro kiel taŭro en porcelana butiko kaj frakasos viajn supozojn denove.

Bitmono estas infano de multaj disciplinoj. Kiel blindaj monaĥoj ekzamenantaj elefanton, ĉiuj, kiuj alproksimiĝas al ĉi tiu nova teknologio, faras tion de malsama angulo. Kaj ĉiuj venos al malsamaj konkludoj pri la naturo de la besto.

La sekvaj lecionoj temas pri iuj el miaj supozoj, kiujn bitmono frakasis, kaj la konkludoj, al kiuj mi alvenis. Filozofiaj demandoj de neŝanĝebleco, malabundeco, loko kaj identeco estas esploritaj en la unuaj kvar lecionoj.

Leciono 1: Neŝanĝebleco kaj ŝanĝo
Leciono 2: La malabundeco de malabundeco
Leciono 3: Reproduktado kaj loko
Leciono 4: La problemo de identeco
Leciono 5: Senmakula koncepto
Leciono 6: La potenco de libera parolado
Leciono 7: La limoj de scio

Leciono 5 esploras kiel la originrakonto de bitmono estas ne nur fascina sed absolute esenca por sengvidanto-sistemo. La lastaj du lecionoj de ĉi tiu ĉapitro esploras la potencon de libera parolado kaj la limojn de nia individua scio, reflektitaj de la surpriza profundo de la bitmono-kuniklotruo.

Mi esperas, ke vi trovos la mondon de bitmono tiel eduka, fascina kaj distra kiel mi faris kaj ankoraŭ faras. Mi invitas vin sekvi la blankan kuniklon kaj esplori la profundojn de ĉi tiu kuniklotruo. Nun tenu vian poŝhorloĝon, malleviĝu kaj ĝuu la falon.

Leciono 1

Neŝanĝebleco kaj ŝanĝo

Mi scivolas, ĉu mi estis ŝanĝita en la nokto. Lasu min pensi. Ĉu mi estis la sama, kiam mi ellitiĝis ĉi-matene? Mi preskaŭ pensas, ke mi povas memori, ke mi sentis min iom malsama. Sed se mi ne estas la sama, la sekva demando estas 'Kiu en la mondo mi estas?' Ha, jen la granda enigmo!

Bitmono estas esence malfacile priskribi. Ĝi estas nova afero, kaj ĉiu provo fari komparon al antaŭaj konceptoj - ĉu nomante ĝin cifereca oro aŭ la interreto de mono - nepre mankos al la tuto. Kia ajn estu via plej ŝatata analogio, du aspektoj de bitmono estas absolute esencaj: malcentralizo kaj neŝanĝebleco.

Unu maniero pensi pri Bitmono estas kiel aŭtomatigita socia kontrakto. La programaro estas nur unu peco de la enigmo, kaj esperi ŝanĝi Bitmonon ŝanĝante la programaron estas ekzerco en vano. Oni devus konvinki la reston de la reto adopti la ŝanĝojn, kio estas pli psikologia penado ol programaro-inĝenierado.

La sekvanta povus soni absurda komence, kiel tiom da aliaj aferoj en ĉi tiu spaco, sed mi kredas, ke ĝi tamen estas profunde vera: Vi ne ŝanĝos Bitmonon, sed Bitmono ŝanĝos vin.

"Bitmono ŝanĝos nin pli ol ni ŝanĝos ĝin."
Marty Bent

Mi bezonis longan tempon por kompreni la profundecon de ĉi tio. Ĉar Bitmono estas nur programaro kaj ĉio el ĝi estas malfermfonta, vi povas simple ŝanĝi aferojn laŭplaĉe, ĉu ne? Malĝuste. Tre malĝuste. Ne surprize, la kreinto de Bitmono sciis ĉi tion tro bone.

"La naturo de Bitmono estas tia, ke post kiam versio 0.1 estis publikigita, la kerndezajno estis fiksita en ŝtono por la resto de sia vivdaŭro."
Satoshi Nakamoto

Multaj homoj provis ŝanĝi la naturon de Bitmono. Ĝis nun ĉiuj malsukcesis. Dum estas senfina maro de forkoj kaj altkoinoj, la reto Bitmono ankoraŭ faras

sian aferon, same kiel ĝi faris kiam la unua nodo enretiĝis. La altkoins ne gravas longtempe. La forkoj fine mortos de malsato. Bitmono estas kio gravas. Dum nia fundamenta kompreno pri matematiko kaj/aŭ fiziko ne ŝanĝiĝos, la Bitmono honeybadger daŭre ne zorgos.

"Bitmono estas la unua ekzemplo de nova formo de vivo. Ĝi vivas kaj spiras en la interreto. Ĝi vivas ĉar ĝi povas pagi homojn por konservi ĝin vivanta. […] Ĝi ne povas esti ŝanĝita. Ĝi ne povas esti argumentita. Ĝi ne povas esti mistraktata. Ĝi ne povas esti koruptita. Ĝi ne povas esti haltigita. […] Se la nuklea milito detruus duonon de nia planedo, ĝi daŭre vivus, senkorupta. "
Ralph Merkle

La korbato de la Bitmono-reto daŭros super ĉiuj niaj.

Rimarki la supre ŝanĝis min multe pli ol la pasintaj blokoj de la Bitmono-blokĉeno iam faros. Ĝi ŝanĝis mian temppreferon, mian komprenon pri ekonomio, miajn politikajn opiniojn, kaj multe pli. Diablo, ĝi eĉ ŝanĝas la dietojn de homoj. Se ĉio ĉi sonas freneza al vi, vi estas en bona kompanio. Ĉio ĉi estas freneza, kaj tamen ĝi okazas.

Bitmono instruis al mi, ke ĝi ne ŝanĝos. Mi ŝanĝos.

Leciono 2

La malabundeco de malabundeco

Tio sufiĉas — mi esperas, ke mi ne plu kreskos...

Ĝenerale, la antaŭeniĝo de teknologio ŝajnas fari aferojn pli abundaj. Pli kaj pli da homoj povas ĝui tion, kio antaŭe estis luksaj varoj. Baldaŭ, ni ĉiuj vivos kiel reĝoj. Plej multaj el ni jam faras. Kiel Peter Diamandis skribis en Abundeco: "Teknologio estas rimedo-liberiga mekanismo. Ĝi povas fari la iam malabundan la nun abundan."

Bitmono, altnivela teknologio en si mem, rompas ĉi tiun tendencon kaj kreas novan varon, kiu estas vere malabunda. Iuj eĉ argumentas, ke ĝi estas unu el la plej malabundaj aferoj en la universo. La provizo ne povas esti ŝveligita, negrave kiom da penado oni elektas elspezi por krei pli.

"Nur du aferoj estas vere malabundaj: tempo kaj Bitmono."
Saifedean Ammous

Paradokse, ĝi faras tion per mekanismo de kopiado. Transakcioj estas elsenditaj, blokoj estas disvastigitaj, la distribuita ĉeflibro estas - nu, vi divenis - distribuita. Ĉio ĉi estas nur luksaj vortoj por kopii. Diablo, Bitmono eĉ kopias sin sur tiom da komputiloj kiel ĝi povas, instigante individuajn homojn prizorgi plenajn nodojn kaj minigi novajn blokojn.

Ĉio ĉi tiu duobligo mirinde funkcias kune en kunordigita klopodo produkti malabundecon.

En tempo de abundo, Bitmono instruis al mi, kio estas vera malabundeco.

Leciono 3

Reproduktado kaj loko

Poste aŭdiĝis kolera voĉo—tiu de la kuniklo—" Pat, Pat! kie vi estas?"

Kvantuma mekaniko flankenmetite, loko estas ne-afero en la fizika mondo. La demando "Kie estas X?" povas esti respondita en signifoplena maniero, negrave ĉu X estas persono aŭ objekto. En la cifereca mondo, la demando pri kie jam estas malfacila, sed ne neebla respondi. Kie estas viaj retpoŝtoj, vere? Malbona respondo estus "la nubo", kiu estas nur la komputilo de iu alia. Tamen, se vi volus elspuri ĉiun stokan aparaton, kiu havas viajn retpoŝtojn sur ĝi, vi povus, teorie, lokalizi ilin.

Kun Bitmono, la demando pri "kie" estas vere malfacila. Kie, ĝuste, estas viaj bitmonoj?

"Mi malfermis miajn okulojn, ĉirkaŭrigardis, kaj demandis la neeviteblan, la tradician, la bedaŭrinde manitan postoperacian demandon: 'Kie mi estas?'"
Daniel Dennett

La problemo estas duobla: Unue, la distribuita ĉeflibro estas distribuita per plena reproduktado, signifante ke la ĉeflibro estas ĉie. Due, ne ekzistas bitmonoj. Ne nur fizike, sed teknike.

Bitmono kontrolas aron de neeluzitaj transakciaj eliroj, sen iam devi rilati al ento kiu reprezentas Bitmono. La ekzisto de Bitmono estas konkludita rigardante la aron de neeluzitaj transakciaj eliroj kaj nomante ĉiun eniron kun 100 milionoj da bazaj unuoj Bitmono.

"Kie ĝi estas, en ĉi tiu momento, en trafiko? […] Unue, ne estas bitmonoj. Nur ne estas. Ili ne ekzistas. Estas ĉeflibroj enskriboj en ĉeflibro kiu estas dividita […] Ili ne ekzistas en ajna fizika loko. La ĉeflibro ekzistas en ĉiu fizika loko, esence. Geografio ne havas sencon ĉi tie - ĝi ne helpos vin eltrovi vian politikon ĉi tie."
Peter Van Valkenburgh

Do, kion vi efektive posedas kiam vi diras "Mi havas bitmonon" se ne ekzistas bitmonoj? Nu, ĉu vi memoras ĉiujn ĉi tiujn strangajn vortojn, kiujn vi estis

devigita skribi per la monujo, kiun vi uzis? Montriĝas, ke ĉi tiuj magiaj vortoj estas tio, kion vi posedas: magia sorĉo, kiu povas esti uzata por aldoni iujn enskribojn al la publika ĉeflibro - la ŝlosiloj por "movi" iujn bitmonojn. Jen kial, por ĉiuj celoj, viaj privataj ŝlosiloj estas viaj bitmonoj. Se vi pensas, ke mi faras ĉion ĉi, bonvolu sendi al mi viajn privatajn ŝlosilojn.

Bitmono instruis al mi, ke loko estas malfacila komerco.

Leciono 4

La problemo de identeco

"Kiu vi estas?" diris la raŭpo.

Nic Carter, en omaĝo al la traktado de Thomas Nagel de la sama demando rilate al vesperto, skribis bonegan pecon, kiu diskutas la sekvan demandon: Kiel ĝi estas esti Bitmono? Li brile montras, ke malfermaj, publikaj blokĉenoj ĝenerale, kaj Bitmono aparte, suferas de la sama enigmo kiel la Ŝipo de Tezeo : kiu Bitmono estas la vera Bitmono?

"Konsideru kiom malmulte da persisto havas la komponantoj de Bitmono. La tuta kodbazo estis reverkita, ŝanĝita kaj vastigita tiel ke ĝi apenaŭ similas sian originalan version. […] La registro de kiu posedas kion, la ĉeflibro mem, estas preskaŭ la sola persista trajto de la reto […]

Por esti konsiderata vere sengvidanto, vi devas cedi la facilan solvon havi enton, kiu povas indiki unu ĉenon kiel la legitiman."
Nic Carter

Ŝajnas, ke la progreso de teknologio daŭre devigas nin preni ĉi tiujn filozofiajn demandojn serioze. Pli aŭ malpli frue, memveturantaj aŭtoj alfrontos realajn versiojn de la troleoproblemo, devigante ilin fari etikajn decidojn pri kies vivoj gravas kaj kies ne gravas.

Kriptaj moneroj, precipe ekde la unua disputiga malmola forko, devigas nin pensi kaj konsenti pri la metafiziko de identeco. Interese, la du plej grandaj ekzemploj, kiujn ni havas ĝis nun, kondukis al du malsamaj respondoj. La 1-an de aŭgusto 2017, Bitmono dividiĝis en du tendarojn. La merkato decidis, ke la senŝanĝa ĉeno estas la originala Bitmono. Unu jaron pli frue, la 25-an de oktobro 2016, Ethereum dividiĝis en du tendarojn. La merkato decidis, ke la ŝanĝita ĉeno estas la origina Ethereum.

Se ĝuste malcentralizitaj, la demandoj starigitaj de la Ŝipo de Tezeo devos esti responditaj eterne dum ĉi tiuj retoj de valortransigo ekzistas.

Bitmono instruis al mi, ke malcentralizo kontraŭdiras identecon.

Leciono 5

Senmakula koncepto

"Iliaj kapoj malaperis," la soldatoj kriis responde...

Ĉiuj amas bonan originrakonton. La originrakonto de Bitmono estas fascina, kaj la detaloj de ĝi estas pli gravaj ol oni povus pensi komence. Kiu estas Satoshi Nakamoto? Ĉu li estis unu homo aŭ grupo de homoj? Ĉu li estis ŝi? Tempo-vojaĝanta eksterterano, aŭ altnivela AI? Eksterordinaraj teorioj flankenmetitе, ni verŝajne neniam scios. Kaj ĉi tio estas grava.

Satoshi elektis esti anonima. Li plantis la semon de Bitmono. Li restis sufiĉe longe por certigi, ke la reto ne mortos en sia infanaĝo. Kaj tiam li malaperis.

Kio povus aspekti kiel stranga anonima riskagaĵo estas fakte decida por vere malcentralizita sistemo. Neniu centralizita kontrolo. Neniu centralizita aŭtoritato. Neniu inventinto. Neniu por procesi, torturi, ĉantaĝi aŭ eldevigi. Senmakula koncepto de teknologio.

"Unu el la plej grandaj aferoj, kiujn faris Satoshi, estis malaperi."
Jimmy Kanto

Ekde la naskiĝo de Bitmono, miloj da aliaj kriptaj moneroj estis kreitaj. Neniu el ĉi tiuj klonoj dividas ĝian originrakonton. Se vi volas anstataŭi Bitmono, vi devos transcendi ĝian originrakonton. En milito de ideoj, rakontoj diktas supervivon.

"Oro unue estis formita en juvelaĵon kaj uzita por interŝanĝo antaŭ pli ol 7,000 jaroj. La alloga brilo de oro kondukis al ĝi esti konsiderata donaco de la dioj."

Kiel oro en antikvaj tempoj, Bitmono povus esti konsiderata donaco de la dioj. Male al oro, la originoj de bitmonoj estas tro homaj. Kaj ĉi-foje, ni scias, kiuj estas la dioj de evoluo kaj bontenado: homoj en la tuta mondo, anonimaj aŭ ne. Bitmono instruis al mi, ke rakontoj estas gravaj.

Leciono 6

La potenco de libera sinesprimo

"Pardonu min?" diris la muso sulkigante la brovojn, sed tre ĝentile, "ĉu vi parolis?"

Bitmono estas ideo. Ideo kiu, en sia nuna formo, estas la manifestiĝo de maŝinaro pure funkciigita de teksto. Ĉiu aspekto de Bitmono estas teksto: La blankpapero estas teksto. La programaro, kiu funkcias per siaj nodoj, estas teksto. La ĉeflibro estas teksto. Transakcioj estas teksto. Publikaj kaj privataj ŝlosiloj estas teksto. Ĉiu aspekto de Bitmono estas teksto, kaj tiel ekvivalenta al parolado.

"La Kongreso faros neniun leĝon koncerne starigon de religio, aŭ malpermesante la liberan ekzercon de ĝi; aŭ mallongigante la sinesprimliberecon, aŭ de gazetaro; aŭ la rajton de homoj pace kunveni, kaj peti la Registaron pri kompenso de plendoj."
Unua Amendo al la Usona Konstitucio

Kvankam la fina batalo de la Kriptaj Militoj ankoraŭ ne estis batalita, estos tre malfacile krimigi ideon, des malpli ideon, kiu baziĝas sur interŝanĝo de tekstmesaĝoj. Ĉiufoje kiam registaro provas malpermesi tekston aŭ paroladon, ni deglitas laŭ vojo de absurdaĵo, kiu neeviteble kondukas al abomenaĵoj kiel kontraŭleĝaj nombroj kaj kontraŭleĝaj primoj.

Tiel longe kiel ekzistas parto de la mondo kie parolado estas libera kiel en libereco, Bitmono estas nehaltigebla.

"Ne estas signifo en iu Bitmono-transakcio, ke Bitmono ĉesas esti teksto. Ĉio estas teksto, ĉiam . […]

Bitmono estas teksto. Bitmono estas parolado. Ĝi ne povas esti reguligita en libera lando kiel Usono kun garantiitaj neforigeblaj rajtoj kaj Unua Amendo kiu eksplicite ekskludas la agon de eldonado de registara superrigardo."
Beautyon

Bitmono instruis al mi, ke en libera socio, libera parolado kaj libera programaro estas nehaltigeblaj.

Leciono 7

La limoj de scio

Down, down, down. Ĉu la falo neniam finiĝos?

Eniri Bitmono estas humiliga sperto. Mi pensis, ke mi scias aferojn. Mi pensis, ke mi estas edukita. Mi pensis ke mi konas mian komputikon, almenaŭ. Mi studis ĝin dum jaroj, do mi devas scii ĉion pri ciferecaj subskriboj, haŝiŝoj, ĉifrado, funkcia sekureco kaj retoj, ĉu ne?

Malĝuste.

Lerni ĉiujn bazaĵojn, kiuj igas Bitmono funkcii, estas malfacile. Kompreni ĉiujn el ili profunde estas limo neebla.

"Neniu trovis la fundon de la Bitmono-kuniklotruo."
Jameson Lopp

Mia listo de legindaj libroj daŭre vastiĝas multe pli rapide ol mi eble povus legi ilin. La listo de artikoloj kaj artikoloj por legi estas preskaŭ senfina. Estas pli da podkastoj pri ĉiuj ĉi tiuj temoj ol mi iam povus aŭskulti. Ĝi vere estas humiliga. Plue, Bitmono evoluas kaj estas preskaŭ neeble resti ĝisdatigita kun la akcela indico de novigado. La polvo de la unua tavolo ankoraŭ ne ekloĝis, kaj homoj jam konstruis la duan tavolon kaj laboras pri la tria.

Bitmono instruis al mi, ke mi scias tre malmulte pri preskaŭ io ajn. Ĝi instruis al mi, ke ĉi tiu kuniklotruo estas senfunda.

Ĉapitro II

Ekonomiko

Granda rozarbo staris proksime de la enirejo de la ĝardeno: la rozoj sur ĝi estis blankaj, sed estis tri ĝardenistoj ĉe ĝi, okupante pentrante ilin ruĝaj. Ĉi tiu Alico pensis tre kuriozan aferon...

Mono ne kreskas sur arboj. Kredi ke ĝi faras estas malsaĝe, kaj niaj gepatroj certigas, ke ni scias pri tio, ripetante ĉi tiun diron kiel mantro. Ni estas kuraĝigitaj uzi monon saĝe, ne elspezi ĝin frivole, kaj ŝpari ĝin en bonaj tempoj por helpi nin tra la malbonaj. Mono ja ne kreskas sur arboj.

Bitmono instruis min pli pri mono ol mi iam ajn pensis, ke mi bezonus scii. Per ĝi, mi estis devigita esplori la historion de mono, bankado, diversaj lernejoj de ekonomia penso kaj multajn aliajn aferojn. La serĉo por kompreni Bitmonon kondukas min laŭ multego da vojoj, kelkajn el kiuj mi provas esplori en ĉi tiu serio.

En la unuaj sep lecionoj iuj el la filozofiaj demandoj, kiujn Bitmono tuŝas, estis diskutitaj. La venontaj sep lecionoj pli detale rigardos monon kaj ekonomion.

Leciono 8: Financa nescio
Leciono 9: Inflacio
Leciono 10: Valoro
Leciono 11: Mono
Leciono 12: La historio kaj falo de mono
Leciono 13: Frakcia Rezerva Frenezo
Leciono 14: Sona mono

Denove, mi nur povos grati la surfacon. Bitmono estas ne nur ambicia, sed ankaŭ larĝa kaj profunda amplekso, ebligante kovri ĉiujn rilatajn temojn en ununura leciono, eseo, artikolo aŭ libro. Mi dubas, ĉu ĝi eĉ entute eblas.

Bitmono estas nova formo de mono, kiu faras lerni pri ekonomio plej grava por kompreni ĝin. Pritraktante la naturon de homa ago kaj la interagojn de ekonomiaj agentoj, ekonomio verŝajne estas unu el la plej grandaj kaj malklaraj pecoj de la Bitmono-enigmo.

Denove, ĉi tiuj lecionoj estas esplorado de la diversaj aferoj, kiujn mi lernis de Bitmono. Ili estas persona reflekto de mia vojaĝo laŭ la kuniklotruo. Havante neniun fonon pri ekonomio, mi certe estas ekster mia komforta zono kaj precipe konscias, ke ajna kompreno, kiun mi povus havi, estas nekompleta. Mi faros mian plejeblon por skizi tion, kion mi lernis, eĉ kun la risko de stulti min. Post ĉio, mi ankoraŭ provas respondi la demandon: "Kion vi lernis de Bitmono?"

Post sep lecionoj ekzamenitaj tra la lenso de filozofio, ni uzu la lenson de ekonomio por rigardi sep pliajn. Ekonomia klaso estas ĉio, kion mi povas proponi ĉi-foje. Fina celo: solida mono.

Leciono 8

Financa nescio

Kaj kia malklera knabineto ŝi pensos, ke mi demandas! Ne, neniam konvenos demandi: eble mi vidos ĝin skribita ie.

Unu el la plej surprizaj aferoj, al mi, estis la kvanto de financo, ekonomio kaj psikologio necesa por ekkompreni kio unuavide ŝajnas esti pure teknika sistemo - komputila reto. Por parafrazi ulo kun harplenaj piedoj: "Estas danĝera komerco, Frodo, enpaŝi Bitmono. Vi legas la blankpaperon, kaj se vi ne tenas viajn piedojn, oni ne povas scii kien vi povus esti forbalaita."

Por kompreni novan monsistemon, vi devas konatiĝi kun la malnova. Mi ekkomprenis tre baldaŭ, ke la kvanto de financa edukado, kiun mi ĝuis en la eduka sistemo, estas esence nula.

Kiel kvinjarulo, mi komencis demandi al mi multajn demandojn: Kiel funkcias la banka sistemo? Kiel funkcias la borso? Kio estas fiatmono? Kio estas regula mono? Kial estas tiom da ŝuldo? Kiom da mono estas efektive presita, kaj kiu decidas tion?

Post milda paniko pri la pura amplekso de mia nescio, mi trovis trankvilon konsciante, ke mi estas en bona kompanio.

"Ĉu ne estas ironie, ke Bitmono instruis min pli pri mono ol ĉiuj ĉi tiuj jaroj, kiujn mi pasigis laborante por financaj institucioj? ...inkluzive komenci mian karieron ĉe centra banko"
Aarontaycc

"Mi lernis pli pri financo, ekonomio, teknologio, kriptografio, homa psikologio, politiko, ludoteorio, leĝaro, kaj mi mem en la lastaj tri monatoj de kripto ol la lastaj tri jaroj kaj duono de kolegio"
Bitcoindunny

Ĉi tiuj estas nur du el la multaj konfesoj tra la tuta tvitero. Bitmono, kiel estis esplorita en Leciono 1, estas vivanto. Mises argumentis ke ekonomiko ankaŭ

estas vivanta aĵo. Kaj kiel ni ĉiuj scias el persona sperto, vivaĵoj estas esence malfacile kompreneblaj.

"Scienca sistemo estas nur unu stacio en senfine progresanta serĉado de scio. Ĝin nepre tuŝas la nesufiĉo propra al ĉiu homa penado. Sed agnoski tiujn faktojn ne signifas, ke la nuna ekonomio estas postiĝinta. Ĝi nur signifas, ke ekonomio estas vivanto - kaj vivi implicas kaj neperfektecon kaj ŝanĝon."
Ludwig von Mises

Ni ĉiuj legas pri diversaj financaj krizoj en la novaĵoj, scivolas pri kiel funkcias ĉi tiuj grandaj savadoj kaj estas konfuzitaj pri la fakto, ke neniu neniam ŝajnas respondeci pri damaĝoj, kiuj estas en bilionoj. Mi ankoraŭ estas konfuzita, sed almenaŭ mi komencas ekvidi, kio okazas en la mondo de financo.

Kelkaj homoj eĉ iras ĝis atribui la ĝeneralan nescion pri tiuj temoj al sistema, intenca nescio. Dum historio, fiziko, biologio, matematiko kaj lingvoj estas ĉiuj parto de nia edukado, la mondo de mono kaj financo surprize estas nur supraĵe esplorita, se entute. Mi scivolas, ĉu homoj ankoraŭ volonte akirus tiom da ŝuldo kiom ili nuntempe faras, se ĉiuj estus edukitaj pri persona financo kaj la funkciado de mono kaj ŝuldo. Tiam mi scivolas, kiom da tavoloj de aluminio faras efikan stanfolion ĉapelon. Verŝajne tri.

"Tiuj kraŝoj, ĉi tiuj savadoj, ne estas akcidentoj. Kaj ankaŭ ne estas hazardo, ke ne ekzistas financa edukado en la lernejo. […] Estas premeditita. Same kiel antaŭ la Civita milito estis kontraŭleĝe eduki sklavon, ni ne rajtas lerni pri mono en la lernejo."
Robert Kiyosaki

Kiel en La Sorĉisto de Oz, oni diras al ni ne atenti la viron malantaŭ la kurteno. Male al La Sorĉisto de Oz, ni nun havas veran sorĉadon: cenzurrezista, malfermita, senlima reto de valortransigo. Ne estas kurteno, kaj la magio estas videbla por iu ajn.
Bitmono instruis min rigardi malantaŭ la kurteno kaj alfronti mian financan nescion.

Leciono 9

Inflacio

Kara, ĉi tie ni devas kuri kiel eble plej rapide, nur por resti surloke. Kaj se vi volas iri ien, vi devas kuri duoble pli rapide ol tio.

Provi kompreni monan inflacion, kaj kiel ne-inflacia sistemo kiel Bitmono povus ŝanĝi kiel ni faras aferojn, estis la deirpunkto de mia entrepreno en ekonomikon. Mi sciis, ke inflacio estas la rapideco je kiu kreiĝas nova mono, sed mi ne sciis tro multe pli ol tio.

Dum iuj ekonomikistoj argumentas, ke inflacio estas bona afero, aliaj argumentas, ke "malmola" mono, kiu ne povas esti ŝveligita facile - kiel ni havis en la tempo de la ora normo - estas esenca por sana ekonomio. Bitmono, havanta fiksan provizon de 21 milionoj, konsentas kun ĉi-lasta tendaro.

Kutime, la efikoj de inflacio ne estas tuj evidentaj. Depende de la inflacia indico (same kiel aliaj faktoroj) la tempo inter kaŭzo kaj efiko povas esti pluraj jaroj. Ne nur tio, sed inflacio influas malsamajn grupojn de homoj pli ol aliaj. Kiel Henry Hazlitt notas en Economics in One Lesson: “La arto de ekonomiko konsistas en rigardi ne nur la tujan sed la pli longajn efikojn de iu ago aŭ politiko; ĝi konsistas en spuri la sekvojn de tiu politiko ne nur por unu grupo sed por ĉiuj grupoj."

Unu el miaj personaj ampolaj momentoj estis la konstato, ke eldonado de nova valuto — presi pli da mono — estas tute malsama ekonomia aktiveco ol ĉiuj aliaj ekonomiaj agadoj. Dum realaj varoj kaj realaj servoj produktas realan valoron por realaj homoj, presi monon efektive faras la malon: ĝi forprenas valoron de ĉiuj, kiuj tenas la valuton, kiu estas ŝveligita.

"Nura inflacio - tio estas, la nura elsendo de pli da mono, kun la sekvo de pli altaj salajroj kaj prezoj - povas aspekti kiel la kreado de pli da postulo. Sed laŭ la fakta produktado kaj interŝanĝo de realaj aferoj ne estas."
Henry Hazlitt

La detrua forto de inflacio evidentiĝas tuj kiam iom da inflacio fariĝas multe. Se mono hiperŝveliĝas, aferoj malbeliĝas vere rapide. Dum la ŝveliga valuto

disfalos, ĝi malsukcesos stoki valoron kun la tempo kaj homoj rapidos akiri siajn manojn sur ajnajn varojn, kiuj povus fari.

Alia konsekvenco de hiperinflacio estas, ke la tuta mono, kiun homoj ŝparis dum sia vivo, efektive malaperos. La papera mono en via monujo ankoraŭ estos tie, kompreneble. Sed estos ĝuste tio: senvalora papero.

Mono malpliiĝas en valoro kun tiel nomata "milda" inflacio ankaŭ. Okazas sufiĉe malrapide, ke la plej multaj homoj ne rimarkas la malpliiĝon de sia aĉetpovo. Kaj post kiam la presiloj funkcias, monero povas esti facile ŝveligita, kaj tio, kio antaŭe estis milda inflacio, povus iĝi forta taso da inflacio per la premo de butono. Kiel Friedrich Hayek indikis en unu el siaj eseoj, milda inflacio kutime kondukas al rekta inflacio.

""Milda" konstanta inflacio ne povas helpi,
Ĝi povas konduki nur al rekta inflacio."
Friedrich Hayek

Inflacio estas precipe ruza ĉar ĝi favoras tiujn, kiuj estas pli proksimaj al la presiloj. Necesas tempo por ke la nove kreita mono cirkuli kaj prezoj alĝustigi, do se vi kapablas akiri pli da mono antaŭ ol ĉiuj aliaj malplivaloriĝas, vi estas antaŭ la inflacia kurbo. Tial ankaŭ inflacio povas esti vidita kiel kaŝita imposto ĉar finfine registaroj profitas el ĝi dum ĉiuj aliaj finas pagi la prezon.

"Mi ne pensas, ke estas troigo diri, ke historio estas plejparte historio de inflacio, kaj kutime de inflacioj kreitaj de registaroj por la gajno de registaroj."
Friedrich Hayek

Ĝis nun, ĉiuj registaraj valutoj poste estis anstataŭigitaj aŭ tute kolapsis. Kiom ajn malgranda estas la inflacio, "konstanta" kresko estas nur alia maniero diri eksponenta kresko. En naturo kiel en ekonomio, ĉiuj sistemoj kiuj kreskas eksponente devos eventuale ebenigi aŭ suferi de katastrofa kolapso.

"Ĝi ne povas okazi en mia lando," estas kion vi verŝajne pensas. Vi ne pensas tion se vi estas el Venezuelo, kiu nuntempe suferas de hiperinflacio. Kun inflacia indico de pli ol 1 miliono procento, mono estas esence senvalora.

Ĝi eble ne okazos en la venontaj du jaroj, aŭ al la aparta valuto uzata en via lando. Sed rigardo al la listo de historiaj valutoj montras, ke ĝi neeviteble okazos dum sufiĉe longa tempo. Mi memoras kaj uzis multe da tiuj listigitaj: la aŭstra skilingo, la germana marko, la itala liro, la franca franko, la irlanda funto, la kroata dinaro, ktp. Mia avino eĉ uzis la aŭstro-hungaran kronon. Dum la tempo pasas, la moneroj nuntempe uzataj malrapide sed certe moviĝos al siaj respektivaj tombejoj. Ili hipersŭeliĝos aŭ estos anstataŭigitaj. Ili baldaŭ estos historiaj valutoj. Ni faros ilin malnoviĝintaj.

"Historio montris, ke registaroj neeviteble venkiĝos al la tento ŝveligi la monprovizon."
Saifedean Ammous

Kial Bitmono estas malsama? Kontraste al valutoj postulitaj fare de la registaro, monaj varoj kiuj ne estas reguligitaj fare de registaroj, sed de la leĝoj de fiziko, tendencas pluvivi kaj eĉ teni sian respektivan valoron dum tempo. La plej bona ekzemplo de tio ĝis nun estas oro, kiu, kiel la taŭge nomita Oro-al-Deca-Kostumo Proporcio, tenas sian valoron dum centoj kaj eĉ miloj da jaroj. Ĝi eble ne estas perfekte "stabila" - dubinda koncepto en la unua loko - sed la valoro, kiun ĝi tenas, almenaŭ estos en la sama grandordo.

Se mona bono aŭ valuto bone tenas sian valoron dum tempo kaj spaco, ĝi estas konsiderata malfacila. Se ĝi ne povas teni sian valoron, ĉar ĝi facile plimalboniĝas aŭ ŝveliĝas, ĝi estas konsiderata mola valuto. La koncepto de malmoleco estas esenca por kompreni Bitmonon kaj estas inda je pli profunda ekzameno. Ni revenos al ĝi en la lasta ekonomia leciono: solida mono.

Ĉar pli kaj pli da landoj suferas de hiperinflacio, pli kaj pli da homoj devos alfronti la realon de malmola kaj mola mono. Se ni bonŝancas, eble eĉ iuj centraj bankistoj estos devigitaj retaksi siajn monajn politikojn. Kio ajn povus okazi, la komprenoj, kiujn mi akiris danke al Bitmono, verŝajne estos valoregaj, negrave la rezulto.

Bitmono instruis min pri la kaŝita imposto de inflacio kaj la katastrofo de hiperinflacio.

Leciono 10

Valoro

Ĝi estis la blanka kuniklo, denove trotante malrapide reen, kaj maltrankvile rigardante ĉirkaŭ ĝi dum ĝi iris, kvazaŭ ĝi perdis ion...

Valoro estas iom paradoksa, kaj ekzistas multoblaj teorioj kiuj provas klarigi kial ni taksas certajn aferojn super aliaj. Homoj konscias pri ĉi tiu paradokso jam de miloj da jaroj. Kiel skribis Platono en sia dialogo kun Eŭtidemo, ni aprezas kelkajn aferojn ĉar ili estas maloftaj, kaj ne simple bazitaj sur sia neceso por nia supervivo.

"Kaj se vi estas prudenta, vi donos ĉi tiun saman konsilon ankaŭ al viaj lernantoj — ke ili neniam konversaciu kun iu ajn krom vi kaj unu la alian. Ĉar estas la malofta, Eŭtidemo, kiu estas altvalora, dum akvo estas plej malmultekosta, kvankam plej bona, kiel diris Pindaro."
Platono

Ĉi tiu paradokso de valoro montras ion interesan pri ni homoj: ni ŝajnas taksi aferojn sur subjektiva bazo, sed faras tion kun certaj ne-arbitraj kriterioj. Io povus esti altvalora por ni pro diversaj kialoj, sed aferoj, kiujn ni aprezas, havas certajn trajtojn. Se ni povas kopii ion tre facile, aŭ se ĝi estas nature abunda, ni ne taksas ĝin.

Ŝajnas, ke ni taksas ion ĉar ĝi estas malabunda (oro, diamantoj, tempo), malfacila aŭ laborintensa por produkti, ne estas anstataŭigebla (malnova foto de amato), utilas tiel, ke ĝi ebligas nin fari aferojn, kiujn ni alie ne povus, aŭ kombinaĵon de tiuj, kiel grandajn artaĵojn.

Bitmono estas ĉio ĉi-supra: ĝi estas ege malofta (21 milionoj), ĉiam pli malfacile produktebla (rekompenco duoniĝo), ne povas esti anstataŭigita (perdita privata ŝlosilo estas perdita por ĉiam), kaj ebligas al ni fari kelkajn sufiĉe utilajn aferojn. Ĝi estas verŝajne la plej bona ilo por valortransigo trans limoj, preskaŭ imuna al cenzuro kaj konfisko en la procezo, kaj plie, ĝi estas mem-suverena butiko de valoro, permesante al individuoj stoki sian riĉaĵon sendepende de bankoj kaj registaroj, nur por nomi du.
Bitmono instruis al mi, ke valoro estas subjektiva sed ne arbitra.

Leciono 11

Mono

"En mia juneco," diris la saĝulo, dum li skuis siajn grizajn buklojn,
"mi konservis ĉiujn miajn membrojn tre flekseblaj,
Per la uzo de ĉi tiu ungvento,
kvin ŝilingoj la skatolo— Permesu al mi vendi al vi paro."

Kio estas mono? Ni uzas ĝin ĉiutage, tamen ĉi tiu demando estas surprize malfacile respondebla. Ni dependas de ĝi en manieroj grandaj kaj malgrandaj, kaj se ni havas tro malmulte da ĝi niaj vivoj fariĝas tre malfacilaj. Tamen, ni malofte pensas pri la afero, kiu supozeble ĉirkaŭigas la mondon. Bitmono devigis min respondi ĉi tiun demandon denove kaj denove: Kio diable estas mono?

En nia "moderna" mondo, plej multaj homoj verŝajne pensos pri paperpecoj kiam ili parolas pri mono, kvankam la plej granda parto de nia mono estas nur nombro en bankkonto. Ni jam uzas nulojn kaj unojn kiel nian monon, do kiel estas Bitmono malsama? Bitmono estas malsama ĉar ĉe ĝia kerno ĝi estas tre malsama tipo de mono ol la mono, kiun ni nuntempe uzas. Por kompreni ĉi tion, ni devos pli detale rigardi kio estas mono, kiel ĝi fariĝis, kaj kial oro kaj arĝento estis uzataj dum la plej granda parto de komerca historio.

"En ĉi tiu senco, ĝi estas pli tipa por valormetalo. Anstataŭ la provizo ŝanĝiĝas por konservi la valoron la sama, la provizo estas antaŭdeterminita kaj la valoro ŝanĝiĝas."
Satoshi Nakamoto

Konkoj, oro, arĝento, papero, Bitmono. Finfine, mono estas ĉio, kion homoj uzas kiel monon, negrave ĝia formo kaj formo, aŭ manko de tio.

Mono, kiel invento, estas sprita. Mondo sen mono estas freneze komplika: Kiom da fiŝoj aĉetos al mi novajn ŝuojn? Kiom da bovinoj aĉetos al mi domon? Kio se mi nun bezonas nenion sed mi devas forigi miajn baldaŭ putrajn pomojn? Vi ne bezonas multe da imago por rimarki, ke interŝanĝo-ekonomio estas freneze malefika.

La bonega afero pri mono estas, ke ĝi povas esti interŝanĝita kontraŭ io ajn alia — tio estas tute la invento! Kiel Nick Szabo brile resumas en Shelling Out: The Origins of Money, ni homoj uzis ĉiajn aĵojn kiel monon: bidoj faritaj el maloftaj materialoj kiel eburo, konkoj aŭ specialaj ostoj, diversaj specoj de juvelaĵoj, kaj poste maloftaj metaloj kiel arĝento kaj oro.

Estante la maldiligentaj estaĵoj ni estas, ni ne tro pensas pri aferoj kiuj nur funkcias. Mono, por plej multaj el ni, funkcias bone. Kiel ĉe niaj aŭtoj aŭ niaj komputiloj, la plej multaj el ni nur estas devigitaj pensi pri la interna funkciado de ĉi tiuj aferoj se ili malfunkcias. Homoj, kiuj vidis siajn vivŝparaĵojn malaperi pro hiperinflacio, scias la valoron de malmola mono, same kiel homoj, kiuj vidis siajn amikojn kaj familion malaperi pro la abomenaĵoj de Nazia Germanio aŭ Sovetrusio, scias la valoron de privateco.

La afero pri mono estas, ke ĝi estas ĉio ampleksa. Mono estas duono de ĉiu transakcio, kiu trempas tiujn, kiuj respondecas pri kreado de mono, kun enorma potenco.

"Konsiderante ke mono estas duono de ĉiu komerca transakcio kaj ke tutaj civilizacioj laŭvorte leviĝas kaj falas surbaze de la kvalito de sia mono, ni parolas pri mirinda potenco, kiu flugas sub la kovro de nokto. Ĝi estas la potenco teksi iluziojn kiuj ŝajnas realaj tiel longe kiel ili daŭras. Tio estas la kerno mem de la potenco de la Fed."
Ron Paul

Bitmono pace forigas ĉi tiun potencon, ĉar ĝi forigas monkreadon kaj ĝi faras tion sen la uzo de forto.

Mono trapasis plurajn ripetojn. Plej multaj ripetoj estis bonaj. Ili plibonigis nian monon en unu maniero aŭ alia. Tre lastatempe, tamen, la interna funkciado de nia mono koruptiĝis. Hodiaŭ, preskaŭ ĉio el nia mono estas simple kreita el la aero de la potencoj. Por kompreni, kiel ĉi tio okazis, mi devis lerni pri la historio kaj posta falo de mono.

Se necesos serio da katastrofoj aŭ simple monumenta eduka klopodo por korekti ĉi tiun korupton, restas por vidi. Mi preĝas al la dioj de sana mono, ke ĝi estu la lasta. Bitmono instruis al mi, kio estas mono.

Leciono 12

La historio kaj falo de mono

Ili ne memorus la simplajn regulojn kiujn iliaj amikoj donis al ili, kiel ekzemple, ke, se vi eniros la fajron, ĝi bruligos vin, kaj ke, se vi tranĉas vian fingron tre profunde per tranĉilo, ĝi ĝenerale sangas, kaj ŝi neniam forgesis, ke, se oni trinkas botelon kun markita "veneno", estas preskaŭ certe malkonsenti kun vi, baldaŭ aŭ malfrue.

Multaj homoj opinias, ke mono estas subtenata de oro, kiu estas ŝlosita for en grandaj volboj, protektitaj de dikaj muroj. Ĉi tio ĉesis esti vera antaŭ multaj jardekoj. Mi ne certas, kion mi pensis, ĉar mi havis multe pli profundan problemon, praktike ne havante komprenon pri oro, papera mono, aŭ kial ĝi devus esti subtenata de io en la unua loko.

Unu parto de lernado pri Bitmono estas lerni pri fiatmono: kion ĝi signifas, kiel ĝi fariĝis, kaj kial ĝi eble ne estas la plej bona ideo, kiun ni iam havis. Do, kio ĝuste estas fiatmono? Kaj kiel ni finis uzi ĝin?

Se io estas trudita per fiat, ĝi simple signifas ke ĝi estas trudita per formala rajtigo aŭ propono. Tiel, fida mono estas mono simple ĉar iu diras, ke ĝi estas mono. Ĉar ĉiuj registaroj uzas fidan moneron hodiaŭ, ĉi tiu iu estas via registaro. Bedaŭrinde, vi ne rajtas malkonsenti kun ĉi tiu valorpropono. Vi rapide sentos, ke ĉi tiu propono estas ĉio krom neperforta. Se vi rifuzas uzi ĉi tiun paperan moneron por fari komercon kaj pagi impostojn, la solaj homoj kun kiuj vi povos diskuti pri ekonomio estos viaj ĉelkamaradoj.

La valoro de fiatmono ne devenas de siaj propraj proprajĵoj. Kiom bona estas certa speco de fiatmono, estas nur korelaciita al la politika kaj fiska (mal) stabileco de tiuj, kiuj revas ĝin en ekziston. Ĝia valoro estas trudata per dekreto, arbitre.

Ĝis antaŭ nelonge, du specoj de mono estis uzataj: vara mono, farita el altvaloraj aferoj , kaj reprezenta mono , kiu simple reprezentas la valorajĵon, plejparte skribe.

Ni jam tuŝis varan monon supre. Homoj uzis specialajn ostojn, konkojn kaj valormetalojn kiel monon. Pli poste, plejparte moneroj faritaj el valormetaloj

kiel oro kaj arĝento estis utiligitaj kiel mono. La plej malnova monero trovita ĝis nun estas farita el natura oro-kaj-arĝenta miksaĵo kaj estis farita antaŭ pli ol 2700 jaroj. Se io estas nova en Bitmono, la koncepto de monero ne estas ĝi.

Montriĝas, ke akaparado de moneroj, aŭ hodling, por uzi la hodiaŭan lingvaĵon, estas preskaŭ same malnova kiel moneroj. La plej frua monerhodler estis iu kiu metis preskaŭ cent el tiuj moneroj en poton kaj entombigis ĝin en la fundamentoj de templo, nur por esti trovita 2500 jarojn poste. Sufiĉe bona malvarma konservado, se vi demandas min.

Unu el la malavantaĝoj de uzado de valormetalaj moneroj estas, ke ili povas esti tranĉitaj, efike malbonigante la valoron de la monero. Novaj moneroj povas esti monfaritaj el la eltondaĵoj, ŝveligante la monprovizon laŭlonge de la tempo, malplivalorigante ĉiun individuan moneron en la procezo. Homoj laŭvorte razis tiom kiom ili povis eliri el siaj arĝentaj dolaroj. Mi scivolas, kiajn reklamojn de Dollar Shave Club ili havis tiutempe.

Ĉar registaroj estas trankvilaj kun inflacio nur se ili estas tiuj kiuj faras ĝin, klopodoj estis faritaj por ĉesigi ĉi tiun gerilan malaltiĝon. En klasika modo de policistoj kaj rabistoj, monertondiloj fariĝis ĉiam pli kreemaj per siaj teknikoj, devigante la "mastrojn de la mento" fariĝi eĉ pli kreivaj per siaj kontraŭrimedoj. Isaac Newton, la mondfama fizikisto de Principia Mathematica famo, kutimis esti unu el ĉi tiuj majstroj. Li ricevas kun aldonado de la malgrandaj strioj ĉe la flanko de moneroj kiuj daŭre ĉeestas hodiaŭ. For estis la tagoj de facila monera razado.

Eĉ kun ĉi tiuj metodoj de monermalboniĝo tenitaj en kontrolo, moneroj ankoraŭ suferas aliajn aferojn. Ili estas dikaj kaj ne tre oportunaj por transporti, precipe kiam grandaj valortranspagoj devas okazi. Aperi kun grandega sako da arĝentaj dolaroj ĉiufoje kiam vi volas aĉeti Mercedes ne estas tre oportuna.

Parolante pri germanaj aferoj: Kiel la usona dolaro ricevis sian nomon estas alia interesa rakonto. La vorto "dolaro" estas derivita de la germana vorto Thaler, mallongigo por Joachimsthaler. Joachimsthaler estis monero monfarita en la urbo Sankt Joachimsthal. Thaler estas simple stenografio por iu (aŭ io) venanta de la valo, kaj ĉar Joachimsthal estis la valo por arĝentmoneroproduktado, homoj simple nomis tiujn arĝentajn monerojn Thaler. Thaler (germana) transformiĝis en daalders (nederlande), kaj finfine dolarojn (angla).

La enkonduko de reprezenta mono anoncis la falon de malmola mono. Oraj atestiloj estis lanĉitaj en 1863, kaj proksimume dek kvin jarojn poste, la arĝenta dolaro ankaŭ estis malrapide sed certe anstataŭigita per papera prokurilo: la arĝenta atestilo.

Daŭris proksimume 50 jarojn de la enkonduko de la unuaj arĝentaj atestiloj ĝis ĉi tiuj paperpecoj transformiĝis al io, kion ni hodiaŭ rekonus kiel unu usona dolaro.

Usona arĝenta dolaro de 1928. — Pagebla al la portanto laŭpeto. Bildkredito al la Nacia Numismatika Kolekto ĉe la Smithsonian Institucio

Notu, ke la usona arĝenta dolaro de 1928 supre ankoraŭ havas la nomon de arĝenta atestilo, indikante ke tio ja estas simple dokumento deklarante ke la portanto de ĉi tiu papero estas ŝuldata de arĝento. Estas interese vidi, ke la teksto kiu indikas tion malpligrandiĝis kun la tempo. La spuro de "atestilo" tute malaperis post iom da tempo, estante anstataŭigita per la trankviliga deklaro, ke ĉi tiuj estas federaciaj rezervaj notoj.

Kiel menciite supre, la sama afero okazis al oro. La plej granda parto de la mondo estis sur bimetala normo, signifante ke moneroj estis faritaj ĉefe el oro kaj arĝento. Havi atestilojn por oro, elaĉeteblajn en oraj moneroj, verŝajne estis teknologia plibonigo. Papero estas pli oportuna, pli malpeza, kaj ĉar ĝi povas esti dividita arbitre per simple presado de pli malgranda nombro sur ĝi, estas pli facile rompi en pli malgrandajn unuojn.

Por memorigi la portantojn (uzantoj), ke ĉi tiuj atestiloj estis reprezentaj por reala oro kaj arĝento, ili estis kolorigitaj laŭe kaj deklaris tion klare sur la atestilo mem. Vi povas flue legi la skribaĵon de supre ĝis malsupre:

"Ĉi tio atestas, ke estis deponitaj en la trezorejo de la Usono de Ameriko cent dolaroj en ora monero pagendaj al la portanto laŭ postulo."

Bildkredito al Nacia Numismatika Kolekto, Nacia Muzeo de Amerika Historio.

En 1963, la vortoj "PAGO AL LA PORTANTO SUR PETO" estis forigitaj de ĉiuj lastatempe eldonitaj notoj. Kvin jarojn poste, la elsaviĝo de papernotoj por oro kaj arĝento finiĝis.

La vortoj sugestaj pri la originoj kaj la ideo malantaŭ papera mono estis forigitaj. La ora koloro malaperis. Restis nur la papero kaj kun ĝi la kapablo de la registaro presi tiom da ĝi kiel ĝi deziras.

Kun la abolicio de la ora normo en 1971, ĉi tiu jarcent-longa lertaĵo estis kompleta. Mono fariĝis la iluzio, kiun ni ĉiuj dividas ĝis hodiaŭ: fiatmono. Ĝi valoras ion ĉar iu komandanta armeon kaj funkciigante malliberejojn diras, ke ĝi valoras ion. Kiel oni povas klare legi sur ĉiu dolar-bileto en cirkulado hodiaŭ, "ĈI NOTO ESTAS LEGALA OFERO". Alivorte: Ĝi estas valora ĉar la noto diras tion.

Serio de 2004 usona dudek-dolara bileto uzata hodiaŭ. 'ĈI NOTO ESTAS LEGALA OFERO'

Cetere, estas alia interesa leciono pri la hodiaŭaj bankbiletoj, kaŝita en plena vido. La dua linio legas, ke ĉi tio estas laŭleĝa pagilo "PRO ĈIUJ ŜULDOJ, PUBLIKA KAJ PRIVATA". Kio povus esti evidenta por ekonomikistoj estis surpriza al mi: Ĉiu mono estas ŝuldo. Mia kapo ankoraŭ doloras pro tio, kaj mi lasos la esploradon de la rilato de mono kaj ŝuldo kiel ekzercon al la leganto.

Kiel ni vidis, oro kaj arĝento estis uzataj kiel mono dum jarmiloj. Kun la tempo, moneroj faritaj el oro kaj arĝento estis anstataŭigitaj per papero. Papero malrapide iĝis akceptita kiel pago. Ĉi tiu akcepto kreis iluzion - la iluzion ke la papero mem havas valoron. La fina movo estis tute distrancĉi la ligon inter la reprezentado kaj la fakta: abolicii la oran standardon kaj konvinki ĉiujn ke la papero en si mem estas altvalora.

Bitmono instruis al mi pri la historio de mono kaj la plej granda lertaĵo en la historio de ekonomio: fiat-valuto.

Leciono 13

Frakcia Rezervo Frenezo

Ve! estis tro malfrue: ŝi daŭre kreskis kaj kreskis, kaj tre baldaŭ devis surgenuiĝi: post alia minuto ne estis loko eĉ por tio, kaj ŝi provis la efikon kuŝi, kun unu kubuto kontraŭ la pordo, kaj la alia brako kurbiĝis ĉirkaŭ ŝia kapo. Tamen ŝi daŭre kreskis, kaj kiel lasta rimedo ŝi metis unu brakon tra la fenestro, kaj unu piedon supren laŭ la kamentubo, kaj diris al si "nun mi ne povas fari plu—kio fariĝos kun mi?"

Valoro kaj mono ne estas bagatelaj temoj, precipe en la nunaj tempoj. La procezo de monkreado en nia banka sistemo estas same ne bagatela, kaj mi ne povas skui la senton, ke tio estas intence tiel. Kion mi antaŭe nur renkontis en akademio kaj juraj tekstoj ŝajnas esti ofta praktiko ankaŭ en la financa mondo: nenio estas klarigita per simplaj terminoj, ne ĉar ĝi estas vere kompleksa, sed ĉar la vero kaŝiĝas malantaŭ tavoloj kaj tavoloj de ĵargono kaj ŝajna kompleksеco. "Ekspansia monpolitiko, kvanta malstreĉiĝo, fiska stimulo al la ekonomio." La spektantaro kapjesas konsente, hipnotigita de la luksaj vortoj.

Frakcia rezerva bankado kaj kvanta mildigo estas du el tiuj elegantaj vortoj, malklarigante tion, kio vere okazas, maskante ĝin kiel kompleksa kaj malfacile komprenebla. Se vi klarigus ilin al kvinjara infano, la frenezo de ambaŭ evidentiĝos rapide.

Godfrey Bloom, alparolante la Eŭropan Parlamenton dum komuna debato, diris tion multe pli bone ol mi iam povus:

“[…] vi ne vere komprenas la koncepton de bankado. Ĉiuj bankoj estas rompitaj. Banko Santandero, Deutsche Bank, Royal Bank of Scotland — ili ĉiuj estas rompitaj! Kaj kial ili estas rompitaj? Ĝi ne estas ago de Dio. Ĝi ne estas ia cunamo. Ili estas rompitaj ĉar ni havas sistemon nomitan 'frakcia rezerva bankado' kio signifas, ke bankoj povas pruntedoni monon, kiun ili fakte ne havas! Ĝi estas krima skandalo kaj ĝi daŭras tro longe. […]

Ni havas falsaĵon - foje nomatan kvanta mildigo - sed falsaĵon sub iu alia nomo. La artefarita presado de mono kiun, se iu ordinara homo farus, ili irus al malliberejo por tre longa tempo […] kaj ĝis ni komencos sendi bankistojn —

kaj mi inkluzivas centrajn bankistojn kaj politikistojn — al malliberejo pro ĉi tiu indigno, ĝi daŭros. ."

Godfrey Bloom

Mi ripetu la plej gravan parton: bankoj povas pruntedoni monon, kiun ili fakte ne havas.

Danke al frakcia rezerva bankado, banko devas nur konservi malgrandan frakcion de ĉiu dolaro kiun ĝi ricevas. Ĝi estas ie inter 0 kaj 10%, kutime ĉe la malsupera fino, kio eĉ plimalbonigas la aferojn.

Ni uzu konkretan ekzemplon por pli bone kompreni ĉi tiun frenezan ideon: Frakcio de 10% faros la lertaĵon kaj ni devus povi fari ĉiujn kalkulojn en nia kapo. Venko-gajno. Do, se vi portas 100 USD al banko - ĉar vi ne volas konservi ĝin sub via matraco - ili devas nur konservi la interkonsentitan frakcion de ĝi. En nia ekzemplo tio estus $10, ĉar 10% de $100 estas $10. Facile, ĉu ne?

Kion do bankoj faras kun la resto de la mono? Kio okazas al viaj $90? Ili faras tion, kion faras bankoj, ili pruntedonas ĝin al aliaj homoj. La rezulto estas mona multiplika efiko, kiu ege pliigas la monprovizon en la ekonomio. Via komenca deponejo de $100 baldaŭ transformiĝos en $190. Pruntedonante 90%-frakcion de la nove kreitaj 90 USD, baldaŭ estos 271 USD en la ekonomio. Kaj $343.90 post tio. La monprovizo rekursie pliiĝas, ĉar bankoj laŭvorte pruntedonas monon, kiun ili ne havas. Sen ununura Abracadabra, bankoj magie transformas $100 en mil dolarojn aŭ pli. Rezultas 10x estas facila. Ĝi bezonas nur kelkajn pruntedonajn rondojn.

Ne miskomprenu min: Estas nenio malbona pri pruntedonado. Estas nenio malbona kun intereso. Eĉ ne estas io malbona ĉe bonaj malnovaj regulaj bankoj por konservi vian riĉaĵon ie pli sekura ol en via ŝtrumpeta tirkesto.

Centraj bankoj, tamen, estas malsama besto. Abomenaĵoj de financa reguligo, duone publika duone privata, ludanta dion kun io, kio tuŝas ĉiujn, kiuj estas parto de nia tutmonda civilizacio, sen konscienco, nur interesita pri la tuja estonteco, kaj ŝajne sen ajna respondeco aŭ revizio .

Dum Bitmono ankoraŭ estas inflacia, ĝi ĉesos esti tiel sufiĉe baldaŭ. La strikte limigita provizo de 21 milionoj da bitmonoj fine forigos inflacion tute. Ni nun

havas du monajn mondojn: inflacian, kie mono estas presita arbitre, kaj la mondo de Bitmono, kie fina provizo estas fiksita kaj facile kontrolebla por ĉiuj. Unu estas devigita al ni per perforto, al la alia povas aliĝi ĉiu, kiu deziras fari tion. Neniuj baroj al eniro, neniu por peti permeson. Volontula partopreno. Tio estas la beleco de Bitmono.

Mi argumentus, ke la argumento inter kejnesaj kaj aŭstraj ekonomikistoj ne plu estas pure akademia. Satoshi sukcesis konstrui sistemon por valortransigo sur steroidoj, kreante la plej solidan monon kiu iam ekzistis en la procezo. Unu maniero aŭ alia, pli kaj pli da homoj lernos pri la fraŭdo, kiu estas frakcia rezerva bankado. Se ili venas al similaj konkludoj kiel la plej multaj aŭstroj kaj Bitcoiners, ili eble aliĝos al la ĉiam kreskanta interreto de mono. Neniu povas haltigi ilin se ili elektas fari tion.

Bitmono instruis al mi, ke frakcia rezerva bankado estas pura frenezo.

Leciono 14

Sona mono

"La unua afero, kiun mi devas fari," diris Alicio al si mem, dum ŝi vagadis en la arbaro, "estas kreski ĝis mia ĝusta grandeco, kaj la dua estas trovi mian vojon en tiun belan ĝardenon. Mi pensas. Tio estos la plej bona plano."

La plej grava leciono, kiun mi lernis de Bitmono, estas, ke longtempe malmola mono superas mola mono. Malmola mono, ankaŭ nomata solida mono, estas ajna tutmonde komercita valuto, kiu funkcias kiel fidinda vendejo de valoro.

Konsentite, Bitmono ankoraŭ estas juna kaj volatila. Kritikistoj diros, ke ĝi ne konservas valoron fidinde. La argumento pri volatilo maltrafas. Volatileco estas atendata. La merkato daŭros iom por ekscii la justan prezon de ĉi tiu nova mono. Ankaŭ, kiel ofte ŝerce atentigas, ĝi baziĝas sur eraro de mezurado. Se vi pensas en dolaroj, vi malsukcesos vidi, ke unu Bitmono ĉiam valoros unu Bitmono.

"Fiksa monprovizo, aŭ provizo ŝanĝita nur laŭ objektivaj kaj kalkuleblaj kriterioj, estas necesa kondiĉo al senchava justa prezo de mono."
Fr. Bernard W. Dempsey, SJ

Kiel montris rapida promenado tra la tombejo de forgesitaj valutoj, mono, kiu povas esti presita, estos presita. Ĝis nun neniu homo en la historio povis rezisti ĉi tiun tenton.

Bitmono forigas la tenton presi monon en sprita maniero. Satoshi konsciis pri nia avideco kaj erareblo — tial li elektis ion pli fidindan ol homan sindetenon: matematikon.

$$\frac{\sum_{i=0}^{32} 210000 \left\lfloor \frac{50*10^8}{2^i} \right\rfloor}{10^8}$$

La provizoformulo de Bitmono

Dum ĉi tiu formulo estas utila por priskribi la provizon de Bitmono, ĝi fakte estas nenie en la kodo. Eldono de nova Bitmono estas farita en algoritme kontrolita modo, reduktante la rekompencon kiu estas pagita al ministoj ĉiujn kvar jarojn. La supra formulo estas uzata por rapide resumi tion, kio okazas sub la kapuĉo. Kio vere okazas, oni povas plej bone vidi rigardante la ŝanĝon en bloka rekompenco, la rekompenco pagita al kiu ajn trovas validan blokon, kio okazas proksimume ĉiujn 10 minutojn.

Formuloj, logaritmaj funkcioj kaj eksponencialoj ne estas ĝuste intuiciaj por kompreni. La koncepto de solideco povus esti pli facile komprenebla se rigardita alimaniere. Kiam ni scias kiom da io estas, kaj kiam ni scias kiom malfacile ĉi tiu io estas produkti aŭ atingi niajn manojn, ni tuj komprenas ĝian valoron. Kio validas por la pentraĵoj de Picasso, la gitaroj de Elvis Presley kaj la violonoj de Stradivarius, estas ankaŭ por la fiat-valuto, oro kaj bitmonoj.

La malmoleco de fiat-valuto dependas de kiu respondecas pri la respektivaj presiloj. Iuj registaroj eble pli volonte presis grandajn kvantojn da valuto ol aliaj, rezultigante pli malfortan valuton. Aliaj registaroj povus esti pli restriktaj en sia monpreso, rezultigante pli malmolan valuton.

Antaŭ ol ni havis fidajn monerojn, la solideco de mono estis determinita de la naturaj trajtoj de la aĵoj kiujn ni uzis kiel mono. La kvanto de oro sur la tero estas limigita de la leĝoj de fiziko. Oro estas malofta ĉar supernovaoj kaj neŭtronstelaj kolizioj estas maloftaj. La "fluo" de oro estas limigita ĉar ĉerpi ĝin estas sufiĉe penado. Estante peza elemento ĝi estas plejparte entombigita profunde subtere.

La abolicio de la ora normo cedis lokon al nova realo: aldoni novan monon postulas nur guton da inko. En nia moderna mondo aldoni kelkajn nulojn al la bilanco de bankkonto postulas eĉ malpli da peno: ĵeti kelkajn bitojn en banka komputilo sufiĉas.

"Unu grava aspekto de ĉi tiu nova realaĵo estas, ke institucioj kiel la Fed ne povas bankroti. Ili povas presi ajnan monsumon, kiun ili eble bezonos por si mem je preskaŭ nula kosto."
Jörg Guido Hülsmann

La principo skizita supre povas esti esprimita pli ĝenerale kiel la rilatumo de "akcio" al "fluo". Simple dirite, la stoko estas kiom da io estas nuntempe tie. Por niaj celoj, la stoko estas mezuro de la nuna monprovizo. La fluo estas kiom multe tie estas produktita dum tempodaŭro (ekz. jare). La ŝlosilo por kompreni solidan monon estas kompreni ĉi tiun akcion-al-fluan rilatumon.

Kalkuli la akcio-al-fluan rilatumon por fiat-valuto estas malfacila, ĉar kiom da mono ekzistas dependas de kiel vi rigardas ĝin. Vi povus kalkuli nur monbiletojn kaj monerojn (M0), aldoni vojaĝĉekojn kaj ĉekpagojn (M1), aldoni ŝparkontojn kaj reciprokajn fondusojn kaj iujn aliajn aferojn (M2), kaj eĉ aldoni atestojn pri deponejo al ĉio (M3). Plue, kiel ĉio ĉi estas difinita kaj mezurita varias de lando al lando kaj ĉar la Usona Federacia Rezervo ĉesis publikigi nombrojn por M3, ni devos kontentiĝi kun la mona provizo de M2. Mi ŝatus kontroli ĉi tiujn nombrojn, sed mi supozas, ke ni devas fidi la fed nuntempe.

Oro, unu el la plej raraj metaloj sur la tero, havas la plej altan akcio-al-fluan rilatumon. Laŭ la usona Geologia Enketo, iom pli ol 190 000 tunoj estis elminitaj. En la lastaj jaroj, ĉirkaŭ 3100 tunoj da oro estis elminitaj jare.

Uzante ĉi tiujn nombrojn, ni povas facile kalkuli la akcio-al-fluan rilatumon por oro: 190,000 tunoj / 3,100 tunoj = ~61.

Nenio havas pli altan akcio-al-fluan rilatumon ol oro. Tial oro, ĝis nun, estis la plej malfacila, plej sana mono en ekzisto. Estas ofte dirite ke la tuta oro elminita ĝis nun taŭgus en du olimpik-grandaj naĝejoj. Laŭ miaj kalkuloj, ni bezonus kvar. Do eble ĉi tio bezonas ĝisdatigon, aŭ olimpikaj naĝejoj malgrandiĝis.

Enigu Bitmono. Kiel vi verŝajne scias, Bitmono-minado furiozis en la lastaj du jaroj. Ĉi tio estas ĉar ni ankoraŭ estas en la fruaj fazoj de tio, kio nomiĝas la rekompenca epoko, kie minindustriaj nodoj estas rekompencitaj per multe da Bitmono pro sia komputila penado. Ni estas nuntempe en la rekompenca epoko numero 4, kiu komenciĝis en 2020 kaj finiĝos komence de 2024, verŝajne en majo. Dum la Bitmono-provizo estas antaŭdeterminita, la interna funkciado de Bitmono nur permesas proksimumajn datojn. Tamen, ni povas antaŭdiri kun certeco kiom alta estos la akcio-al-flua proporcio de Bitmono. Atentigo de Spoiler: ĝi estos alta.

Kiom alta? Nu, rezultas, ke Bitmono fariĝos senfine malfacila.

Pro eksponenta malkresko de la minindustria rekompenco, la fluo de nova Bitmono malpliiĝos rezultigante ĉiel-raketan akcion-al-fluan rilatumon. Ĝi preskaŭ atingis oron en 2020, nur por superi ĝin kvar jarojn poste denove duobligante sian solidecon. Tia duobligo okazos 32 fojojn entute. Danke al la potenco de eksponencialoj, la nombro da bitmono minitaj jare falos sub 100 Bitmono en 50 jaroj kaj sub 1 Bitmono en 75 jaroj. La tutmonda krano, kiu estas la bloka rekompenco, sekiĝos ie ĉirkaŭ la jaro 2140, efike ĉesigante la produktadon de Bitmono. Ĉi tio estas longa ludo. Se vi legas ĉi tion, vi ankoraŭ estas frua.

Ĉar Bitmono alproksimiĝas al senfina stoko al fluo-proporcio, ĝi estos la plej solida mono ekzistanta. Senfina solideco estas malfacile venki.

Rigardita tra la lenso de ekonomio, la malfacilaĵĝustigo de Bitmono estas verŝajne ĝia plej grava komponanto. Kiom malfacile estas minigi Bitmono dependas de kiom rapide novaj bitmonoj estas minitaj*. Ĝi estas la dinamika alĝustigo de la minindustria malfacilaĵo de la reto, kiu ebligas al ni antaŭdiri ĝian estontan provizon.

(* Ĝi fakte dependas de kiom rapide validaj blokoj estas trovitaj, sed por niaj celoj, ĉi tio estas la sama afero kiel "minado de bitmonoj" kaj estos tiel dum la venontaj 120 jaroj.)

La simpleco de la malfacilecĝustigo-algoritmo povus malatentigi de sia profundo, sed la malfacilecĝustigo vere estas revolucio de Einsteinianaj proporcioj. Ĝi certigas, ke kiom ajn aŭ kiom malmulte da fortostreĉo estas elspezita por minado, la kontrolita provizo de Bitmono ne estos interrompita. Kontraste al ĉiu alia rimedo, kiom ajn energio iu metos en minado de Bitmono, la totala rekompenco ne pliiĝos.

Same kiel $E=mc^2$ diktas la universalan rapidlimon en nia universo, la malfacilecĝustigo de Bitmono diktas la universalan monlimon en Bitmono.

Se ne estus ĉi tiu malfacileca ĝustigo, ĉiuj bitmonoj jam estus minitaj. Se ne estus ĉi tiu malfacileca ĝustigo, Bitmono verŝajne ne travivus en sia infanaĝo. Ĝi estas kio sekurigas la reton en ĝia rekompenca epoko. Ĝi estas kio certigas konstantan

kaj justan distribuadon de nova Bitmono. Ĝi estas la termostato kiu reguligas la monpolitikon de Bitmono.

Einstein montris al ni ion novan: kiom ajn vi puŝas objekton, en certa punkto vi ne povos akiri pli rapide el ĝi. Satoshi ankaŭ montris al ni ion novan: kiom ajn vi fosas por ĉi tiu cifereca oro, je certa punkto vi ne povos eltiri pli da bitmono el ĝi. Por la unua fojo en la homa historio, ni havas monan bonon, kiun, kiom ajn vi klopodos, vi ne povos produkti pli.

Bitmono instruis al mi, ke solida mono estas esenca.

Ĉapitro III

Teknologio

"Nun, mi plibonigos ĉi-foje" ŝi diris al si, kaj komencis preni la oran ŝlosilon kaj malŝlosi la pordon, kiu kondukis en la ĝardenon.

Oraj ŝlosiloj, horloĝoj, kiuj funkcias nur hazarde, kuroj por solvi strangajn enigmojn, kaj konstruistoj, kiuj ne havas vizaĝojn aŭ nomojn. Kio sonas kiel fabeloj de Mirlando estas ĉiutaga komerco en la mondo de Bitmono.

Kiel ni esploris en Ĉapitro 2, grandaj partoj de la nuna financa sistemo estas sisteme rompitaj. Kiel Alicio, ni povas nur esperi pli bone administri ĉi-foje. Sed, danke al pseŭdonima inventinto, ni havas nekredeble altnivelan teknologion por subteni nin ĉi-foje: Bitmono.

Solvi problemojn en radikale malcentralizita kaj kontraŭa medio postulas unikajn solvojn. Kio alie estus banalaj problemoj por solvi estas ĉio krom en ĉi tiu stranga mondo de nodoj. Bitmono dependas de forta kriptografio por plej multaj solvoj, almenaŭ se rigardite tra la lenso de teknologio. Kiom forta estas ĉi tiu ĉi kripto estos esplorita en unu el la sekvaj lecionoj.

Kriptografio estas kion Bitmono uzas por forigi fidon al aŭtoritatoj. Anstataŭ fidi je centralizitaj institucioj, la sistemo dependas de la fina aŭtoritato de nia universo: fiziko. Kelkaj grajnoj de fido ankoraŭ restas, tamen. Ni ekzamenos ĉi tiujn grajnojn en la dua leciono de ĉi tiu ĉapitro.

Leciono 15: Forto en nombroj
Leciono 16: Interkonsiliĝoj pri "Ne Fidu, Kontrolu"
Leciono 17: Rakonti tempon postulas laboron
Leciono 18: Movu malrapide kaj ne rompu aferojn
Leciono 19: Privateco ne mortis
Leciono 20: Cypherpunks skribas kodon
Leciono 21: Metaforoj por la estonteco de Bitmono

La lasta paro da lecionoj esploras la etoson de teknologia evoluo en Bitmono, kiu estas verŝajne same grava kiel la teknologio mem. Bitmono ne estas la sekva

brila programo en via telefono. Ĝi estas la fundamento de nova ekonomia realaĵo, tial Bitmono devus esti traktita kiel nuklea-grada financa programaro.

Kie ni estas en ĉi tiu financa, socia kaj teknologia revolucio? Retoj kaj teknologioj de la pasinteco povas servi kiel metaforoj por bitmonoj estonteco, kiuj estas esploritaj en la lasta leciono de ĉi tiu ĉapitro.

Denove, rimenu kaj ĝuu la veturon. Kiel ĉiuj eksponentaj teknologioj, ni estas parabolaj.

Leciono 15

Forto en nombroj

Mi vidu: kvaroble kvin estas dek du, kaj kvaroble ses estas dek tri, kaj kvaroble sep estas dek kvar—ho kara! Mi neniam atingos dudek kun tia rapideco!

Nombroj estas esenca parto de nia ĉiutaga vivo. Grandaj nombroj, tamen, ne estas io, kiun la plimulto el ni tro konas. La plej grandaj nombroj, kiujn ni povus renkonti en la ĉiutaga vivo, estas en la gamo de milionoj, miliardoj aŭ duilionoj. Ni povus legi pri milionoj da homoj en malriĉeco, miliardoj da dolaroj elspezitaj por bankaj savadoj, kaj bilionoj da nacia ŝuldo. Kvankam estas malfacile kompreni ĉi tiujn fraptitolojn, ni estas iom komfortaj kun la grandeco de tiuj nombroj.

Kvankam ni povus ŝajni komfortaj kun miliardoj kaj duilionoj, nia intuicio jam komencas malsukcesi kun nombroj de ĉi tiu grandeco. Ĉu vi havas intuicion, kiom longe vi devus atendi ke miliono/miliardo/triliono da sekundoj pasus? Se vi estas io kiel mi, vi estas perdita sen efektive kraki la nombrojn.

Ni rigardu pli detale ĉi tiun ekzemplon: la diferenco inter ĉiu estas pliiĝo je tri grandordoj: 10^6, 10^9, 10^{12}. Pensi pri sekundoj ne estas tre utila, do ni traduku ĉi tion en ion, kion ni povas ĉirkaŭvolvi nian kapon:

10^6: Unu miliono da sekundoj estis antaŭ 1½ semajnoj.
10^9: Unu miliardo da sekundoj estis antaŭ preskaŭ 32 jaroj.
10^{12}: Antaŭ unu duiliono da sekundoj Manhatano estis kovrita sub dika tavolo de glacio.

Tuj kiam ni eniras la preter-astronomian sferon de moderna kriptografio, nia intuicio malsukcesas katastrofe. Bitmono estas konstruita ĉirkaŭ grandaj nombroj kaj la virtuala neeblo diveni ilin. Ĉi tiuj nombroj estas multe pli grandaj ol ĉio, kion ni povus renkonti en la ĉiutaga vivo. Multaj grandordoj pli granda. Kompreni kiom grandaj ĉi tiuj nombroj vere estas estas esenca por kompreni Bitmonon kiel tuto.

Ni prenu SHA-256, unu el la hashfunkcioj uzataj en Bitmono, kiel konkreta ekzemplo. Estas nature pensi pri 256 bitoj kiel "ducent kvindek ses", kio tute ne estas granda nombro. Tamen, la nombro en SHA-256 parolas pri grandordoj - io, kion niaj cerboj ne estas bone ekipitaj por trakti.

Dum bita longo estas oportuna metriko, la vera signifo de 256-bita sekureco estas perdita en traduko. Simile al la milionoj (10^6) kaj miliardoj (10^9) supre, la nombro en SHA-256 temas pri grandordoj ($2^{2^{56}}$).

Do, kiom forta estas SHA-256, ĝuste?

"SHA-256 estas tre forta. Ĝi ne estas kiel la pliiga paŝo de MD5 al SHA1. Ĝi povas daŭri plurajn jardekojn krom se estas iu masiva trarompa atako."
Satoshi Nakamoto

Tio estas multe da neilionoj! Envolvi vian kapon ĉirkaŭ ĉi tiu nombro estas preskaŭ neeble. Estas nenio en la fizika universo por kompari ĝin. Ĝi estas multe pli granda ol la nombro da atomoj en la observebla universo. La homa cerbo simple ne estas farita por kompreni ĝin.

Bruce Schneier uzis la fizikajn limojn de komputado por meti ĉi tiun nombron en perspektivon: eĉ se ni povus konstrui optimuman komputilon, kiu uzus ajnan provizitan energion por perfekte renversi pecojn, konstrui Dyson-sferon ĉirkaŭ nia suno kaj lasus ĝin funkcii por 100 miliardoj. Miliardoj da jaroj, ni ankoraŭ havus nur 25% ŝancon trovi kudrilon en 256-bita fojnamaso.

"Ĉi tiu la j nombroj havas nenion komunan kun la teknologio de la aparatoj; ili estas maksimumoj, kiujn termodinamiko permesos. Kaj ili forte implicas, ke krudfortaj atakoj kontraŭ 256-bitaj ŝlosiloj estos nefareblaj ĝis komputiloj estos konstruitaj el io alia ol materio kaj okupos ion alian ol spacon."
Bruce Schneier

Estas malfacile troigi la profundecon de ĉi tio. Forta ĉifro renversas la potenco-ekvilibron de la fizika mondo al kiu ni estas tiel kutimita. Nerompeblaj aferoj ne ekzistas en la reala mondo. Apliku sufiĉe da forto, kaj vi povos malfermi ajnan pordon, skatolon aŭ trezorkeston.

La trezorkesto de Bitmono estas tre malsama. Ĝi estas sekurigita per forta kriptografio, kiu ne cedas lokon al kruda forto. Kaj tiel longe kiel la subestaj matematikaj supozoj validas, krudforto estas ĉio, kion ni havas. Konsentite, ekzistas ankaŭ la eblo de tutmonda atako de 5 USD. Sed torturo ne funkcios por ĉiuj Bitmono-adresoj, kaj la kriptaj muroj de Bitmono venkos krudfortajn atakojn. Eĉ se vi venos al ĝi kun la forto de mil sunoj. Laŭvorte.

Ĉi tiu fakto kaj ĝiaj implicoj estis kortuŝe resumitaj en la alvoko al kriptografiaj brakoj: " Neniu kvanto da truda forto iam solvos matematikan problemon."

"Ne estas evidente, ke la mondo devis funkcii tiel.
Sed iel la universo ridetas pro ĉifrado."
Julian Assange

Neniu ankoraŭ scias certe ĉu la rideto de la universo estas aŭtenta aŭ ne. Estas eble ke nia supozo de matematikaj malsimetrioj estas malĝusta kaj ni trovas ke P efektive egalas NP, aŭ ni trovas surprize rapidajn solvojn al specifaj problemoj kiujn ni nuntempe supozas esti malfacilaj. Se tio devus esti la kazo, kriptografio kiel ni scias ĝin ĉesos ekzisti, kaj la implicoj plej verŝajne ŝanĝus la mondon preter rekono.

"Vires in Numeris" = "Forto en Nombroj"
Epii

Vires in numeris ne estas nur alloga moto uzata de bitcoiners. La konscio, ke estas nesondebla forto trovebla en nombroj, estas profunda. Kompreni tion, kaj la inversigo de ekzistantaj potenc-ekvilibroj, kiujn ĝi ebligas, ŝanĝis mian vidpunkton pri la mondo kaj la estonteco, kiu estas antaŭ ni.

Unu rekta rezulto de ĉi tio estas la fakto, ke vi ne devas peti iun ajn permeson partopreni Bitmono. Ne estas paĝo por registriĝi, neniu kompanio respondeca, neniu registara agentejo al kiu sendi aliĝilojn. Simple generu grandan nombron kaj vi estas sufiĉe bona por iri. La centra aŭtoritato de kreado de kontoj estas matematiko. Kaj Dio nur scias, kiu respondecas pri tio.

Bitmono estas konstruita sur nia plej bona kompreno de realeco. Kvankam estas ankoraŭ multaj malfermitaj problemoj en fiziko, komputiko kaj matematiko, ni estas sufiĉe certaj pri iuj aferoj. Ke ekzistas malsimetrio inter trovi solvojn kaj

validigi la ĝustecon de ĉi tiuj solvoj estas tia afero. Tiu komputado bezonas energion estas alia. Alivorte: trovi kudrilon en fojnamaso estas pli malfacila ol kontroli ĉu la pintaĵo en via mano estas ja kudrilo aŭ ne. Kaj trovi la kudrilon postulas laboron.

La vasteco de la adresspaco de Bitmono estas vere mirinda. La nombro da privataj ŝlosiloj eĉ pli. Estas fascine kiom multe de nia moderna mondo resumiĝas al la malprobableco trovi kudrilon en nesondeble granda fojnamaso. Mi nun pli konscias pri ĉi tiu fakto ol iam ajn.

Bitmono instruis al mi, ke ekzistas forto en nombroj.

Leciono 16

Reflektadoj pri "Ne Fidu, Konfirmu"

"Nun por la pruvo," diris la Reĝo, "kaj poste la frazo."

Bitmono celas anstataŭigi, aŭ almenaŭ provizi alternativon al, konvencia valuto. Konvencia valuto estas ligita al centralizita aŭtoritato, negrave ĉu ni parolas pri jura pagilo kiel la usona dolaro aŭ moderna monopola mono kiel la V-Bucks de Fortnite. En ambaŭ ekzemploj, vi nepre fidi la centran aŭtoritaton por elsendi, administri kaj cirkuli vian monon. Bitmono malligas ĉi tiun ligon, kaj la ĉefa problemo kiun Bitmono solvas estas la temo de fido.

"La radika problemo kun konvencia valuto estas la tuta fido, kiu estas bezonata por ke ĝi funkciu. […] Kio necesas estas elektronika pagsistemo bazita sur kripta pruvo anstataŭ fido"
Satoshi

Bitmono solvas la problemon de fido estante tute malcentralizita, sen centra servilo aŭ fidindaj partioj. Eĉ ne fidindaj triaj, sed fidindaj partioj, punkto. Kiam ne ekzistas centra aŭtoritato, simple estas neniu por fidi. Kompleta malcentralizo estas la novigo. Ĝi estas la radiko de la fortikeco de Bitmono, la kialo kial ĝi ankoraŭ vivas. Malcentralizo ankaŭ estas kial ni havas minadon, nodojn, aparatajn monujojn, kaj jes, la blokĉenon. La nura afero, kiun vi devas "fidi", estas, ke nia kompreno pri matematiko kaj fiziko ne estas tute malfunkcia kaj ke la plimulto de ministoj agas honeste (kion ili estas instigitaj fari).

Dum la regula mondo funkcias sub la supozo de "fidu, sed kontrolu", Bitmono funkcias sub la supozo de "ne fidu, kontrolu." Satoshi tre klaras la gravecon forigi fidon kaj en la enkonduko kaj ankaŭ en la konkludo de la Bitmono-blankpapero.

"Konkludo: Ni proponis sistemon por elektronikaj transakcioj sen fidi je fido."
Satoshi Nakamoto

Notu, ke "sen fidi fidon" estas uzata en tre specifa kunteksto ĉi tie. Ni parolas pri fidindaj triaj partioj, te aliaj estaĵoj, kiujn vi fidas produkti, teni kaj prilabori vian monon. Oni supozas, ekzemple, ke vi povas fidi vian komputilon.

Kiel Ken Thompson montris en sia Turing Award prelego, fido estas ekstreme delikata afero en la komputila mondo. Dum funkciado de programo, vi devas fidi ĉiajn programojn (kaj aparataron) kiuj, teorie, povus ŝanĝi la programon, kiun vi provas ruli en malica maniero. Kiel Thompson resumis en siaj Reflections on Trusting Trust: "La moralo estas evidenta. Vi ne povas fidi kodon, kiun vi ne tute kreis mem."

Thompson pruvis, ke eĉ se vi havas aliron al la fontkodo, via kompililo — aŭ ajna alia programo-traktanta programo aŭ aparataro — povus esti endanĝerigita kaj detekti ĉi tiun malantaŭan pordon estus tre malfacila. Tiel, en la praktiko, vere nefidinda sistemo ne ekzistas. Vi devus krei vian tutan programaron kaj vian tutan aparataron (asembloj, kompililoj, ligiloj, ktp.) de nulo, sen la helpo de iu ekstera programaro aŭ programaro helpata maŝinaro.

"Se vi volas fari pomkukton de nulo, vi unue devas inventi la universon."
Carl Sagan

La Ken Thompson Hako estas precipe sprita kaj malfacile detektebla malantaŭa pordo, do ni rapide rigardu malfacile detekteblan malantaŭan pordon, kiu funkcias sen modifi ajnan programaron. Esploristoj trovis manieron endanĝerigi sekurec-kritikan aparataron ŝanĝante la polusecon de siliciaj malpuraĵoj. Nur ŝanĝante la fizikajn trajtojn de la aĵoj, el kiuj estas faritaj komputilaj blatoj, ili povis kompromiti ĉifri-sekuran hazardan nombrogeneratoron. Ĉar ĉi tiu ŝanĝo ne videblas, la malantaŭa pordo ne povas esti detektita per optika inspektado, kiu estas unu el la plej gravaj detektaj mekanismoj por ĉi tiuj blatoj.

Sonas timiga? Nu, eĉ se vi povus konstrui ĉion de nulo, vi ankoraŭ devus fidi la subestan matematikon. Vi devus fidi, ke secp256k1 estas elipsa kurbo sen malantaŭaj pordoj. Jes, malicaj malantaŭaj pordoj povas esti enmetitaj en la matematikajn fundamentojn de kriptografiaj funkcioj kaj verŝajne ĉi tio jam okazis almenaŭ unufoje. Estas bonaj kialoj por esti paranoja, kaj la fakto, ke ĉio de via aparataro, ĝis via programaro, ĝis la elipsaj kurboj uzataj povas havi malantaŭajn pordojn estas kelkaj el ili.

“Ne fidu. Kontrolu.”

La supraj ekzemploj devus ilustri, ke senfida komputado estas utopa. Bitmono verŝajne estas la unu sistemo, kiu plej proksimiĝas al ĉi tiu utopio, sed tamen ĝi estas fidominimigita - celante forigi fidon kie ajn eblas. Verŝajne, la ĉeno de konfido estas senĉesa, ĉar vi ankaŭ devos fidi ke komputado postulas energion, ke P ne egalas NP, kaj ke vi estas fakte en baza realeco kaj ne malliberigita en simulado de malicaj aktoroj.

Programistoj laboras pri iloj kaj proceduroj por minimumigi ajnan restantan fidon eĉ plu. Ekzemple, Bitmono-programistoj kreis Gitian, kio estas programara distribua metodo por krei determinismajn konstruojn. La ideo estas, ke se pluraj programistoj kapablas reprodukti identajn binarojn, la ŝanco de malica mistraktado estas reduktita. Fantaziaj malantaŭaj pordoj ne estas la sola atakvektoro. Simpla ĉantaĝo aŭ ĉantaĝo estas realaj minacoj ankaŭ. Kiel en la ĉefa protokolo, malcentralizo estas uzata por minimumigi fidon.

Diversaj klopodoj estas faritaj por plibonigi la problemon de kokido kaj ovo de ekŝargado, kiun la hako de Ken Thompson tiel brile atentigis. Unu tia fortostreĉo estas Guix (prononcita geeks), kiu uzas funkcie deklaritan pakaĵadministradon kondukantan al peceto-por-petaj reprodukteblaj konstruoj laŭ dezajno. La rezulto estas, ke vi ne plu devas fidi iujn ajn programarajn servilojn, ĉar vi povas kontroli, ke la servita binaro ne estis mistraktita rekonstruante ĝin de nulo. Lastatempe, tiro-peto estis kunfandita por integri Guix en la Bitmono-konstruprocezon.

Feliĉe, Bitmono ne dependas de ununura algoritmo aŭ peco de aparataro. Unu efiko de la radikala malcentralizo de Bitmono estas distribuita sekureca modelo. Kvankam la malantaŭaj pordoj priskribitaj supre ne devas esti prenitaj malpeze, estas neverŝajne ke ĉiu programara monujo, ĉiu aparatara monujo, ĉiu kriptografa biblioteko, ĉiu noda efektivigo kaj ĉiu kompililo de ĉiu lingvo estas kompromitita. Ebla, sed tre neverŝajna.

Rimarku, ke vi povas generi privatan ŝlosilon sen fidi al iu ajn komputila aparataro aŭ programaro. Vi povas ĵeti moneron kelkajn fojojn, kvankam depende de via monero kaj ĵetstilo ĉi tiu fonto de hazardo eble ne estas sufiĉe hazarda. Estas kialo, kial stokaj protokoloj kiel Glacier konsilas uzi kazingradajn ĵetkubojn kiel unu el du fontoj de entropio.

Bitmono devigis min pripensi, kion fido de neniu efektive implicas. Ĝi levis mian konscion pri la ekfunkciigo-problemo, kaj la implica ĉeno de fido en evoluigado kaj funkciado de programaro. Ĝi ankaŭ levis mian konscion pri la multaj manieroj en kiuj programaro kaj aparataro povas esti endanĝerigitaj.

Bitmono instruis min ne fidi, sed kontroli.

Leciono 17

Rakonti tempon postulas laboron

"Kara, kara! Mi estos tro malfrue!"

Ofte oni diras, ke bitmonoj estas minitaj ĉar miloj da komputiloj laboras pri solvado de tre kompleksaj matematikaj problemoj. Iuj problemoj estas solvitaj, kaj se vi komputas la ĝustan respondon, vi "produktas" Bitmono. Dum ĉi tiu simpligita vido de Bitmono-minado povus esti pli facile transdoni, ĝi iom maltrafas la punkton. bitmonoj ne estas produktitaj aŭ kreitaj, kaj la tuta suferado ne vere temas pri solvado de apartaj matematikaj problemoj. Ankaŭ, la matematiko ne estas precipe kompleksa. Kio estas kompleksa estas diri la tempon en malcentralizita sistemo.

Kiel skizite en la blankpapero, la pruvo-de-laborsistemo (alinome minado) estas maniero efektivigi distribuitan tempstampilon.

Kiam mi unue lernis kiel Bitmono funkcias, mi ankaŭ pensis, ke pruvo de laboro estas malefika kaj malŝparema. Post iom da tempo, mi komencis ŝanĝi mian perspektivon pri la energikonsumo de Bitmono. Ŝajnas, ke pruvo-de-laboro estas ankoraŭ vaste miskomprenita hodiaŭ, en la jaro 13 AB (post Bitmono).

Ĉar la problemoj solvendaj en pruvo-laboro estas konsistigitaj, multaj homoj ŝajnas kredi ke ĝi estas senutila laboro. Se la fokuso estas sole sur la komputado, ĉi tio estas komprenebla konkludo. Sed Bitmono ne temas pri komputado. Temas pri sendepende konsenti pri la ordo de aferoj.

Pruvo de laboro estas sistemo en kiu ĉiuj povas validigi kio okazis kaj en kia ordo ĝi okazis. Ĉi tiu sendependa validumado estas kio kondukas al konsento, individua interkonsento de multoblaj partioj pri kiu posedas kion.

En radikale malcentralizita medio, ni ne havas la lukson de absoluta tempo. Ĉiu horloĝo prezentus fidindan trian partion, centran punkton en la sistemo, pri kiu oni devis fidi kaj povus esti atakita. "La tempo estas la radika problemo," kiel Grisha Trubetskoy rimarkas. Kaj Satoshi brile solvis ĉi tiun problemon efektivigante malcentralizitan horloĝon per pruvo-de-labora blokĉeno. Ĉiuj konsentas antaŭe, ke la ĉeno kun la plej akumula laboro estas la fonto de vero.

Estas laŭdifino kio efektive okazis. Ĉi tiu interkonsento estas kio nun estas konata kiel Nakamoto-konsento.

"La reto tempostampas transakciojn havante ilin en daŭran ĉenon, kiu servas kiel pruvo de la sinsekvo de atestitaj eventoj"
Satoshi Nakamoto

Sen konsekvenca maniero diri la tempon, ne ekzistas konsekvenca maniero diri antaŭ ol post. Fidinda mendado estas neebla. Kiel menciite supre, Nakamoto-konsento estas la maniero de Bitmono konstante diri la tempon. La instigstrukturo de la sistemo produktas probabilisman, malcentralizitan horloĝon, uzante kaj avidecon kaj memintereson de konkurantaj partoprenantoj. La fakto, ke ĉi tiu horloĝo estas malpreciza, estas negrava ĉar la ordo de la okazaĵoj estas eventuale malambigua kaj povas esti kontrolita de iu ajn.

Danke al pruvo de laboro, kaj la laboro kaj la validigo de la laboro estas radikale malcentralizitaj. Ĉiu povas aliĝi kaj foriri laŭplaĉe, kaj ĉiu povas validigi ĉion ĉiam. Ne nur tio, sed ĉiuj povas validigi la staton de la sistemo individue, sen devi fidi al iu alia por validigo.

Kompreni pruvon de laboro postulas tempon. Ĝi ofte estas kontraŭintuicia, kaj dum la reguloj estas simplaj, ili kondukas al sufiĉe kompleksaj fenomenoj. Por mi, ŝanĝi mian perspektivon pri minado helpis. Utila, ne senutila. Valido, ne komputado. Tempo, ne blokoj.

Bitmono instruis al mi, ke diri la tempon estas malfacila, precipe se vi estas malcentralizita.

Leciono 18

Movu malrapide kaj ne rompu aferojn

Do la boato malrapide flugis, sub la hela somera tago, kun sia gaja ŝipanaro kaj sia muziko de voĉoj kaj ridado...

Ĝi povus esti morta mantro, sed "movu rapide kaj rompu aferojn" ankoraŭ estas kiom multe de la teknologia mondo funkcias. La ideo, ke ne gravas, se vi korektas la aferojn la unuan fojon, estas baza kolono de la malsukceso frue, malsukcesas ofte pensmaniero. Sukceso estas mezurita en kresko, do dum vi kreskas ĉio estas bona. Se io unue ne funkcias, vi simple pivotas kaj ripetas. Alivorte: ĵetu sufiĉe da merdo kontraŭ la muron kaj vidu, kio algluiĝas.

Bitmono estas tre malsama. Ĝi estas malsama laŭ dezajno. Ĝi estas malsama pro neceso. Kiel Satoshi indikis, elektronika monero estis provita multfoje antaŭe, kaj ĉiuj antaŭaj provoj malsukcesis ĉar estis kapo kiu povus esti fortranĉita. La noveco de Bitmono estas, ke ĝi estas besto sen kapoj.

"Multaj homoj aŭtomate malakceptas elektronikan valuton kiel perditan kaŭzon pro ĉiuj kompanioj, kiuj fiaskis ekde la 1990-aj jaroj. Mi esperas, ke estas evidente, ke nur la centre kontrolita naturo de tiuj sistemoj kondamnis ilin."
Satoshi Nakamoto

Unu sekvo de ĉi tiu radikala malcentralizo estas eneca rezisto al ŝanĝo. "Movu rapide kaj rompu aferojn" ne kaj neniam funkcios sur la baza tavolo de Bitmono. Eĉ se estus dezirinde, ĝi ne eblus sen konvinki ĉiujn ŝanĝi sian manieron. Tio estas distribuita konsento. Tio estas la naturo de Bitmono.

"La naturo de Bitmono estas tia, ke post kiam versio 0.1 estis publikigita, la kerndezajno estis fiksita en ŝtono por la resto de sia vivdaŭro."
Satoshi Nakamoto

Ĉi tio estas unu el la multaj paradoksaj propraĵoj de Bitmono. Ni ĉiuj kredis, ke ĉio, kio estas programaro, povas esti facile ŝanĝita. Sed la naturo de la besto malfaciligas ĝin ŝanĝi.

Kiel Hasu bele montras en la Socia Kontrakto de Malpakado de Bitmono, ŝanĝi la regulojn de Bitmono nur eblas proponante ŝanĝon, kaj sekve konvinkante ĉiujn uzantojn de Bitmono adopti ĉi tiun ŝanĝon. Ĉi tio faras Bitmono tre rezistema al ŝanĝo, kvankam ĝi estas programaro.

Ĉi tiu fortikeco estas unu el la plej gravaj propraĵoj de Bitmono. Kritikaj programaj sistemoj devas esti kontraŭfragilaj, kio estas tio, kion garantias la interagado de la socia tavolo de Bitmono kaj ĝia teknika tavolo. Monsistemoj estas kontraŭaj nature, kaj kiel ni scias dum miloj da jaroj solidaj fundamentoj estas esencaj en kontraŭa medio.

"La pluvo falis, la inundoj venis, kaj la ventoj blovis, kaj batis tiun domon; kaj ĝi ne falis, ĉar ĝi estis fondita sur roko."
[Mateo 7:25]

Verŝajne, en ĉi tiu parabolo de la saĝaj kaj la malsaĝaj konstruistoj Bitmono ne estas la domo. Ĝi estas la roko. Neŝanĝebla, senmova, provizante la fundamenton por nova financa sistemo.

Same kiel geologoj, kiuj scias, ke rokformacioj ĉiam moviĝas kaj evoluas, oni povas vidi, ke Bitmono ĉiam moviĝas kaj evoluas ankaŭ. Vi nur devas scii kie rigardi kaj kiel rigardi ĝin.
La enkonduko de pago al skripto hash kaj apartigita atestanto estas pruvo, ke la reguloj de Bitmono povas esti ŝanĝitaj se sufiĉe da uzantoj estas konvinkitaj, ke adopti koncernan ŝanĝon profitas al la reto. Ĉi-lasta ebligis la disvolviĝon de la fulma reto, kiu estas unu el la domoj konstruitaj sur la solida fundamento de Bitmono. Estontaj ĝisdatigoj kiel Schnorr-subskriboj plibonigos efikecon kaj privatecon, same kiel skriptojn (legu: inteligentaj kontraktoj) kiuj estos nedistingeblaj de regulaj transakcioj danke al Taproot. Saĝaj konstruantoj ja konstruas sur solidaj fundamentoj.

Satoshi ne estis nur saĝa konstruanto teknologie. Li ankaŭ komprenis, ke necesus ideologie fari saĝajn decidojn.

"Esti malferma fonto signifas, ke ĉiu povas sendepende revizii la kodon. Se ĝi estis fermita fonto, neniu povus kontroli la sekurecon. Mi pensas, ke estas esenca por ĉi tiu speco programo esti malferma fonto."
Satoshi Nakamoto

Malfermo estas plej grava al sekureco kaj eneca en malferma fonto kaj la libera programaro movado. Kiel Satoshi indikis, sekuraj protokoloj kaj la kodo, kiu efektivigas ilin, devas esti malfermitaj - ne ekzistas sekureco per obskureco. Alia profito denove rilatas al malcentralizo: kodo, kiu povas esti rulita, studita, modifita, kopiita kaj distribuita libere, certigas, ke ĝi estas disvastigita malproksimen.

La radikale malcentralizita naturo de Bitmono estas kio igas ĝin moviĝi malrapide kaj intence. Reto de nodoj, ĉiu administrita de suverena individuo, estas esence imuna al ŝanĝo - malica aŭ ne. Sen maniero devigi ĝisdatigojn al uzantoj, la nura maniero enkonduki ŝanĝojn estas malrapide konvinki ĉiujn kaj ĉiujn tiujn individuojn adopti ŝanĝon. Ĉi tiu ne-centra procezo de enkonduko kaj deplojado de ŝanĝoj estas kio faras la reton nekredeble rezistema al malicaj ŝanĝoj. Ĝi estas ankaŭ kio faras ripari rompitajn aferojn pli malfacila ol en centralizita medio, tial ĉiuj provas ne rompi aferojn en la unua loko.

Bitmono instruis al mi, ke moviĝi malrapide estas unu el ĝiaj trajtoj, ne cimo.

Leciono 19

Privateco ne mortis

La ludantoj ĉiuj ludis samtempe sen atendi turnojn, kaj dum la tuta tempo kverelis je la supro de siaj voĉoj, kaj post tre malmultaj minutoj la Reĝino estis en furioza pasio, kaj ĉirkaŭpaŝis kaj kriis "for per sia kapo!" aŭ "for kun ŝia kapo!" proksimume unufoje en minuto.

Se oni kredas, ke la privateco estas mortinta ekde la 80-aj jaroj. La pseŭdonima invento de Bitmono kaj aliaj eventoj en lastatempa historio montras, ke ĉi tio ne estas la kazo. Privateco vivas, kvankam estas neniel facile eskapi de la gvata stato.

Satoshi ekzamenis grandajn longojn por kovri siajn spurojn kaj kaŝi sian identecon. Dek tri jarojn poste, estas daŭre nekonate ĉu Satoshi Nakamoto estis ununura persono, grupo de homoj, masklo, ino, aŭ temp-vojaĝanta AI kiu startigis sin por transpreni la mondon. Konspiraj teorioj flankenmetite, Satoshi elektis identigi sin kiel japana masklo, tial mi ne supozas sed respektas lian elektitan sekson kaj nomas lin li.

Kia ajn lia reala identeco povus esti, Satoshi sukcesis en kaŝado de ĝi. Li donis kuraĝigan ekzemplon por ĉiuj, kiuj deziras resti anonimaj: eblas havi privatecon rete.

"Ĉifrado funkcias. Ĝuste efektivigitaj fortaj kriptaj sistemoj estas unu el la malmultaj aferoj, pri kiuj vi povas fidi."
Edward Snowden

Satoshi ne estis la unua pseŭdonima aŭ anonima inventinto, kaj li ne estos la lasta. Iuj rekte imitis ĉi tiun pseŭdoniman publikigstilon, kiel Tom Elvis Yedusor de MimbleWimble famo, dum aliaj publikigis progresintajn matematikajn pruvojn restante tute anonimaj.

Ĝi estas stranga nova mondo, en kiu ni vivas. Mondo kie identeco estas laŭvola, kontribuoj estas akceptitaj laŭ merito, kaj homoj povas kunlabori kaj komerci libere. Necesos iom da alĝustigo por komfortiĝi kun ĉi tiuj novaj paradigmoj, sed mi forte kredas, ke ĉio ĉi havas la eblecon ŝanĝi la mondon al pli bona.

Ni ĉiuj memoru, ke privateco estas fundamenta homa rajto . Kaj dum homoj ekzercas kaj defendas ĉi tiujn rajtojn, la batalo por privateco estas malproksima de finita.

Bitmono instruis al mi, ke privateco ne mortis.

Leciono 20

Ĉifrpunkoj skribas kodon

Mi vidas, ke vi provas elpensi ion.

Kiel multaj bonegaj ideoj, Bitmono ne eliris de nenie. Ĝi fariĝis ebla utiligante kaj kombinante multajn inventojn kaj eltrovaĵojn en matematiko, fiziko, komputiko, kaj aliaj kampoj. Kvankam sendube geniulo, Satoshi ne povintus inventi Bitmono sen la gigantoj sur kies ŝultroj li staris.

"Kiu nur deziras kaj esperas, tiu ne enmiksiĝas aktive en la kurson de la okazaĵoj kaj en la formadon de sia propra destino."
Ludwig Von Mises

Unu el ĉi tiuj gigantoj estas Eric Hughes, unu el la fondintoj de la cypherpunk-movado kaj aŭtoro de la cypherpunk manifesto. Estas malfacile imagi, ke Satoshi ne estis influita de ĉi tiu manifesto. Ĝi parolas pri multaj aferoj, kiujn Bitmono ebligas kaj uzas, kiel rektaj kaj privataj transakcioj, elektronika mono kaj kontantmono, anonimaj sistemoj, kaj defendado de privateco per kriptografio kaj ciferecaj subskriboj.

"Privateco estas necesa por malferma socio en la elektronika epoko. […] Ĉar ni deziras privatecon, ni devas certigi, ke ĉiu partio al transakcio havas scion nur pri tio, kio estas rekte necesa por tiu transakcio. […]

Tial privateco en malferma socio postulas anonimajn transakciajn sistemojn. Ĝis nun, kontantmono estis la ĉefa tia sistemo. Anonima transakcia sistemo ne estas sekreta transakcia sistemo. […]

Ni la Cypherpunks dediĉas sin al konstruado de anonimaj sistemoj. Ni defendas nian privatecon per kriptografio, per anonimaj poŝtsendsistemoj, per ciferecaj subskriboj kaj per elektronika mono.

Cypherpunks skribas kodon."
Eric Hughes

Cypherpunks ne trovas konsolon en esperoj kaj deziroj. Ili aktive malhelpas la kurson de la eventoj kaj formas sian propran destinon. Cypherpunks skribas kodon.

Tiel, laŭ vera ĉifrpunka modo, Satoshi sidiĝis kaj komencis skribi kodon. Kodo kiu prenis abstraktan ideon kaj pruvis al la mondo ke ĝi efektive funkciis. Kodo kiu plantis la semon de nova ekonomia realo. Danke al ĉi tiu kodo, ĉiuj povas kontroli, ke ĉi tiu nova sistemo efektive funkcias, kaj ĉiun 10 minutojn Bitmono pruvas al la mondo, ke ĝi ankoraŭ vivas.

Por certigi ke lia novigado transcendas fantazion kaj iĝas realeco, Satoshi skribis kodon por efektivigi sian ideon antaŭ ol li skribis la blankpaperon. Li ankaŭ certigis ne prokrasti ajnan liberigon por ĉiam. Post ĉio, "ĉiam estos unu plia afero por fari."

"Mi devis skribi la tutan kodon antaŭ ol mi povis konvinki min, ke mi povas solvi ĉiun problemon, tiam mi skribis la paperon."
Satoshi Nakamoto

En la hodiaŭa mondo de senfinaj promesoj kaj dubinda ekzekuto, ekzercado en dediĉita konstruaĵo estis urĝe bezonata. Estu intenca, konvinku vin, ke vi efektive povas solvi la problemojn, kaj efektivigi la solvojn. Ni ĉiuj devus celi esti iom pli ĉifrpunkaj.

Bitmono instruis al mi, ke ĉifrpunkoj skribas kodon.

Leciono 21

Metaforoj por la estonteco de Bitmono

Mi scias, ke io interesa certe okazos...

En la lastaj kelkaj jardekoj, evidentiĝis, ke teknologia novigo ne sekvas linearan tendencon. Ĉu vi kredas je la teknologia singularo aŭ ne, estas nekontesteble, ke progreso estas eksponenta en multaj kampoj. Ne nur tio, sed la rapideco je kiu teknologioj estas adoptitaj akcelas, kaj antaŭ ol vi scias tion, la arbusto en la loka lerneja korto malaperis kaj viaj infanoj uzas Snapchat anstataŭe. Eksponenciaj kurboj havas la emon vangofrapi vin antaŭ ol vi vidas ilin veni.

Bitmono estas eksponenta teknologio konstruita sur eksponenta teknologioj. Nia Mondo en Datumoj bele montras la altiĝantan rapidecon de teknologia adopto, komencante en 1903 kun la enkonduko de fikstelefonoj. Fiksaj telefonoj, elektro, komputiloj, interreto, saĝtelefonoj; ĉiuj sekvas eksponentajn tendencojn en prezo-efikeco kaj adopto. Bitmono ankaŭ faras.

Bitmono havas ne unu sed multoblajn retajn efikojn, ĉiuj el kiuj rezultigas eksponentajn kreskopadronojn en ilia respektiva areo: prezo, uzantoj, sekureco, programistoj, merkatparto kaj adopto kiel tutmonda mono.

Postvivinte sian infanaĝon, Bitmono daŭre kreskas ĉiutage en pli da aspektoj ol unu. Konsentite, la teknologio ankoraŭ ne atingis maturecon. Ĝi povus esti en sia adoleskeco. Sed se la teknologio estas eksponenta, la vojo de obskureco al ĉieo estas mallonga.

En lia 2003 TED-babilado, Jeff Bezos elektis utiligi elektron kiel metaforon por la estonteco de la reto. Ĉiuj tri fenomenoj — elektro, interreto, Bitmono — ebligas teknologiojn, retojn kiuj ebligas aliajn aferojn. Ili estas konstruotaj infrastrukturoj, fundamentaj en naturo.

Elektro ekzistas jam de kelka tempo. Ni prenas ĝin por koncedita. La interreto estas sufiĉe pli juna, sed la plej multaj homoj jam konsideras ĝin ankaŭ. Bitmono havas dek jarojn kaj eniris publikan konscion dum la lasta ciklo de ekzaltiĝo. Nur la plej fruaj adoptantoj prenas ĝin por koncedita. Dum pli da tempo pasas, pli kaj pli da homoj rekonos Bitmono kiel io, kio simple estas.

En 1994, la interreto daŭre estis konfuza kaj neintuicia. Rigardi ĉi tiun malnovan registradon de la Today Show evidentigas, ke tio, kio nun sentas natura kaj intuicia, fakte ne estis tiam. Bitmono ankoraŭ estas konfuza kaj fremda al la plej multaj, sed same kiel interreto estas dua naturo por ciferecaj indiĝenoj, elspezado kaj stakigado de satoj estos dua naturo al la Bitmono-indiĝenoj de la estonteco.

"La estonteco jam estas ĉi tie - ĝi simple ne estas tre egale distribuita."
Vilhelmo Gibson

En 1995, ĉirkaŭ 15% de amerikaj plenkreskuloj uzis la interreton. Historiaj datumoj de la Pew Research Center montras kiel interreto teksis sin en niajn tutajn vivojn. Laŭ enketo pri konsumantoj de Kaspersky Lab, 13% de la respondantoj uzis Bitmono kaj ĝiajn klonojn por pagi varojn en 2018. Kvankam pagoj ne estas la sola uzkazo de Bitmono, ĝi estas iu indiko de kie ni estas en Interreta tempo en la frua- ĝis mez-90-aj jaroj.

En 1997, Jeff Bezos deklaris en letero al akciuloj ke "ĉi tio estas Tago 1 por la Interreto", rekonante la grandan neeluzitan potencialon por la interreto kaj, per etendaĵo, lia firmao. Kia ajn tago ĉi tio estas por Bitmono, la vastaj kvantoj de neeluzita potencialo estas klaraj por ĉiuj krom la plej hazarda observanto.

La unua nodo de Bitmono enretiĝis en 2009 post kiam Satoshi minis la genezan blokon kaj liberigis la programaron en la sovaĝejon. Lia nodo longe ne estis sola. Hal Finney estis unu el la unuaj homoj se temas pri repreni la ideon kaj aliĝi al la reto. Dek jarojn poste, de ĉi tiu skribado, pli ol 75.000 nodoj kuras Bitmono.

La baza tavolo de la protokolo ne estas la nura aĵo kreskanta eksponente. La fulma reto, dua tavola teknologio, kreskas eĉ pli rapide.

En januaro 2018, la fulma reto havis 40 nodojn kaj 60 kanalojn. En aprilo 2019, la reto kreskis al pli ol 4000 nodoj kaj ĉirkaŭ 40.000 kanaloj. Memoru, ke ĉi tio estas ankoraŭ eksperimenta teknologio, kie perdo de financo povas kaj okazas. Tamen la tendenco estas klara: miloj da homoj estas malzorgemaj kaj fervoraj uzi ĝin.

Por mi, travivinte la fulman kreskon de la reto, la paraleloj inter la interreto kaj Bitmono estas evidentaj. Ambaŭ estas retoj, ambaŭ estas eksponentaj teknologioj, kaj ambaŭ ebligas novajn eblecojn, novajn industriojn, novajn vivmanierojn. Same kiel elektro estis la plej bona metaforo por kompreni kien interreto iras, la interreto povus esti la plej bona metaforo por kompreni kien Bitmono iras. Aŭ, laŭ la vortoj de Andreas Antonopoulos, Bitmono estas La Interreto de Mono. Ĉi tiuj metaforoj estas bonega rememorigilo, ke kvankam la historio ne ripetas sin, ĝi ofte rimiĝas.

Eksponencaj teknologioj estas malfacile kompreneblaj kaj ofte subtaksitaj. Kvankam mi havas grandan intereson pri tiaj teknologioj, mi estas konstante surprizita de la ritmo de progreso kaj novigo. Rigardi la Bitmono-ekosistemon kreski estas kiel rigardi la pliiĝon de la interreto rapide antaŭen. Ĝi estas ĝojiga.

Mia serĉo provi kompreni Bitmonon kondukis min laŭ la vojoj de la historio en pli ol unu manieroj. Kompreni antikvajn sociajn strukturojn, pasintajn monojn kaj kiel evoluis komunikadaj retoj estis ĉiuj parto de la vojaĝo. De la manhakilo ĝis la saĝtelefono, teknologio sendube ŝanĝis nian mondon multfoje. Interretaj teknologioj estas precipe transformaj: skribo, vojoj, elektro, interreto. Ĉiuj ili ŝanĝis la mondon. Bitmono ŝanĝis la mian kaj daŭre ŝanĝos la mensojn kaj korojn de tiuj, kiuj kuraĝas uzi ĝin.

Bitmono instruis al mi, ke kompreni la pasintecon estas esenca por kompreni ĝian estontecon. Estonto kiu ĵus komenciĝas.

Konkludo

Lecionoj lernitaj

"Komencu de la komenco," diris la Reĝo, tre serioze,
"kaj daŭrigu ĝis vi venos al la fino: tiam ĉesu."

Kiel menciite en la komenco, mi pensas, ke ajna respondo al la demando "Kion vi lernis de Bitmono?" ĉiam estos nekompleta. La simbiozo de tio, kio povas esti vidita kiel multoblaj vivsistemoj - Bitmono, la teknosfero kaj ekonomio - estas tro interplektitaj, la temoj tro multaj, kaj aferoj moviĝas tro rapide por iam esti plene komprenataj de ununura persono.

Eĉ sen kompreni ĝin plene, kaj eĉ kun ĉiuj ĝiaj strangaĵoj kaj ŝajnaj mankoj, Bitmono sendube funkcias. Ĝi daŭre produktas blokojn proksimume ĉiujn dek minutojn kaj faras tion bele. Ju pli longe Bitmono daŭre funkcias, des pli da homoj elektos por uzi ĝin.

"Estas vere, ke aferoj estas belaj kiam ili funkcias. Arto estas funkcio."
Giannina Braschi

Bitmono estas infano de interreto. Ĝi kreskas eksponente, malklarigante la liniojn inter disciplinoj. Ne estas klare, ekzemple, kie la sfero de pura teknologio finiĝas kaj kie alia sfero komenciĝas. Kvankam Bitmono postulas komputilojn funkcii efike, komputiko ne sufiĉas por kompreni ĝin. Bitmono estas ne nur senlima rilate al sia interna funkciado sed ankaŭ senlima rilate akademiajn disciplinojn.

Ekonomio, politiko, ludoteorio, monhistorio, reto-teorio, financo, kriptografio, informa teorio, cenzuro, leĝo kaj reguligo, homa organizo, psikologio - ĉio ĉi kaj pli estas kompetentecoj kiuj povus helpi en la serĉo de kompreno kiel Bitmono funkcias kaj kio estas Bitmono.

Neniu ununura invento respondecas pri ĝia sukceso. Ĝi estas la kombinaĵo de multoblaj, antaŭe senrilataj pecoj, kungluitaj per ludteoriaj instigoj, kiuj konsistigas la revolucion kiu estas Bitmono. La bela miksaĵo de multaj disciplinoj estas kio igas Satoshi geniulo.

Kiel ĉiu kompleksa sistemo, Bitmono devas fari kompensojn laŭ efikeco, kosto, sekureco kaj multaj aliaj propraĵoj. Same kiel ne ekzistas perfekta solvo por derivi kvadraton el cirklo, ĉiu solvo al la problemoj, kiujn Bitmono provas solvi, ĉiam estos ankaŭ neperfekta.

"Mi ne kredas, ke ni iam denove havos bonan monon antaŭ ol ni forprenos la aferon el la manoj de la registaro, tio estas, ni ne povas forpreni ĝin perforte el la manoj de la registaro, ĉio kion ni povas fari estas de iuj ruzaj ĉirkaŭvojoj enkonduku ion, kion ili ne povas ĉesigi."

Friedrich Hayek

Bitmono estas la ruza, ĉirkaŭvojo por reenkonduki bonan monon al la mondo. Ĝi faras tion metante suverenan individuon malantaŭ ĉiu nodo, same kiel Da Vinci provis solvi la nesolveblan problemon de kvadratado de cirklo metante la Vitruvan Homon en ĝian centron. Nodoj efike forigas ajnan koncepton de centro, kreante sistemon kiu estas mirige kontraŭfragila kaj ekstreme malfacile fermebla. Bitmono vivas, kaj ĝia korbato verŝajne postvivos ĉiujn niajn.

Mi esperas, ke vi ĝuis ĉi tiujn dudek unu lecionojn. Eble la plej grava leciono estas, ke Bitmono devus esti ekzamenita holisme, de pluraj anguloj, se oni ŝatus havi ion proksimuman kompletan bildon. Same kiel forigi unu parton de kompleksa sistemo detruas la tuton, ekzameni partojn de Bitmono izole ŝajnas makuli la komprenon de ĝi. Se nur unu persono batos "blokĉeno" el ŝia vortprovizo kaj anstataŭigas ĝin per "ĉeno de blokoj" mi mortos feliĉa viro.

Ĉiukaze mia vojaĝo daŭras. Mi planas enriskiĝi pli malsupre en la profundon de ĉi tiu kuniklotruo, kaj mi invitas vin kuntaksi por la veturo.

Rekonoj

"Dankon," diris Alicio

Dankon al la sennombraj aŭtoroj kaj enhavproduktantoj, kiuj influis mian pensadon pri Bitmono kaj la temoj kiujn ĝi tuŝas. Estas tro multaj por listigi ilin ĉiujn, sed mi faros mian eblon por nomi kelkajn.

Dankon al Arjun Balaji pro la ĉirpeto, kiu instigis min skribi ĉi tion.

Dankon al Marty Bent pro provizi senfinan manĝaĵon por penso kaj distro. Se vi ne estas abonita al Marty's Ƀent kaj Tales From The Crypt, vi maltrafas. Salutojn Matt kaj Marty por gvidi nin tra la kuniklotruo.

Dankon al Michael Goldstein kaj Pierre Rochard pro vikario kaj provizi la plej bonegan Bitmono-literaturon per la Instituto Nakamoto. Kaj dankon pro krei la Noded Podkaston, kiu multe influis miajn filozofiajn opiniojn pri Bitmono.

Dankon al Peter McCormack pro liaj honestaj tweets kaj la podkasto What Bitcoin Did, kiu daŭre provizas bonegajn komprenojn de multaj areoj de la spaco.

Dankon al Andreas M. Antonopoulos pro la tuta eduka materialo, kiun li elmetis dum la jaroj.

Dankon al Saifedean Ammous pro siaj konvinkoj, sovaĝaj tweets kaj verkado de The Bitcoin Standard

Dankon al Francis Pouliot pro dividi sian eksciton pri ekscii pri la tempoĉeno.

Dankon al Jannik, Brandon, Matt, Camilo, Daniel, Michael, kaj Raphael por provizi komentojn al fruaj skizoj de kelkaj lecionoj. Specialan dankon al Jannik, kiu plurfoje provlegis plurajn malnetojn.

Dankon al Dhruv Bansal kaj Matt Odell por preni la tempon diskuti kelkajn el ĉi tiuj ideoj kun mi.

Dankon al Guy Swann pro produktado de sonversio de 21lessons.com.

Laste sed ne malpli, danke al ĉiuj Bitmono-maksimumistoj, shitcoin-minimistoj, shills, bots, kaj shitposters kiuj loĝas en la bela ĝardeno kiu estas Bitmono-twitter. Kaj finfine, dankon pro legi ĉi tion. Mi esperas, ke vi ĝuis ĝin tiom kiom mi ĝuis skribi ĝin. Bonvolu kontakti min per tvitero. Miaj DM estas malfermitaj.

https://twitter.com/dergigi

Dankon

...por legi, por esti ĉi tie, por provi kompreni.

"Ĝi ŝajnas tre bela," ŝi diris kiam ŝi finis ĝin,
"sed ĝi estas sufiĉe malfacile komprenebla!"