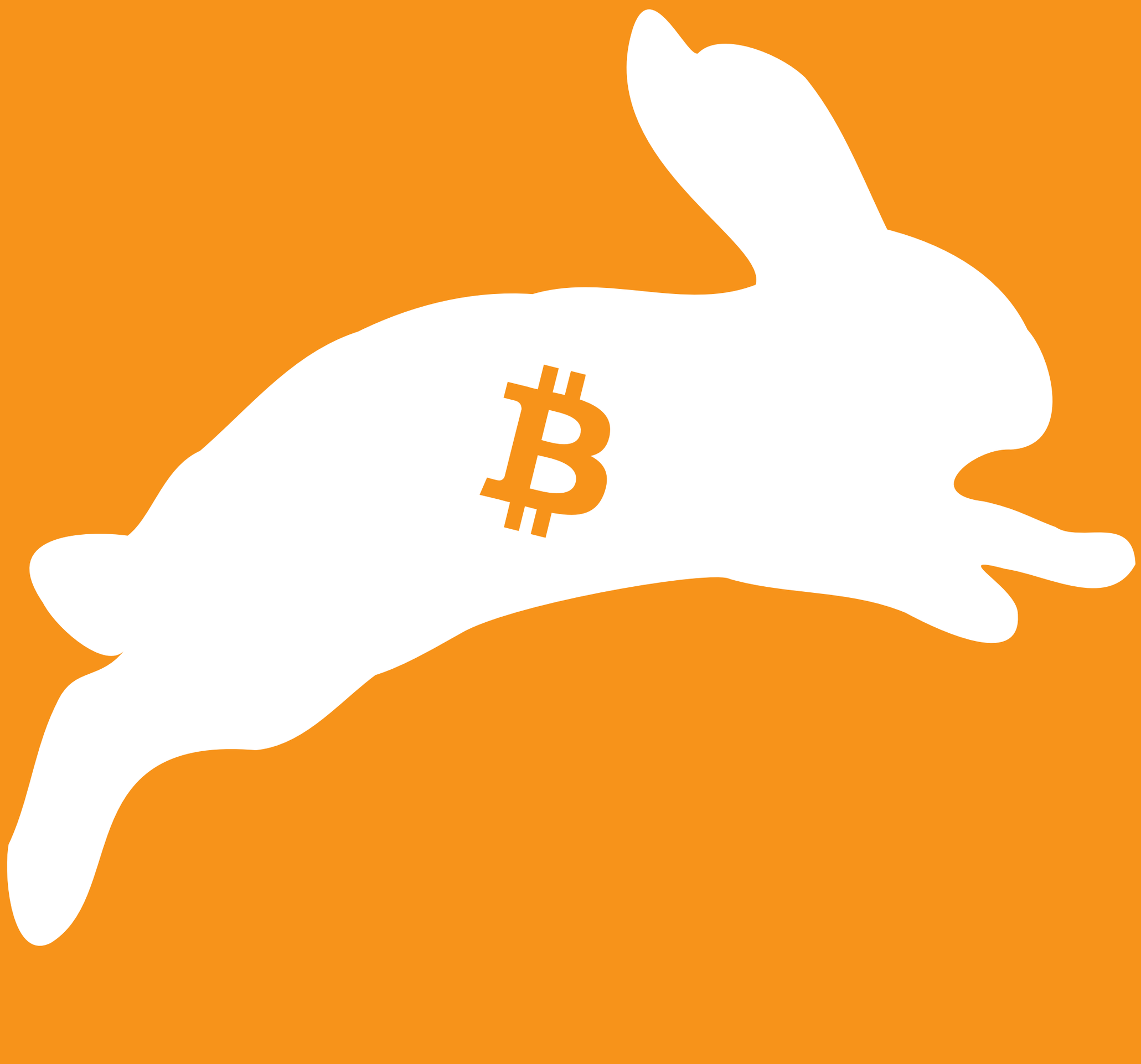
21 ЛЕКЦИЈА



ШТА САМ НАУЧИО ПАДАЈУЋИ У ЗЕЧЈУ РУПУ

Ђиђи

21 Лекција

ШТА САМ НАУЧИО ПАДАЈУЋИ У ЗЕЧЈУ РУПУ

Ђиђи

www.21Lessons.com

Преводилац: Михаило | Suri Translations
Руководилац пројекта: Рагхав Сури

Преведено са енглеског на српски.

Пратите Ђиђи:
www.DerGigi.com
nostr

Пратите Suri Translations:
www.SuriTranslations.com
X | Instagram

Предговор

Падање низ зечју рупу биткоина је чудно искуство. Као и многи други, осећам да сам научио више у последњих пар година проучавајући биткоин него за две деценије формалног образовања.

Лекције које следе су есенција онога што сам научио. Испрва објављено као серија чланака под насловом "Шта сам научио од Биткоина" ово што следи може се сматрати за друго издање те првобитне серије.

Као и Биткоин, ове лекције нису статична ствар. Планирам да их обрађујем периодично, објављујући у будућности ажуриране верзије и додатни материјал.

За разлику од Биткоина, будуће верзије овог пројекта не морају да буду компатибилне са претходним. Неке лекције ће можда бити проширене, остале прерађене или замењене. Надам се да ће нека будућа верзија бити нешто што можете држати у руци, али засада још ништа не желим да обећам.

Биткоин је неисцрпни учитељ, и то је оно због чега не тврдим да су ове лекције свеобухватне или потпуне. Оне су одраз мог личног путовања низ зечју рупу. Има још много лекција за учење, и свака особа научи нешто друго када уђе у свет Биткоина.

Надам се да ће вам ове лекције бити корисне и да ће процес њиховог учења читањем бити мање тежак и болан од учења из прве руке.

Ђиђи

Садржај

Увод

У октобру 2018, Арџун Балаџи поставио је безазлено питање, Шта сте научили од Биткоина?. Пошто сам покушао да одговорим на ово питање у кратком твиту, и пошто сам јадно пропао, схватио сам да су ствари које сам научио сувише бројне да би се могло одговорити кратко, ако би уопште и могло.

Ствари које сам научио су, очигледно, о Биткоину – или су бар везане за њега. Међутим, иако је нешто од унутрашњег рада Биткоина објашњено, лекције које следе нису објашњене тога како биткоин ради или шта је он, међутим, једно би могло да помогне да се истраже неке од ствари које се Биткоин дотиче: филозофска питања, економске реалности, и технолошке иновације.

Ова 21 лекција структурирана је у пакетима од по седам, што чини три главе. Свака глава гледа на Биткоин кроз другачију призму, извлачећи лекције које би могле бити научене испитивањем те чудне мреже из другачијег угла.

Глава 1 истражује филозофске поуке Биткоина. Међуигру неизменљивости и промене, концепт истинске недовољности, Биткоинову концепцију без мане, проблем идентитета, контрадикцију копирања и локалитета, снагу слободног говора, и границе сазнања.

Глава 2 истражује економске поуке Биткоина. Лекције о финансијском незнању, инфлацији, вредности, новцу и историји новца, банкарству фракционих резерви, и како Биткоин поново уводи здрав новац на лукав, заобилазан начин.

Глава 3 истражује неке од лекција које су научене кроз испитивање технологије Биткоина. Зашто у бројевима лежи снага, размишљања о поверењу, зашто одређивање времена захтева рад, зашто је споро кретање и неломљење ствари особина, а не баговање, шта нам стварање Биткоина може рећи о приватности, зашто сајферпанкови пишу кодова (а не законе), и које би метафоре могле бити корисне да се истражи будућност Биткоина.

Свака лекција садржи неколико цитата и линкова током самог текста. Ако сам неку идеју истражио са више детаља, можете наћи линкове за моје сродне радове у одељку „Иза огледала”. Ако желите да идете дубље, линкови за релевантнији материјал су уређени у одељку „Низ зечју рупу”. Оба одељка можете наћи на крају сваке лекције.

Иако је неко претходно знање о Биткоину од користи, надам се да ове лекције може савладати сваки радознао читалац. Иако се неке надовезују једну на другу, свака лекција би требало да може да стоји сама и да се може читати независно. Дао сам све од себе да се склањам од техничког жаргона, мада је неки речник специфичан за овај домен ипак неизбежан.

Надам се да ће моје писање послужити као инспирација за друге да се копају испод површине и испитају нека од дубљих питања која Биткоин покреће. Моја сопствена

инспирација дошла је од великог броја аутора и стваралаца садржаја којима сам свима вечито захвалан.

Последње, али не и најбезначајније: мој циљ у писању овога није да вас убедим у било шта. Мој циљ је да вас натерам да размишљате, и да вам покажем да у Биткоину има много више од онога што одмах пада у очи. Ја чак не могу ни да вам кажем шта је Биткоин и чему ће вас Биткоин научити. То ћете морати да откријете сами.

„После овога, нема кајања. Узмеш ли плаву пилулу— прича се завршава, ти се будиш у свом кревету и верујеш у шта год желиш да верујеш. Узмеш ли црвену пилулу— остајеш у Земљи чуда, и ја ти показујем колико се дубоко пружа зечја рупа.”

-Морфеус

Глава 1: Филозофија

Миш је погледао у њу прилично љубопитљиво, и њој је изгледало да је намигнуо једним од својих малих очију, али није рекао ништа.

Гледајући на Биткоин површно, човек би закључио да је он спор, неисплатив, непотребно сувишан, и изнад свега параноидан. Гледајући на Биткоин љубопитљиво, човек би могао открити да ствари нису оне какве изгледају на први поглед.

Биткоин има начин да узмете ваше претпоставке и да их окренете наглавачке. Мало после, баш када сте почели поново да се осећате удобно, биткоин ће провалити кроз зид баш као бик у продавници порцелана и још једном ће развејати ваше претпоставке.

Слепи монаси проучавају Биткоинског слона

Биткоин је дете многих дисциплина. Као и слепи монаси који проучавају слона, свако ко приђе овој новој технологији чини то из другачијег угла. Свакако ћу доћи до другачијих закључака о природи ове звери.

Следе лекције о неким од мојих претпоставки које је биткоин развејао, и о закључцима до којих сам дошао. Филозофска питања неизменљивости, недовољности, локалитета, и идентитета истражују се у прве четири лекције.

- Лекција 1: Неизменљивост и промена
- Лекција 2: Недовољност недовољности
- Лекција 3: Копија и локалитет
- Лекција 4: Проблем идентитета
- Лекција 5: Концепција без мане
- Лекција 6: Снага слободног говора
- Лекција 7: Границе сазнања

Лекција 5 истражује како је прича о пореклу Биткоина није само фасцинантна већ апсолутно неопходан за безлидерски систем. Последње две лекције ове главе истражују снагу слободног говора и границе индивидуалног сазнања, изражене кроз изненађујућу дубину биткоинске зечје рупе.

Надам се да ће за вас свет Биткоина бити поучан, фасцинантан и забаван као што је за мене био, и још увек јесте. Позивам вас да пратите белог зеца и истражите дубине зечје рупе. А сада држите свој џепни сат, ускочите, и уживајте у паду.

Лекција 1: **Неизменљивост и промена**

Питам се да ли сам се изменила током ноћи. Чекај да размислим. Јесам ли била иста када сам устала јутрос? Скоро да мислим да могу да сетим да сам се осећала мало другачије. Али ако нисам иста, следеће питање је „Ко сам ја за име света?“ Ах, то је та велика загонетка!

Биткоин је суштински тежак за описивање. Он је новост, и било који покушај да се повуче паралела са претходним концептима — било називајући га дигиталним златом било интернетом новца — осуђен је да га не обухвати потпуно. Која год је била ваша омиљена аналогија, два аспекта Биткоина су апсолутно основна: децентрализација и неизменљивост.

Један начин да се размишља о Биткоину је да је он компјутеризовани друштвени уговор. Софтвер је само један део загонетке, и онда ће се Биткоин изменити мењањем софтвера једна вежба узалудности. Човек би морао да убеди остатак мреже да прихвати промене, што је више психолошки напор него напор софтверског инжењеринга.

Ово што следи могло би да испрва звучи апсурдно, као и многе друге ствари у овом простору, али верујем да је ипак дубоко истинито: Ви нећете променити Битоин, али ће Биткоин променити вас.

“Биткоин ће мењати нас више него ми њега.”
Марти Бент

Требало ми је много времена да схватим дубину овога. Пошто је Биткоин само софтвер и све у њему је отвореног кода, можете једноставно мењати ствари како хоћете, тачно? Погрешно. Врло погрешно. Немало изненађујуће, креатор Биткоина знао је све ово врло добро.

Природа Биткоина је таква да једном када је пуштена верзија 0.1, његов основни нацрт уклесан је у камену за остатак његовог живота.
Сатоши Накамото

Многи људи покушали су да измене природу Биткоина. До сада нико није успео. Иако постоји читаво море форкова и алткоина, мрежа биткоина и даље врши свој посао, као што је то радила и када се први компјутер укључио у њу.

Алткоини ће бити небитни на дуге стазе. Форкови ће на крају умрети од глади. Биткоин је оно што је битно. Све док се наше темељно разумевање математике и/или физике не промени, Биткоинов Honeybadger живеће и даље без бриге.

“Биткоин је први пример нове форме живота. Он живи и дише на интернету. Он живи зато што може да плати људима да га одржавају живим. […] Он се не може променити. Са њим се не може расправљати. Њега не можеш чачкати. Не може се искварити. Не може се зауставити. […] Ако би нуклеарни рат уништио пола наше планете, он би наставио да живи, неискварен.”
Ралф Меркл

Откуцај срца биткоинове мреже наџивеће све наше откуцаје.

Горе наведена спознаја променила ме је далеко више него што ће пређени блокови Биткоиновог блокчејна икада учинити. Променила је моје одабирање тренутка, моје разумевање економије, моје политичке погледе, и још толико много тога. Đavola, ona čak ljudima мења и начин исхране. Ако вам све ово звучи блесаво, у добром сте друштву. Све ово и јесте блесаво, а ипак се догађа.

Биткоин ме је научио да се неће променити. Ја хоћу.

Иза огледала 🔍
Pratite članke koji razvijaju ideje o kojima se raspravlja u ovoj lekciji:
- 🔍 Bitcoin's Gravity - How idea-value feedback loops are pulling people in
- 🔍 Proof of Life - Why Bitcoin is a Living Organism
- 🔍 The Bitcoin Journey

Низ зечју рупу
- There is no Bitcoin 2.0 од Пита Душанског
- DAOs, Democracy and Governance од Ралфа Ц. Меркла
- Inside the World of the Bitcoin Carnivores - Why a small community of Bitcoin users is eating meat exclusively од Џордана Пирсона
- Unpacking Bitcoin’s Social Contract од Хасуа
- Bitcoin is a Decentralized Organism од Брендона Квитема
- Bitcoin is a Social Creature од Брендона Квитема
- Bitcoin - Two Parts Math, One Part Biology од Хуга Нгујена
- It’s the settlement assurances, stupid од Ника Картера
- Technical Discussion on Bitcoin’s Transactions and Scripts од Сатошија Накамота, Гавина Андресена, и других

- Marty’s Bent - A daily newsletter highlighting signal in Bitcoin од Мартија Бента
- Tales From the Crypt од Мартија Бента
- John Vallis & Richard James & Gigi Der & Robert Breedlove on Bitcoin as The Future of Money
  JBP#440 домаћин Џордан Б. Питерсон
- Antifragile - Things That Gain From Disorder од Насима Николаса Талеба

Лекција 2: Недовољност недовољности

То је сасвим довољно – надам се да нећу више да растем…

Уопште говорећи, изгледа да напредак технологије чини ствари обилнијим. Све више и више људи могу да уживају у ономе што је претходно било луксузна роба. Ускоро, сви ћемо живети као краљеви. Многи од нас већ и живе тако. Како је Питер Дијамандис написао у Изобиљу:„Технологија је механизам ослобађања ресурса. Она може да претвори једном оскудно у данас обилно."

Биткоин, сам по себи усавршена технологија, прекида тај тренд и ствара ново добро којег истински нема довољно. Неки чак тврде да је то једна од најнедовољнијих ствари у васиони. Залихе се не могу увећати, без обзира колико напора одлучимо да потрошимо да бисмо створили више.

„Само две ствари су истински недовољне: време и биткоин."
Сајфедин Амоус

Парадоксално, он то постаје механизмом копирања. Трансакције се објављују, блокови се умножавају, децентрализована евиденција је – па, погодили сте – децентрализована. То су све само маштовити називи за копирање. Ма, Битокоин чак копира и сам себе у највећи могући број компјутера, подстичући појединце да користе пуне чворове и да рударе нове блокове.

Све ово прављење дупликата изванредно функционише заједно, у усаглашеном напору да произведе недовољност.

У времену обиља, биткоин ме је научио шта је то права недовољност.

Низ зечју рупу

- Modeling Bitcoin's Value with Scarcity од PlanB
- Bitcoin Can't Be Copied од Паркера Луиса
- Presentation on The Bitcoin Standard од Сајфедина Амоуса
- 🎧 Misir Mahmudov on the Scarcity of Time and Bitcoin
  TFTC#60 домаћин Марти Бент
- 🎧 BTCDCA on Dollar Cost Averaging Bitcoin
  BEC#20 домаћин Колин
- 🎧 Misir Mahmudov on Bitcoin as Stored Time
  OTC#126 домаћин Помп
- 🎧 Hass McCook on the importance of Auto-DCA
  SLP#288 домаћин Стефан Ливера

- Abundance - The Future is Better Than You Think од Питера Дијамандис
- The Bitcoin Standard - The Decentralized Alternative to Central Banking од Сајфедина Амоуса

Лекција 3: Копија и локалитет

Затим се зачу љутити глас — зечев—"Пат, Пат! где си ти?"

Ако оставимо по страни квантну механику, локалитет није проблем у физичком свету. На питање „Где је ‘X’?“ може се одговорити на смислен начин, без обзира да ли је ‘X’ особа или предмет. У дигиталном свету, питање где је већ само по себи проблематично, али на њега није немогуће одговорити. Где су ваши и-мејлови, заиста? Лош одговор био би “у клауду”, јер је то само неки други компјутер.

Ипак, ако желите да уђете у траг сваком уређају за складиштење информација које имате у себи ваше и-мејлове, могли бисте их, теоријски, лоцирати.

Код биткоина, питање „где” је заиста проблематично. Где су, тачно, ваши биткоини?

„Отворио сам очи, погледао около, и поставио оно неизбежно, традиционално, жалосно отрцано постоперативно питање: „Где сам ја?”
Данијел Денет

Проблем је двострук: Прво, децентрализована евиденција трансакција је расподељена пуним копирањем, што значи да је евиденција свуда. Друго, биткоини не постоје. Не само физички, него и технички. Биткоин чува траг о скупу непотрошених трансакцијских излаза, а да уопште не мора да се позове на неки ентитет који представља биткоин. О постојању биткоина закључује се осматрањем скупа непотрошених трансакционих излаза и називањем сваког уноса са 100 милиона базних јединица биткоином.

„Где је он сада, у овом тренутку, у транзиту? […] Прво, биткоина нема. Њих просто нема. Они не постоје. Они су евиденцијски уноси у евиденцији која је заједничка […] Они не постоје ни на једној физичкој локацији. Та евиденција постоји на свакој физичкој локацији, у принципу. Географија овде нема смисла —она ти неће помоћи да смислиш своју стратегију у овом случају.”
Питер Ван Фолкенберх

Дакле, шта ти поседујеш када кажеш “Ја имам биткоин” када биткоина нема? Па, сети се свих оних чудних речи које си био приморан да запишеш поред новчаника који си користио? Испада да су те магичне речи оно што поседујеш: мађијске чини које се могу употребити да се додају неки уноси у јавну евиденцију – кључеви да се „покрену” неки биткоини. Због тога, за све намере и сврхе, твоји приватни кључеви јесу твоји биткоини. Ако мислиш да све ово измишљам слободно ми пошаљи своје приватне кључеве.

Биткоин ме је научио да је локалитет пипава
ствар.

Иза огледала 🔍

Пратите чланке који развијају идеје о којима се расправља у овој лекцији:
🔍 The Magic Dust of Cryptography - How digital information is changing our society

Низ зечју рупу

- Where Am I? од Данијела Денета
- 🎧 Peter Van Valkenburg on Preserving the Freedom to Innovate with Public Blockchains
  WBD#49 домаћин Питер Мек Кормак

Лекција 4: Проблем идентитета

"Ко смо ми?" рече гусеница.

Ник Картер, као омаж у односу који је Томаш Најџел имао према истом питању када се тицало слепог миша, написао је изврсну ствар која расправља о следећем питању: Како је то бити биткоин? Он је бриљантно показао да отворени јавни блокчејни уопште, а Биткоин посебно, пате од исте загонетке као и Тезејев брод: који биткоин је прави биткоин?

„Узмите у обзир колико кратко опстају Биткоинове компоненте. Цела база кодова је била прерађена, измењена, и проширена толико да једва да подсећа на своју оригиналну верзију. […] Регистар о томе шта поседује, сама евиденција трансакција, је буквално једини трајан траг ове мреже […] Да би се сматрало да сте заиста без лидера, морате одустати од лаког решења да имате један ентитет који може да прогласи један ланац за онај легитимни."
Ник Картер

Изгледа да наш напредак технологије непрестано присиљава да узмемо озбиљно ова филозофска питања. Раније или касније, самоходна возила биће суочена са верзијама тролејбуског проблема у стварном свету, које ће их присиљавати да доносе етичке одлуке о томе чији животи су битни а чији нису.

Криптовалуте, посебно после првог спорног тврдог форка, приморавају нас да размишљамо и да се споразумевамо по питању метафизике идентитета. Занимљиво, два највећа проблема која смо до сада имали, одвела су до два различита одговора.

Првог августа, 2017, Биткоин се расцепио у два табора. Тржиште је одлучило да је неизмењени ланац оригинални Биткоин. Годину дана раније, 25-ог октобра, 2016, Етереум се расцепио у два табора. Тржиште је одлучило да је измењени ланац оригинални Етереум.

Ако се исправно децентрализују, питања која је поставио Тезејев брод мораће непрестано да добијају одговоре онолико дуго колико ове мреже за трансфер вредности постоје. Биткоин ме је научио да децентрализација противречи идентитету.

Низ зечју рупу

- What Is It Like to be a Bat? Од Томаша Нејџела
- What is it like to be a Bitcoin? Од Ника Картера
- Ship of Theseus од аурора Википедиа
- Trolley Problem од аурора Википедиа
- 🎧 Giacomo Zucco on Bitcoin's Identity and Copycats
  SLP#75 домаћин Стефан Ливера
- The Blocksize War - The Battle for Control over Bitcoin’s Protocol Rules од Џонатана Бира

Лекција 5: Концепција без мане

"Немају главе," узвикнуше војници у одговор...

Свако воли добру причу о почетку. Прича о почетку Биткоина је фасцинантна, а њени детаљи су важнији него што би човек прво помислио. Ко је Сатоши Накамото? Да ли је он био једна особа или група људи? Да ли је он био она? Ванземаљац који путује кроз време, или усавршена вештачка интелигенција? И кад одбацимо луде теорије, вероватно никада нећемо знати.

Сатоши је одабрао да буде анониман. Он је посејао семе Биткоина. Остао је у близини довољно дуго да се увери да мрежа неће умрети у детињству. А онда је нестао.

Оно што је можда изгледало као шашава завера анонимности уствари је кључно за истински децентрализован систем. Нема централизоване контроле. Нема централизованог ауторитета. Нема творца. Нема никога кога ћемо законски гонити, терорисати, уцењивати или од кога ћемо изнуђивати. Технолошка концепција без мане.

“Једна од највећих ствари које је Сатоши извео јесто то што је нестао.”
Џими Сонг

Од рођења Биткоина, створене су хиљаде криптовалута. Ниједан од ових клонова нема његову причу о почетку. Ако хоћете да престигнете Биткоин, морате да превазиђете његову причу о почетку. У рату идеја, добре приче диктирају преживљавање.

“Злато је први пут обликовано у накит и употребљено за трговину пре више од 7000 година. Заводнички сјај злата довео је до мишљења да је то дар од богова.“
Злато: Тај необични метал

Као и злато у древним временима, Биткоин би се могао сматрати даром од богова. За разлику од злата, корени Биткоина су сасвим људски. А овог пута, ми знамо ко су богови развоја и одржавања: људи широм целог света, анонимни или не.
Биткоин ме је научио да су добре приче важне.

Низ зечју рупу

- Catallaxy - the origins of Bitcoin, innovation and spontaneous order од Франсиса Пулиоа
- Why Bitcoin is Different од Џимија Сонга
- Only The Strong Survive од Алена Фарингтона и Великог Ала
- Against Cryptocurrency - The Ethical Argument for Bitcoin Maximalism од Пита Рицоа

- Gold - The Extraordinary Metal од Аустријске ковнице
- Robert Breedlove on Bitcoin and the Number Zero
  TFTC#162 домаћин Марти Бент
- The Black Swan - The Impact of the Highly Improbable од Насима Николаса Талеба

Лекција 6: Снага слободног говора

“Опростите?” рече миш, мрштећи се, али врло учтиво, “рекли сте нешто?”

Биткоин је идеја. Једна идеја која, у садашњој форми, представља манифестацију машинерије која ради искључиво на текст. Сваки аспект Биткоина је текст. Бела књига је текст. Софтвер којим управљају његови чворови је текст. Евиденција трансакција је текст. Трансакције су текст. Јавни и приватни кључеви су текст. Сваки аспект Биткоина је текст, и тиме је еквивалентан говору

“Конгрес неће доносити законе који се тичу успостављања религије, или забрањивања њеног слободног упражњавања; или ускраћивања слободе говора, или штампе; или права људи да се мирно окупе, и да уложе петицију Влади ради решавања њихових тешкоћа.”

Први амандман устава Сједињених држава

Иако се коначна битка Крипторатова још није одиграла, биће тешко прогласити криминалном једну идеју, а поготово не идеју која се базира на размени текстуалних порука. Сваки пут када нека влада покуша да стави ван закона текст или говор, ми склизнемо на стазу апсурда која неизбежно води до ужасних ствари као што су илегални бројеви или илегални прајмови.

Докле год постоји део света у коме је говор слободан као у *слободи*, Биткоин је незаустављив.

“Нема поенте у било којој трансакцији са Биткоином у којој Биткоин престаје да буде *текст*. Он је *сав текст*, све време […] Биткоин је текст. Биткоин је говор. Он се не може регулисати у слободној земљи какве су САД са гарантованим неотуђивим правима и Првим амандманом који експлицитно искључује чин публиковања из владиног надзора.”

Бјутион

Биткоин ме је научио да су у слободном друштву, слободни говор и слободни софтвер назаустављиви.

Иза огледала 🔍
Пратите чланке који развијају идеје о којима се расправља у овој лекцији:

- 🔍 The Rise of the Sovereign Individual - How power is re-aligning itself in an internet-native world
- 🔍 How to Kill Bitcoin
- 🔍 Bitcoin's Habitats - How Bitcoin is surviving and thriving between worlds
- 🔍 Implications of Outlawing Bitcoin

Низ зечју рупу

- Why America Can't Regulate Bitcoin од Бјутион
- Why Bitcoin Matters for Freedom од Алекса Гледстајна
- A most peaceful revolution од Ника Картера
- Bitcoin Cannot Be Banned од Паркера Луиса
- Can Governments Stop Bitcoin? од Алекса Гледстајна
- Crypto Wars од сарадника Википедије
- Illegal Numbers од сарадника Википедије
- Illegal Primes од сарадника Википедије
- First Amendment to the United States Constitution од сарадника Википедије
- 🎧 Jameson Lopp on Freedom-Enabling Technologies like Bitcoin
  TFTC#29 домаћин Марти Бент
- 🎧 Alex Gladstein on Bitcoin's Role in the Fight for Human Rights
  TFTC#76 домаћин Марти Бент

Лекција 7: Границе сазнања

Доле, доле, доле. Зар се пад никад неће завршити?

Улажење у Биткоин је понижавајуће искуство. Мислио сам да знам ствари. Мислио сам да сам образован. Мислио сам да познајем своју компјутерску науку, у најгорем случају. Изучавао сам је годинама, тако да сам морао да знам све о дигиталним потписима, хашевима, енкрипцијама, операционој безбедности, и мрежама, тачно?

Погрешно.

Тешко је научити све фундаменталне ствари које омогућавају да Биткоин ради. Разумети их све до краја је на граници немогућег.

“Нико није открио дно зечје рупе Биткоина.”
Џејмсон Лоп

Мој списак књига за читање шири се далеко брже него што ја могу да их прочитам. Списак новина и чланака које треба прочитати је буквално бескрајан. Има више подкаста о свим овим темама него што бих ја икада могао да саслушам. Уз то, Биткоин еволуира и скоро је немогуће остати ажуриран са све већом брзином иновација. Прашина још није пала на први ниво, а људи су већ направили други ниво и раде на трећем.

Биткоин ме је научио да ја о скоро свему знам врло мало. Научио ме је да је ова зечја рупа без дна.

Иза огледала 🔍
Пратите чланке који развијају идеје о којима се расправљало у овој лекцији:

- 🔍 Bitcoin's Eternal Struggle - How Bitcoin Thrives on the Edge between Order and Chaos

Низ зечју рупу

- Bitcoin Information & Resources од Џејмсона Лопа
- Bitcoin Literature од Института Сатоши Накамото
- Educational Resources од Bitcoin Only
- Bitcoin Intro од 6102bitcoin
- 🎧 Matt Corallo on how Everyone is Ignorant when it comes to Bitcoin
  TFTC#7 домаћин Марти Бент
- 🎧 Ben Prentice on the Bitcoin Spectrum
  BEC#14 домаћин Колин

Глава II: Економија

Велико ружино дрво стајало је поред улаза у башту: руже на њему биле су беле, али ту су била три баштована, журно их бојећи у црвено. Алиси се ово учинило врло чудно…

Новац не расте на дрвећу. Глупо је веровати у то да расте, а наши родитељи су се потрудили да ми то знамо, тако што су ту изреку понављали као мантру. Подстицали су нас да користимо новац мудро, да га не трошимо неозбиљно, и да га чувамо у добрим временима да би нам помогао у црним данима. Новац, најзад, не расте на дрвећу.

Биткоин ме је о новцу научио више него што сам икада мислио да би требало да знам. Преко њега, ја сам био присиљен да истражим историју новца, банкарства, разних школа економске мисли, и многе друге ствари. Та потрага за разумевањем Биткоина довела ме је до мноштва путева, од којих неке покушавам да испитам у овој серији.

У првих седам лекција расправљало се о неким од филозофских питања која Биткоин дотиче. Следећих седам лекција ће дати ближи увид у новац и економију.

- Лекција 8: Финансијско незнање
- Лекција 9: Инфлација
- Лекција 10: Вредност
- Лекција 11: Новац
- Лекција 12: Историја и пропаст новца
- Лекција 13: Лудило фракционе резерве
- Лекција 14: Здрав новац

Опет, моћи ћу само да загребем површину. Биткоин није само амбициозан, већ такође и широк и дубок у свом подручју, што онемогућује да се покрију све релевантне теме у једној лекцији, есеју, чланку, или књизи.

Биткоин је нова форма новца, па је учење економије од прворазредног значаја за његово разумевање. Бавећи се природом људске активности и интеракцијама економских агената, економија је вероватно један од највећих и најнејаснијих комада Биткоинове слагалице.

И поново, ове лекције су истраживање разних ствари које сам научио од Биткоина. Оне су лични одраз мог путовања низ зечју рупу. Пошто немам подлогу из економије, ја сам дефинитивно изван своје зоне комфора и посебно сам свестан да је свако моје закључивање које можда имам, непотпуно. Даћу све од себе да представим шта сам научио, чак и ризикујући да од себе направим будалу. Најзад, ја и даље покушавам да одговорим на питање: *“Шта си научио од Биткоина?”*

После седам лекција испитаних кроз призму филозофије, хајде да употребимо призму економије да погледамо седам следећих. Овог пута могу понудити само економску класу. Крајње одредиште: **здрав новац**.

Лекција 8: Финансијско незнање

Ала ће ме она сматрати за незналицу ако будем питала! Не, никако неће ићи да је питам: можда ћу то видети негде написано.

Једна од ствари која ме је највише изненадила, била је количина финансија, економије и психологије потребна да се схвати смисао онога што на први поглед изгледа као чисто *технички* систем – једна компјутерска мрежа. Да парафразирам малог момка са длакавим табанима: "То је опасан посао, Фродо, улазак у Биткоин. Прочиташ белу књигу, и ако не стојиш чврсто, бог зна у ком правцу можеш бити одуван"

Да би разумео нови монетарни систем, мораш се упознати са старим. Почео сам да схватам врло рано да је количина финансијског образовања коју сам имао прилике да добијем у образовном систему у суштини *нула*.

Као неки петогодишњак, почео сам да постављам себи многа питања: Како ради банкарски систем? Како ради берза? Шта је то фиат новац? Шта је то *исправан* новац? Зашто има толико дуга? Колико новца се заиста штампа и ко одлучује о томе?

После благе панике због самог распона мог незнања, нашао сам утеху у спознаји да сам у добром друштву.

"Зар није иронично да ме је Биткоин научио више о новцу него све ове године које сам провео радећи за финансијске институције?... укључујући почетак моје каријере у централној банци"
aarontaycc

"Научио сам више о финансијама економији, технологији, криптографији, људској психологији, политици, теорији игара, законодавству, и себи у последњих три месеца са криптом него у последње три и по године колеџа"
bitcoindunny

Ово су само два од много признања широм твитера. Биткоин, као што смо истражили у Лекцији 1, јесте жива ствар. Мизес је заступао мишљење да је и економија жива ствар. А као што сви знамо из личног искуства, живе ствари су саме по себи тешке за разумевање.

“Систем науке је само једна станица у бескрајно напредујућој потрази за знањем. Он је нужно под утицајем недостатности која је својствена сваком људском напору. Али признавање ових чињеница не значи да је данашња економија назадна. То једноставно значи да је економија жива ствар – а живети значи истовремено несавршеност и промену.”
Лудвиг фон Мизес

Ми сви читамо о разним финансијским кризама у вестима, питамо се како та велика спасавања функционишу и збуњујемо се над чињеницом да изгледа да се нико никада не сматра одговорним за штету која је у трилионима. Ја сам још увек збуњен, али бар почињем да хватам неки наговештај тога што се дешава у свету финансија.

Неки људи чак иду тако далеко да приписују опште непознавање ових тема системском, намерном незнању.

Док су историја, физика, биологија, математика и језици сви део нашег образовања, свет новца и финансија се, што је изненађујуће, истражује само површно, или нимало. Питам се да ли би људи и даље били вољни да нагомилају онолико дуга колико то тренутно раде када би сви били упућени у личне финансије и у то како функционишу новац и дугови. Онда се упитам колико слојева алуминијума чине један ефикасан шешир од станиола.[1] Вероватно три.

“Ови сломови, ова спасавања, нису случајни. А није случајно ни да нема финансијског образовања у школи. […] То је предумишљај. Као што пре Грађанског рата није било дозвољено школовати роба, нама није дозвољено да учимо о новцу у школи.”
Роберт Кијосаки

Као и у Чаробњаку из Оза, говоре нам да не обраћамо пажњу на човека иза завесе. За разлику од Чаробњака из Оза, ми сада имамо стварно чаробњаштво: отпорну на цензуру, отворену, неограничену мрежу трансфера вредности. Нема завесе, а магија је видљива свакоме.
Биткоин ме је научио да гледам иза завесе и суочим се са својим финансијским незнањем.

[1] За овај шешир се веровало да штити од електромагнетних таласа и даљинске контроле ума

Низ зечју рупу

- Why the Rich are Getting Richer од Роберта Кијосакија
- 🎧 Stephan Livera - Intro to Bitcoin Austrian thought
  SLP#71 домаћин Стефан Ливера
- 📚 Economic Depressions - Their Cause and Cure од Марија Н. Ротбарда
- 📚 Human Action од Лудвига фон Мизеса

Лекција 9: Инфлација

Драга моја, сада морамо трчати што брже можемо, само да бисмо остале на месту. А ако хоћеш да одеш било где, мораш трчати два пута брже од тога.

Покушај да разумем монетарну инфлацију, и како би не-инфлаторни систем као Биткоин могао да промени начин на који радимо ствари, био је полазна тачка моје авантуре у економији. Знао сам да је инфлација брзина којом се прави нови новац, али нисам знао баш много даље од тога.
Иако неки економисти заступају став да је инфлација добра ствар, други сматрају да "тврд" новац који не може лако подлећи инфлацији – какав смо имали у време златног стандарда – јесте суштински важан за здраву економију. Биткоин, који има фиксиране резерве од 21 милиона, слаже се са овим другим табором.

Обично, ефекти инфлације нису одмах видљиви. Зависно од стопе инфлације (као и других фактора) период између узрока и последице може бити неколико година. Не само то, већ инфлација погађа различите групе људи више него друге.

Како Хенри Хезлит указује у Економији у једној лекцији:

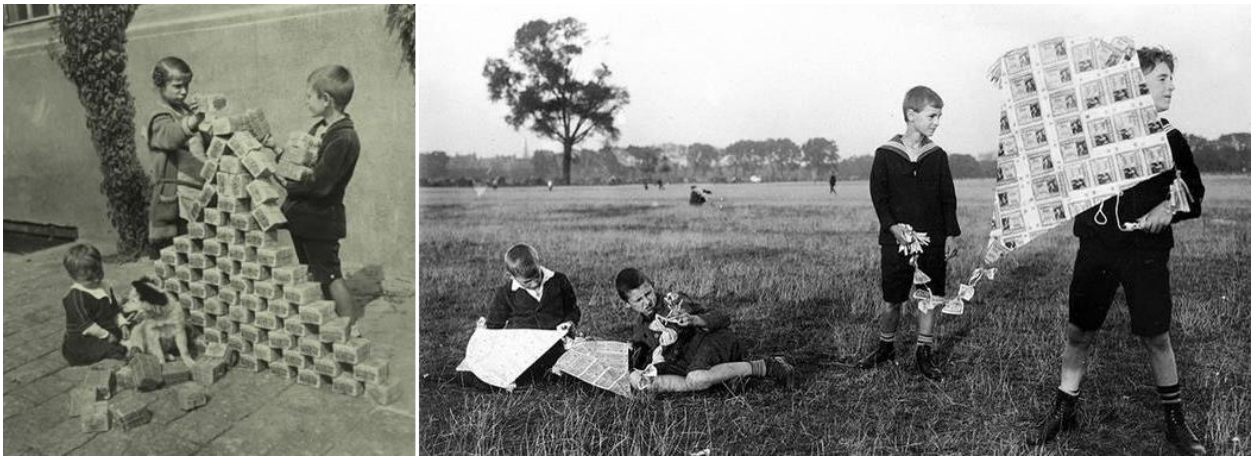
"Уметност економије састоји се не само у гледању у непосредни већ и у дуготрајније ефекте било ког поступка или политике; она се састоји у праћењу последица те политике не само на једну групу већ на све групе."

Један од мојих личних тренутака паљења сијалице била је спознаја да емитовање нове валуте – штампање још новца – представља потпуно различиту економску активност од свих других економских активности. Док стварна добра и стварне услуге производе стварну вредност за стварне људе, штампање новца ефикасно чини супротно: оно одузима вредност од свакога ко поседује новац који се инфлатира.

"Сама инфлација—то јест, само издавање додатног новца, са последицом виших зарада и цена —може изгледати као стварање додатне потражње. Али у терминима стварне производње и размене стварних ствари, она то није."
Хенри Хезлит

Деструктивна снага инфлације постаје очигледна чим се мала инфлација претвори у *много* инфлације. Ако новац хиперинфлатира, ствари врло брзо постану ружне. Кад се валута која је у инфлацији распадне, она неће моћи да депонује вредност током времена и људи ће потрчати да се домогну било ког добра које би то могло.

Наредна последица инфлације је да ће сав новац који су људи уштедели током свог живота практично нестати. Папирни новац у вашем новчанику и даље ће бити тамо, наравно. Али биће управо то: безвредни папир.



Хиперинфлација у Вајмарској републици (1921-1923)

Новцу опада вредност и у такозваној "млакој" инфлацији. Само се то дешава довољно споро да већина људи не примећује смањивање своје куповне моћи. А једном када се штампарске пресе пусте у рад, валута лако може да доживи инфлацију, и оно што је била млака инфлација може да се претвори у шољу јаке инфлације притиском дугмета. Како Фридрих Хајек указује у једном од својих есеја, млака инфлација обично доводи до неувијене инфлације.

"Млака" упорна инфлација не може помоћи —она само може довести до неувијене инфлације."
Фридрих Хајек

Инфлација је посебно покварена јер фаворизује оне који су ближи штампарским пресама. Новостворено новцу потребно је време да процирку лише и ценама да се прилагоде, тако да ако сте у стању да шчепате више новца пре него што новац свих осталих изгуби вредност, ви сте испред инфлаторне криве. Због овога се на инфлацију може гледати и као на скривени порез јер на крају влада профитира од ње док сви остали заврше тако што плаћају цену.

"Мислим да није претеривање ако кажем да је историја већином историја инфлације, и то обично инфлације коју планирају владе ради добитка влада."
Фридрих Хајек

До сада, све валуте које су контролисале владе на крају су замењене или су потпуно пропале. Без обзира како је мала стопа инфлације, "стабилан" раст је само други начин да

се каже експоненцијални раст. У природи као и у економији, сви системи који расту експоненцијално на крају ће морати да се устале на неком нивоу или да доживе катастрофалнии слом.

“То не може да се догоди у мојој земљи,” је оно што вероватно мислите. Не мислите то ако сте из Венецуеле, која тренутно пати од хиперинфлације. Са стопом инфлације од преко милион процената, новац је просто безвредан.

То се можда неће догодити у следећих пар година, или неће оној валути која се користи у вашој земљи. Али један поглед на листу историјских валута показује да ће се то неизбежно десити кроз довољно дуг временски период. Памтим и користо сам многе од наведених: аустријски шилинг, немачку марку, италијанску лиру, француски франак, ирску фунту, хрватски динар, итд. Моја бака користила је чак аустроугарску круну. Како време иде, валуте које су тренутно у употреби ће полако али сигурно да се приближавају својим гробљима. Или ће доживети хиперинфлацију или ће бити замењене. Ускоро ће то бити историјске валуте. Учинићемо их превазиђеним.

“Историја је показала да ће државе неизоставно подлећи искушењу да направе инфлацију залиха новца.” Сајфедин Амоус

Зашто је Биткоин другачији? За разлику од валута које су одредиле владе, монетарна добра која не регулишу владе, већ закони физике, имају тенденцију да преживе и чак држе своју одговарајућу вредност током времена. До сада најбољи пример за ово је злато, које, како то показује пригодно назван *однос Злато према пристојном оделу*, држи своју вредност стотинама и чак хиљадама година. Оно можда неће бити савршено „стабилно“ – што је пре свега један сумњив концепт – али ће вредност коју држи бити бар у истом реду величина.

Ако монетарно добро или валута држи добро своју вредност у времену и простору, сматра се да је *тврдо*. Ако не може да држи своју вредност, јер се лако поквари или доживи инфлацију, сматра се *меком* валутом. Концепт тврдоће је од суштинског значаја да се разуме Биткоин и заслужује више од темељног испитивања. Вратићемо му се у последњој економској лекцији: здравом новцу.

Све више и више земаља пати од хиперинфлације, све више и више људи мора да се суочи са стварношћу тврдог и меког новца. Ако будемо имали среће, можда ће чак и неки од централних банкара бити приморани да ревидирају своје монетарне политике. Што год би могло да се деси, ствари које сам сагледао захваљујући Биткоину вероватно ће бити непроцењиве, без обзира какав буде исход.

Биткоин ме је научио о скривеном порезу инфлације и катастрофи хиперинфлације.

Иза огледала 🔍
Пратите чланке који развијају идеје о којима се расправљало у овој лекцији:

- 🔍 Bitcoin Boots on the Ground - Venezuela

Низ зечју рупу

- Economic Crisis in Venezuela од сарадника Википедије
- Hyperinflation од сарадника Википедије
- List of Currencies од сарадника Википедије
- List of Historical Currencies од сарадника Википедије
- 🎧 Ben Prentice & Heavily Armed Clown on WTF Happened in 1971?
  TFTC#157 домаћин Марти Бент
- 🎧 Saifedean Ammous & George Gammon on Inflation, Deflation, and The Bitcoin Standard
  SSL#23 домаћин Брејди Свенсон
- 📚 1980S Unemployment And The Unions - Essays on the Impotent Price Structure of Britain and Monopoly in the Labour Market од Фридриха фон Хајека
- 📚 Economics In One Lesson од Хенрија Хезлита
- 📚 Good Money, Part 2 - The Standard од Фридриха фон Хајека
- 📚 When Money Dies - The Nightmare of Deficit Spending, Devaluation, and Hyperinflation in Weimar, Germany од Адама Фергусона

Лекција 10: Вредност

Био је то бели зец, који је поново полако каскао натраг, и успут гледао забринуто око себе,као да је изгубио нешто...

Вредност је помало парадоксална, и постоје многе теорије које покушавају да објасне зашто вреднујемо одређене ствари више него друге. Људи су били свесни овог парадокса хиљадама година. Како је Платон написао у своме дијалогу са Еутидемусом, ми вреднујемо неке ствари зато што су ретке, а не само на основу њихове неопходности за наше преживљавање.

“И ако си обазрив даћеш овај исти савет и својим ученицима—да никада не разговарају ни са ким осим са тобом и између себе. Јер оно што је ретко, Еутидемусе, то је драгоцено, док је вода најјевтинија, иако је најбоља, како је то рекао Пиндар.”

Платон

Овај парадокс вредности показује нешто занимљиво о нама људима: изгледа да вреднујемо ствари на субјективној бази, али са одређеним непроизвољним критеријумима. Нешто може бити драгоцено за нас из низа разлога, али ствари које вреднујемо, заиста имају одређене заједничке црте. Ако се нешто може ископирати врло лако, или ако је по природи изобилно, ми то не ценимо.

Изгледа да ми ценимо нешто ако га нема довољно (злато, дијаманти, време), ако се тешко или напорно производи, не може се заменити (стара фотографија вољене особе), корисно је на начин који нам омогућава да радимо ствари које иначе не бисмо могли, или комбинација свега тога, као што су велика уметничка дела.

Биткоин је све од горе наведеног: крајње је редак (21 милион), све је тежи за производњу (преполовљене награде), не може се заменити (изгубљен приватни кључ изгубљен је заувек), и омогућава нам да урадимо неке сасвим корисне ствари. Може се сматрати за најбољи алат за пренос вредности преко граница, буквално отпоран на цензуру и конфискацију током тог процеса, плус, он је само-суверени депо вредности, који дозвољава појединцима да депонују своје богатство независно од банака и влада, да наведем само то двоје.
Биткоин ме је научио да је вредност субјективна, али не и произвољна.

Низ зечју рупу

- Bitcoin Has No Intrinsic Value — and That’s Great од Конера Брауна
- Bitcoin Is Not Too Volatile од Паркера Луиса
- Bitcoin Is Not Backed By Nothing од Паркера Луиса
- Euthydemus од Платона
- Paradox of Value од сарадника Википедије
- Subjective Theory of Value од сарадника Википедије

- Theory of Value од сарадника Википедије
- Skin In The Game - Hidden Asymmetries in Daily Life од Насима Николаса Талеба

Лекција 11: Новац

"Кад сам био млад," рече мудрац, тресући својим седим увојцима,
"Одржавао сам све своје удове врло гипким,
Употребом ове масти, пет шилинга кутија—
Дозволи ми да ти продам неколико."

Шта је новац? Користимо га сваки дан, али ипак на то питање је изненађујуће тешко одговорити. Ми зависимо од њега на крупне и ситне начине, и ако га имамо сувише мало наши животи постају врло тешки. Ипак, ми ретко размишљамо о ствари која, како изгледа, чини да се свет окреће. Биткоин ме је приморавао да одговорим на ово питање поново и поново: Шта је дођавола новац?

У нашем "модерном" свету, већина људи ће вероватно помислити на комаде папира када говоре о новцу, иако је већина нашег новца само број на банковном рачуну. Ми већ користимо нуле и јединице као свој новац, па како је онда Биткоин другачији?

Биткоин је другачији јер је у његовој сржи другачији тип новца од новца који је тренутно у употреби. Да бисмо ово разумели морамо поближе да погледамо шта је то новац, како је то постао, и зашто су злато и сребро били коришћени у већем делу комерцијалне историје.

"У овом смислу, то је више типично за драгоцени метал. Уместо да се залихе мењају да би вредност остала иста, залихе су унапред одређене а вредност се мења."
Сатоши Накамото

Морске шкољке, злато, сребро, папир, биткоин. На крају, **новац је све оно што људи користе као новац,** без обзира на облик и форму, или њихов недостатак.

Новац је, као изум, генијалан. Свет без новца је болесно компликован: колико риба ће ми купити нове ципеле? Колико крава ће ми купити кућу? Шта ако ми сад тренутно ништа не треба али ми треба да се отарасим својих јабука које ће ускоро иструлити? Не треба вам много маште да схватите да је привреда заснована на размени излуђујуће неефикасна.

Велика ствар са новцем је да се може разменити за *било шта друго* – то је баш изум! Као што је Ник Забо бриљантно резимирао у *Излазак из шкољке: Порекло новца*, ми људи користили смо све врсте новца: огрлице направљене од ретких материјала као што је слоновача, шкољке, или посебне кости, разне врсте накита, а још касније ретке метале као што су сребро и злато.

Пошто смо лења створења каква јесмо, ми не размишљамо много о стварима које једноставно функционишу. Новац, за већину нас, функционише баш како треба. Као и са колима и са компјутерима, већина нас је приморана да мисли о унутрашњем раду ових ствари само ако се покваре. Људи који су посматрали како њихова животна уштеђевина нестаје због хиперинфлације знају вредност тврдог новца, као што и људи који су видели своје пријатеље и породицу како нестају због зверстава нацистичке Немачке и Совјетске Русије знају вредност приватности.

Код новца је важно то што је свеобухватан. Новац је половина сваке трансакције, што улива огромну моћ онима којима је у власти прављење новца.

“Када узмемо да је новац једна половина сваке комерцијалне трансакције и да цела цивилизација стоји или пада у зависности од квалитета свог новца, ми говоримо о једној застрашујућој моћи, оној која лети под окриљем ноћи. То је моћ да се изатка илузија која изгледа стварна све док траје. У томе је сама срж моћи Федералних резерви.”
Рон Пол

Биткоин мирно уклања ову моћ, пошто се ослобађа прављења новца и то чини без употребе силе.

Новац је прошао кроз вишеструке итерације. Већина итерација била је добра. Оне су поправиле наш новац овако или онако. Врло недавно, међутим, унутрашње функционисање нашег новца се искварило. Данас, скоро сав наш новац је једноставно направљен *ни из чега* од стране постојећих сила. Да бих разумео како је до овога дошло морао сам да сазнам о историји новца и његовој пропасти која је уследила.

Да ли ће бити потребна серија катастрофа или једноставно један монументални образовни напор да се исправи ово кварење остаје да се види. Молим се боговима здравог новца да буде ово друго.

Биткоин ме је научио шта је то новац.
Низ зечју рупу

- Shelling Out - The Origins of Money од Ника Сабоа
- Money, blockchains, and social scalability од Ника Сабоа
- The Bullish Case for Bitcoin од Вицаја Бојапатија
- Gradually, Then Suddenly од Паркера Луиса
- Masters and Slaves of Money од Роберта Бридлава
- 🎧 Tuur Demeester - Bitcoin 101
  TIP#244 домаћини Престон Пиш и Стиг Бродерсен

- 🎧 Conner Brown on the intersubjective nature of Bitcoin
  TFTC#87 домаћин Марти Бент
- 🎧 Parker Lewis - What is Money?
  WBD#183 домаћин Питер Мек Кормак
- 📚 End The Fed од Рона Пола
- 📚 What Has Government Done To Our Money од Марија Ротбарда

Лекција 12: Историја и пропаст новца

Нису хтели да упамте једноставна правила која су им њихови пријатељи задали, као што је да ако упаднеш у ватру, она ће те спалити, и да ако засечеш свој прст ножем врло дубоко, он ће обично крварити, а она никад није заборавила да ако пијеш из бочице означене са "отров", скоро је сигурно да ти неће пријати, раније или касније.

Многи људи мисле да је основа новца злато, које је закључано далеко у великим трезорима, заштићено дебелим зидовима. Ово је престало да буде истина пре много деценија. Нисам сигуран шта сам ја мислио, пошто сам био у много дубљој невољи, не знајући буквално ништа о злату, папирном новцу, или зашто пре свега нешто треба да буде основа за новац.

Један део сазнавања о Биткоину је сазнавање о fiat новцу: шта он значи, како је постао, и зашто то можда није најбоља идеја коју смо икада имали. Дакле, шта је тачно fiat новац? И како смо завршили користећи њега?

Ако је нешто наметнуто *fiat*-ом, то просто значи да је наметнуто званичним овлашћењем или прописом. Дакле, fiat новац је новац једноставно зато што *неко* каже да је то новац. Пошто све владе данас користе fiat валуте, тај неко је *ваша* влада. Нажалост, немате *слободу* да се не слажете са овим вредносним прописом. Ускоро ћете осетити да је овај пропис све осим не-насилан. Ако одбијете да користите ову папирну валуту да обављате посао и да плаћате порезе једини људи са којима ћете моћи да дискутујете о економији биће ваше колеге у затворској ћелији.

Вредност fiat новца не вуче корен из његових сопствених својстава. Колико је добар одређени тип fiat новца, повезано је једино са политичком и фискалном (не)стабилношћу оних из чије је маште настао. Његова вредност је наметнута декретом, произвољно.

fi·at /ˈfēˌät,ˈfēət/---'Neka bude'

До недавно, коришћена су два типа новца: **новац као роба**, направљен од драгоцених *ствари*, и **репрезентативни новац**, који једноставно *представља* драгоцену ствар, обично написмено.

Већ смо се дотакли новца као робе. Људи су користили посебне кости, морске шкољке, и драгоцене метале као новац. Касније, углавном су се као новац користиле кованице направљене од драгоцених метала као што су сребро и злато. Најстарија кованица до данас пронађена направљена је од природне мешавине сребра и злата и направљена је пр више од 2700 година. Ако је нешто ново у Биткоину, концепт кованице (coin) није.

Лидијски ћилибарни новчић. Picture cc-by-sa Classical Numismatic Group, Inc.

Испада да је гомилање новчића, или ходлинг, да употребим говор данашњице, старо колико и новчићи. Најранији ходлер новчића био је неко ко је ставио скоро стотину ових новчића у котао и закопао га у темеље замка, да би били пронађени 2500 година касније. Ако мене питате прилично добра хладњача.

Једна од лоших страна коришћења новчића од драгоцених метала је да они могу бити подсечени, што у суштини смањује вредност новчића. Од одсечака, могу се стопити нови новчићи, што током времена доводи до инфлације залиха новца, одузимајући вредност сваком поједином новчићу у овом процесу. Људи су буквално бријали своје сребрне доларе колико год су кришом могли. Питам се какве су огласе типа *Бријање за долар* имали у тим данима.

Пошто су владе равнодушне према инфлацији само ако је оне спроводе, предузети су напори да се заустави ово герилско смањивање вредности. На класичан начин жандара-и-лопова, шишачи новчића постали су креативнији у својој техници, присиљавајући "мајсторе ковања новца" да постану још креативнији у својим контрамерама.

Исак Њутн, светски познати физичар славан по *Principia Mathematica*, био је један од тих мајстора. Њему се приписује стављање малих тракица на бокове новчића, а који су присутни још и данас. Прошли су дани лаког шишања новчића.

Чак и кад се овакве методе обезвређивања новчића држе под контролом, новчићи ипак пате од других проблема. Они су гломазни и нису врло погодни за транспорт, нарочито када треба да се догоде велики трансфери вредности. Појављивање са огромним џаком сребрних долара сваки пут када хоћете да купите мерцедес није много практично.

Говорећи о немачким стварима: Како је долар Сједињених држава добио своје име представља још једну занимљиву причу. Реч "долар" извучена је од немачке речи *Thaler*, скраћено од *Joachimsthaler*. Јоакимсталер је био новчић скован у граду *Sankt Joakimstal*. Талер је једноставно скраћено име за неког (или нешто) што долази из те долине, а пошто је Јоакимстал била долина за производњу сребрних новчића, људи су једноставно говорили о тим сребрним новчићима као о *талерима*. Талер (немачки) преобликовао се у далдерс (холандски), и коначно у долар (енглески).

Првобитни 'доларг'. Свети Јоаким представљен са својом одором и чаробњачком капом.. Picture cc-by-sa Berlin-George

Увођење репрезентативног новца најавило је пропаст тврдог новца. Сертификати за злато уведени су 1863, и око петнаест година касније, сребрни долар је такође споро али сигурно био замењен папирним двојником: сертификатом за сребро.

Требало је да прође око 50 година од увођења првих сертификата за сребро да би се ти комади папира претворили у нешто што бисмо ми данас препознали као један САД долар.

Један сребрни долар САД из 1928 'Исплативо доносиоцу на захтев' Picture credit to the National Numismatic Collection at the Smithsonian Institution

Можете приметити да овај сребрни долар Сједињених држава из 1928. још иде под именом *сертификата сребра*, указујући заиста да је то једноставно документ који тврди да носилац овог комада папира поседује комад сребра. Занимљиво је запазити да текст који указује на ово постаје временом све ситнији. Траг "сертификата" потпуно нестаје после неког времена, бивајући замењен утешним исказом да су то новчанице федералних резерви.

Као што је горе поменуто, иста ствар десила се злату. Велики део света био је на биметалном стандарду, што ће рећи да су новчићи прављени првенствено од злата и сребра. Постојање сертификата за злато који су се могли заменити за златне новчиће, може се сматрати технолошким напретком. Папир је погоднији, лаганији, и пошто се може произвољно поделити једноставним штампањем мањег броја на њему, лакше га је разбити у мање јединице.

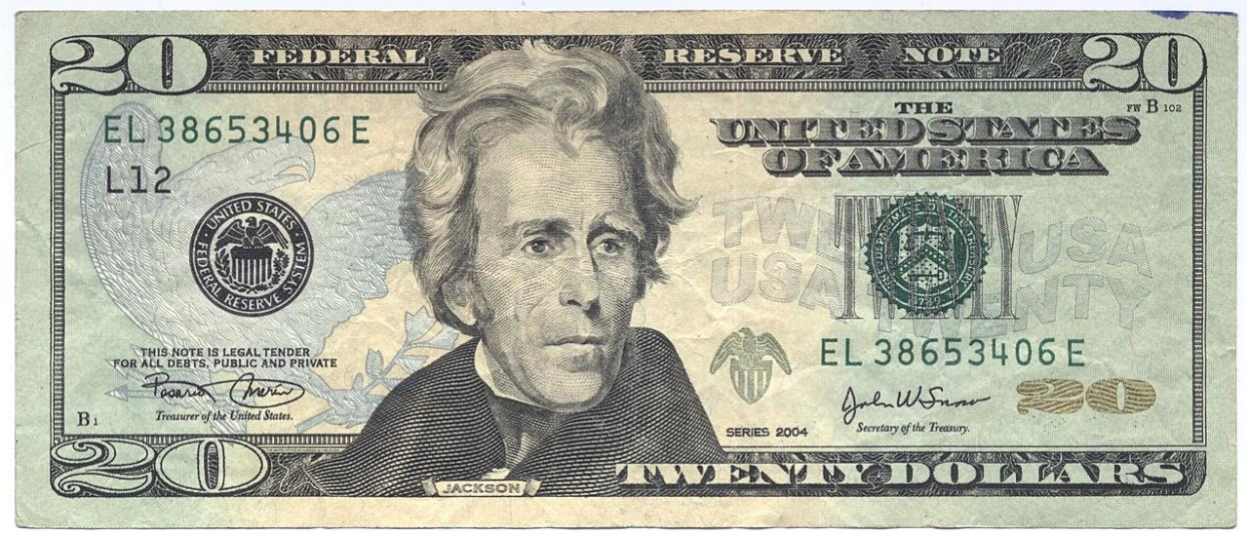
Да би подсетили носиоце (кориснике) да ови сертификати представљају стварно злато и сребро, били су обојени у складу са тим и јасно су то објављивали на самом сертификату. Можете течно прочитати запис од врха до дна:

"Ово потврђује да је у трезору Сједињених америчких држава депоновано сто долара у златним кованицама који су исплативи носиоцу на захтев."

Picture credit to National Numismatic Collection, National Museum of American History.

Године 1963, речи “ИСПЛАТИВО ДОНОСИОЦУ НА ЗАХТЕВ” уклоњене су са свих новоемитованих новчаница. Пет година касније, замена папирних новчаница за злато и сребро је прекинута.
Речи које су наговештавале порекло и идеју која стоји иза папирног новца су уклоњене. Златна боја је нестала. Све што је остало био је папир и са њиме могућност владе да га штампа колико год то жели.

Са укидањем златног стандарда 1971, ова, један век дуга варка руком, била је комплетна. Новац је постао илузија коју ми сви делимо сваки дан: fiat новац. Он вреди нешто јер неко ко командује војском и управља затворима каже да он вреди нешто. Као што се може јасно прочитати на свакој доларској новчаници која је данас у оптицају, “ОВА НОВЧАНИЦА ЈЕ ЗАКОНСКО СРЕДСТВО ПЛАЋАЊА”. Другим речима: Она вреди зато што на њој тако пише.



Новчаница од двадесет долара Сједињених држава из серије 2004 која се користи данас. 'ОВА НОВЧАНИЦА ЈЕ ЗАКОНСКО СРЕДСТВО ПЛАЋАЊА'

Узгред буди речено, постоји још једна занимљива лекција о данашњим банкнотама, сакривена директно пред очима. Други ред каже да је то средство плаћања “ЗА СВЕ ДУГОВЕ, ЈАВНЕ И ПРИВАТНЕ”. Оно што би могло бити очигледно економистима мене је изненадило: Сав новац је дуг. Глава ме још боли због тога, а оставићу истраживање о односу новца и дуга као вежбу за читаоца.

Као што смо видели, злато и сребро користили су се као новац миленијумима. Током времена, кованице од злата и сребра замењене су папиром. Папир је полако прихваћен као средство плаћања. Ово прихватање створило је илузију – илузију да сам папир има вредност. Коначни потез био је да се потпуно пресече веза између замене и стварног: укидање златног стандарда и убеђивање свакога да је сам папир драгоцен.

Биткоин ме је научио историји новца и највећој варци руком у историји економије: fiat валути.

Низ зечју рупу

- Enders Game од Паркера Луиса
- Bitcoin Fixes This од Паркера Луиса
- Bitcoin Obsoletes All Other Money од Паркера Луиса
- Bitcoin Is a Rally Cry од Паркера Луиса
- Bimetallism од сарадника Википедије
- Methods of Coin Debasement од сарадника Википедије
- Thaler од сарадника Википедије
- U.S. Silver Certificate од сарадника Википедије
- How Is Fiat Money Possible од Ханс-Хермана Хопеа
- On The Origins Of Money од Карла Менгера

Лекција 13: Безумље фракционе резерве

Авај! било је сувише касно: наставила је да расте и да расте, и врло брзо морала је да клекне: следећег тренутка није било више простора ни за то, и покушала је да легне, тако да јој један лакат упре у врата, а друга рука јој се обавије око главе. И даље је наставила да расте, и као последње прибежиште истурила је једну руку кроз прозор, а једно стопало у димњак, и рекла је себи "сад не могу више ништа—шта ће бити са мном?"

Вредност и новац нису тривијалне теме, посебно у данашње време. Процес стварања новца у нашем банкарском систему је подједнако не-тривијалан, и не могу да се отресем осећаја да је то намерно тако.

Оно на шта сам раније наилазио само на академији и у правним текстовима изгледа да је општа пракса и у финансијском свету: ништа није објашњено једноставним речима, не зато што је стварно комплексно, већ зато што је истина сакривена иза слојева и слојева жаргона и *привидне* комплексности. "Експанзионарна монетарна политика, квантитативно попуштање, фискални стимулус за привреду." Публика клима главом у знак слагања, хипнотизована китњастим речником.
Банкарство фракционе резерве и квантитативно попуштање су два од ових модерних израза, који замагљују оно што се стварно дешава маскирајући га као комплексно и тешко за разумевање. Ако бисте их објаснили неком петогодишњаку, ненормалност оба израза брзо би постала видљива. Годфри Блум, обраћајући се Европском парламенту на заједничкој дебати, рекао је то далеко боље него што бих ја икада могао:

"[…] ви не разумете заиста концепт банкарства. Све банке су пропале. Банка Сантандер, Дојче банк, шкотска Краљевска банка – све су оне пропале! А зашто су пропале? То није божје дело. То није нека врста цунамија. Оне су пропале јер ми имамо систем који се зове "банкарство фракционе резерве" које значи да банка може да позајмљује новац који уствари нема! То је криминални скандал и он се догађа сувише дуго. […]

Ми имамо фалсификовање—нешто што се зове квантитативно попуштање—али под сваким другим именом је фалсификовање. Вештачко штампање новца које, ако би га вршила било која обична особа, отишла би у затвор на врло много времена […] о све док не

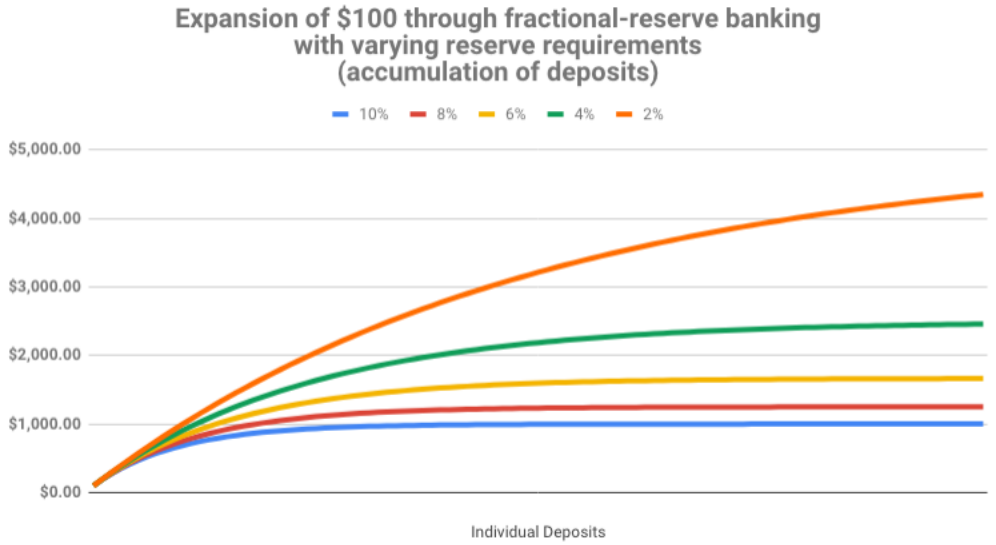
почнемо да шаљемо банкаре —а ту укључујем централне банкаре и политичаре —у затвор за ову срамоту то ће се наставити.”
Годфри Блум

Дозволите да поновим најважнији део: банке могу да позајмљују новац који уствари немају.
Захваљујући банкарству фракционих резерви, банка мора да држи само малу фракцију сваког долара који добија. То је негде између 0 и 10%, обично на нижем крају, што чини ствари још горим.

Хајде да употребимо конкретан пример да боље разумемо ову луду идеју: Фракција од 10% ће завршити посао и ми би требало да можемо да извршимо све прорачуне у глави.Win-win. Дакле, ако однесете 100 долара у банку —зато што нећете да их чувате испод свог душека—они треба само да задрже договорену *фракцију* те суме. У нашем примеру то би било 10 долара, јер 10% од 100 долара је 10 долара. Лако, зар не?

Шта онда банкеураде са остатком новца? Шта се дешава са ваших 90 долара? Оне раде оно што банке раде, позајмљују их другим људима. Резултат је ефекат умножавања новца, који огромно повећава количине новца у привреди. Ваш првобитни депозит од 100 долара ускоро ће се претворити у 190 долара.

Позајмљујући удео од 90% у новостворених 90 долара, у привреди ће се ускоро појавити 271 долар. И 343.90 долара после тога. Резерве новца се стално сваки пут повећавају, пошто банке буквално позајмљују новац који немају. Без иједног Абракадабра, банке магично претворе 100 долара у хиљаду долара или више. Испада да је 10 х лако. Потребно је само неколико кругова позајмљивања.



Не схватајте ово погрешно. Ништа не фали позајмљивању. Нема ничег погрешног у интересу. Ништа није погрешно чак ни у старим добрим исправним банкама које чувају вашу имовину негде где је сигурније него у вашој фиоци са чарапама.

Централне банке су, међутим, друга врста животиње. Одвратности финансијске регулације, пола јавне пола приватне, изигравају бога са нечим што погађа свакога ко је део наше светске цивилизације, без савести, само заинтересоване за непосредну будућност, и наизглед и без било какве одговорности или могућности контроле.

Иако је Биткоин још увек инфлаторан, он ће ускоро престати да буде такав. Строго ограничене залихе на 21 милион биткоина на крају ће сасвим одстранити инфлацију. Ми сада имамо два монетарна света: један инфлаторан у коме се новац штампа произвољно, и свет Биткоина, где је коначна количина фиксирана и лако проверљива са свачије стране. Један нам је наметнут насиљем, другоме се може придружити ко год жели. Нема баријера на улазу, није потребна ничија дозвола. Добровољно учешће. То је лепота Биткона.

Моје је мишљење да расправа између кејнезијанаца и аустријских економиста више није чисто академска. Сатоши је успео да изгради систем за пренос вредности на стероидима, стварајући у овом процесу најздравији новац који је икад постојао

Овако или онако, све више људи упознаће превару коју представља банкарство фракционе резерве. Ако дођу до сличних закључака као и већина аустријских економиста и биткоинера, могли би се придружити стално растућем интернету новца. Нико их не може зауставити ако одлуче да тоураде.

Биткоин ме је научио да је банкарство фракционе резерве чисто безумље.

Низ зечју рупу

- Austrian School од сарадника Википедије
- Keynesian Economics од сарадника Википедије
- Money Multiplier од сарадника Википедије
- Why the whole banking system is a scam од Годфрија Блума
- 🎧 Jörg Guido Hülsmann on Fiat Money and Fractional Reserve Banking SLP#51 домаћин Стефан Ливера
- The Creature From Jekyll Island од Г. Едварда Грифина

Лекција 14: Здрав новац

"Прва ствар коју морам да урадим," рече Алиса себи, док је лутала по шуми, "је да нарастем до своје праве величине, а друга ствар је да нађем пут у ту дивну башту. Мислим да ће то бити најбољи план."

Најважнија ствар коју сам научио од Биткоина је да, на крају крајева, тврд новац буде супериоран над меким новцем. Тврд новац, такође називан и *здрав новац*, је било која валута којом се тргује по свету а која служи као поуздано складиште вредности.

Слажем се, Биткоин је још увек млад и колебљив. Критичари ће рећи да не складишти вредност на поуздан начин. Аргумент колебљивости промашује тему. Колебљивост се очекује. Тржишту ће требати мало да би схватило праведну цену овог новог новца. Такође, како је више пута у шали указано, он се заснива на грешци у мерењу. Ако размишљаш у доларима не успеваш да видиш да ће један биткоин увек вредети један биткоин.

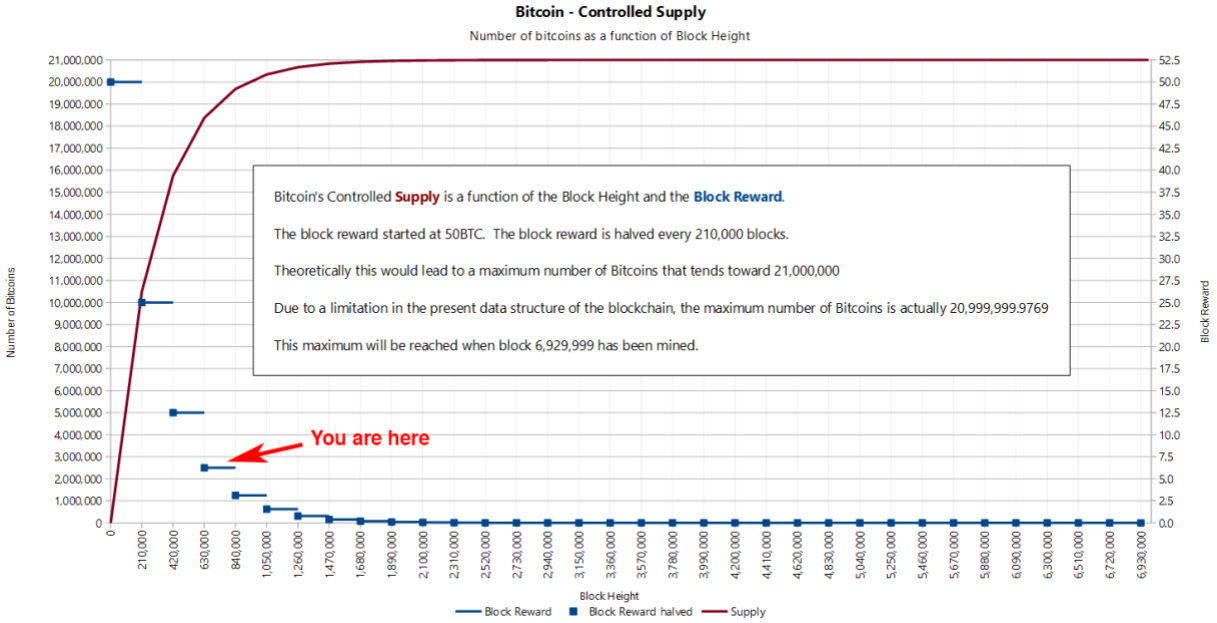
“Фиксна залиха новца, или залиха промењена само у складу са објективним и прорачунљивим критеријумима, је неопходан услов за смислену праведну цену новца.”
Фр. Бернард В. Демпси, С.Ц.

Како нам је брза шетња кроз гробље заборављених валута показала, новац који се може штампати биће наштампан. До сада, ниједан човек у историји није био у стању да се одупре том искуству. Биткоин уклања искушење да се новац штампа на један генијалан начин. Сатоши је био свестан наше похлепе и погрешивости —зато је одабрао нешто поузданије од људске уздржаности: математику.

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

Формула залиха Биткоина

Иако је ова формула корисна да се опишу залихе Биткоина, она се уствари не може наћи нигде у коду. Производње новог биткоина ради се на алгоритамски контролисан начин, смањивањем награде која се исплаћује рударима сваке четири године. Горња формула се користи да се брзо резимира шта се дешава испод површине. Шта се стварно дешава може се најбоље видети гледањем у промену награде за блок, награде која се исплаћује свакоме ко наше важећи блок, што се отприлике дешава на сваких 10 минута.



Формуле, логаритамске функције и експоненцијали не могу се баш интуитивно разумети. Концепт *степена здравља* могао би се лакше разумети ако се гледа на други начин. Једном када схватимо колико има нечега, и једном када схватимо колико је тешко то нешто произвести или га се докопати, ми тренутно схватимо његову вредност.

Оно што важи за Пикасове слике, гитаре Елвиса Преслија, и Страдиваријусове виолине такође важи и за fiat валуте, злато и биткоине.
Тврдоћа fiat валуте зависи од тога у чијим су рукама одговарајуће штампарске пресе.

Неке владе су можда више вољне да штампају велике количине валуте у односу на друге, што доводи до слабије валуте. Друге владе су можда рестриктивније у свом штампању новца, што доводи до тврђе валуте.

Пре него што смо имали fiat валуте, степен здравља новца био је одређен природним својствима ствари коју смо користили као новац. Количина злата на земљи је одређена законима физике. Злато је ретко зато што су ретки судари супернових и неутронских звезда. “Проток” злата је ограничен јер је његово вађење баш напорно. Пошто је тежак елемент оно је већином укопано дубоко испод земље.

Укидање златног стандарда уступило је простор новој стварности: додавање новог новца захтева само кап мастила. У нашем модерном свету додавање пар нула на стању на банковном рачуну захтева још мање напора: преобртање неколико битова у банчином компјутеру је довољно.

“Један значајан аспект ове нове реалности је да институције као што су Федералне резерве не могу да банкротирају. Оне могу да наштампају било коју количину новца која би им можда затребала са трошковима који су буквално нула.”

Јерг Гвидо Хилсман

Принцип који је горе истакнут може се изразити општије као однос “резерви” према “приливу”. Једноставно, *резерве* значе колико много нечега је тренутно ту. За нашу сврху, резерве су мера тренутних залиха новца. *Проток* је колико се произведе у одређеном периоду времена (нпр. на годину дана). Кључ за разумевање здравог новца је разумевање овог односа резерве-према-протоку.

Израчунавање односа резерве-према-протоку (stock-to-flow тешко је за fiat валуте, јер колико новца је ту зависи од тога како гледаш на то. Могли бисте да бројите само банкноте и кованице (M0), да додате путне чекове и чековне депозите (M1), додати штедне рачуне и заједничке фондове и неке друге ствари (M2) и чак додати и потврде о депозиту на све то (M3). Даље, како ће се све ово дефинисати и мерити мења се од земље до земље и пошто су Федералне резерве у САД престале да објављују бројке за M3, мораћемо да се задовољимо са монетарним залихама новца M2. Волео бих да проверим ове цифре, али рекао бих да ћемо морати да верујемо Федералним резервама за сада.

Злато, један од најређих метала на земљи, има највећи однос резерве-према-протоку. Према Геолошком прегледу САД, ископано је мало више од 190.000 тона. У последњих неколико година ископано је 3100 тона злата по години.

Користећи ове цифре, можемо лако да израчунамо да је однос резерве-према-протоку за злато: 190.000 тона/3.100 тона = 61.

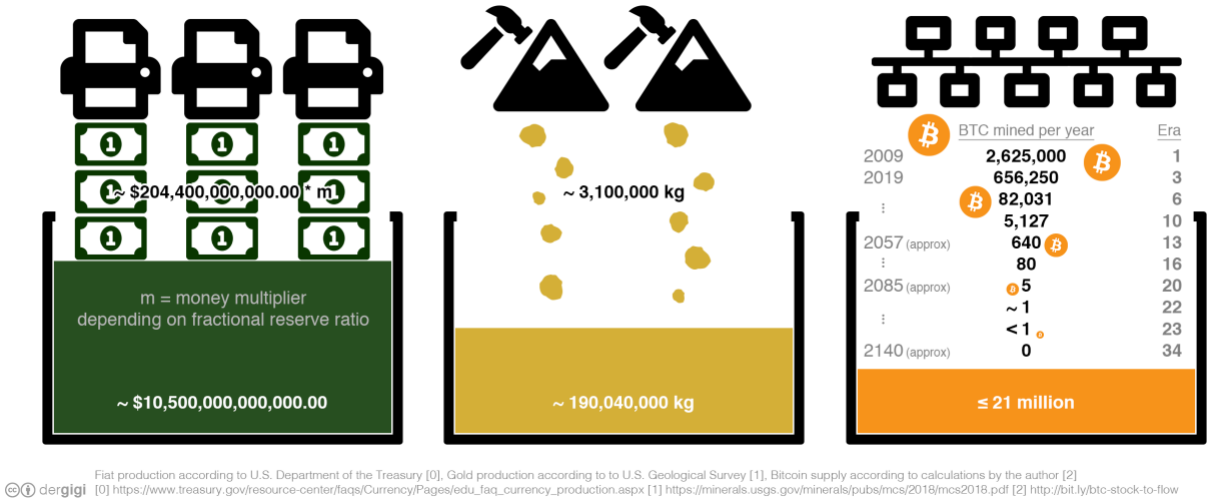
Ништа нема већи однос резерве-према-протоку него злато. Због тога је злато, до сада, било најтврђи, најздравији новац који постоји. Често се каже да би сво злато ископано до сада испунило два базена олимпијских димензија. Према мојим прорачунима, требало би нам четири. Тако да је овоме можда потребно ажурирање, или су се базени олимпијских димензија смањили..

Улази Биткоин. Као што вероватно знате, рударење биткоина било је опште лудило последњих пар година. То је зато што смо још увек у раним фазама онога што се зове *ера награђивања*, где се рударски чворови награђују са *доста* биткоина за њихов процесорски напор.

Ми смо тренутно у ери награђивања број 4, која је почела у 2020. и завршиће се рано у 2024, вероватно у мају. Иако су залихе биткоина унапред одређене, унутрашње функционисање Биткоина дозвољава само приближне датуме. Ипак, можемо да предвидимо колики ће бити однос резерве-према-протоку Биткоина.

Упозорење на спојлер: биће висок.

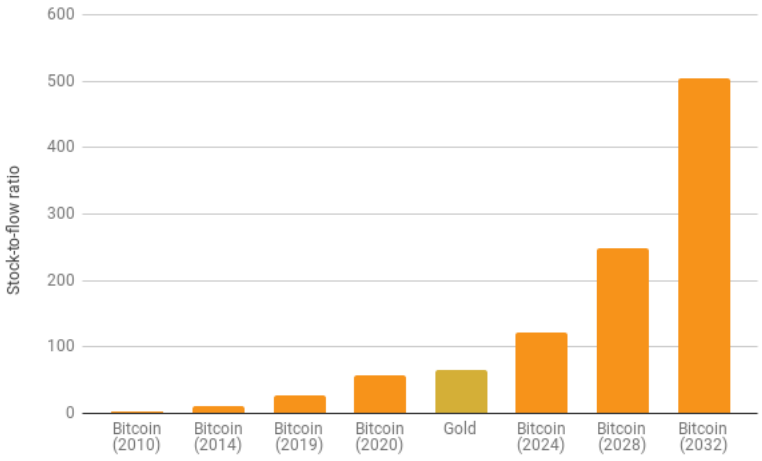
Колико висок? Па, испада да ће Биткоин бити бескрајно тврд.



Визуализација залиха и протока за САД долар, злато и Биткоин

Услед експоненцијлног опадања награде за рударење, проток новог биткоина ће се смањити што ће однос резерве-према-протоку лансирати у небо. Скоро се сустигао са златом у 2020, да би га претекао за само четири године поново удвостручавајући своје стање здравља. Такво удвостручавање ће се догодити укупно 32 пута.

Захваљујући снази експоненцијала, број биткоина који се изрударе за годину дана пашће испод 100 биткоина у 50 година и испод 1 биткоина у 75 година. Глобална славина која је награда за блокове пресушиће негде око 2140, фактички прекидајући продукцију биткоина. Ово је дугачка игра. Ако ово читате, још увек имате времена.



РПораст односа залихе-према-протоку биткоина у поређењу са златом

Пошто се биткоин приближава бесконачном односу резерве-према-протоку, то ће бити најздравији новац који постоји. Бесконачно здравље тешко је победити.

Посматрано кроз призму економије, Биткоиново *прилагођавање тежине рударења* је вероватно његова најважнија компонента. Колико је тешко изрударити биткоин зависи од тога колико брзо се рударе нови биткоини.* Динамичко подешавање тежине рударења у мрежи је оно што нам омогућава да предвидимо његов будући проток.

*(*То уствари зависи од тога колико брзо се проналазе важећи блокови, али за нашу сврху, то је исто као и "рударење биткоина" и тако ће бити кроз следећих 120 година.)*

Једноставност алгоритма за подешавање тежине могла би одвући пажњу од његовог темељног значаја, али прилагођавање тежине је истински једна револуција ајнштајновских пропорција. Оно осигурава да, без обзира колико много или колико мало напора је уложено у рударење, контролисана резерва Биткоина неће бити нарушена

Насупрот сваком другом ресурсу, без обзира колико много енергије неко уложи у рударење биткоина, укупна награда се неће повећати..

Баш као што $E=mc^2$ диктира универзалну границу брзине ун ашем универзуму, Биткоиново прилагођавање тежине диктира **универзални новчани лимит** у Биткоину.

Да нема овог прилагођавања тежине, већ би сви биткоини до сада били изрударени. Да нема овог прилагођавања тежине, Биткоин вероватно не би преживео своје детињство. То је оно што обезбеђује ову мрежу у њеној ери награђивања. То је оно што обезбеђује стабилну и поштену расподелу новог биткоина. То је термостат који регулише Биткоинову монетарну политику.

Ајнштајн нам је показао нешто ново: без обзира колико јако гураш неки предмет, у одређеној тачки нећеш моћи да извучеш више брзине из њега. Сатоши нам је такође показао нешто ново: без обзира колико напорно копаш тражећи дигитално злато, у одређеној тачки нећеш моћи да добијеш више биткоина из њега. По први пут у људској историји, имамо монетарно добро кога, без обзира колико јако покушавате, нећете моћи да створите још.
Биткоин ме је научио да је здрав новац суштински значајан.

Низ зечју рупу

- Bitcoin's distribution was fair од Дена Хелда
- Bitcoin is Common Sense од Паркера Луиса
- Bitcoin's Controlled Supply од сарадника Биткоин Викија
- Mineral Commodity Summaries 2019 од Геолошког прегледа Сједињених држава
- Money Supply од сарадника Википедије
- Speed of Light од сарадника Википедије
- 🎧 Saifedean Ammous on Bitcoin as Sound Money
  Noded#3 домаћини Мајкл Голдстајн и Пјер Рошар
- 🎧 Murad Mahmudov on Bitcoin as the World Reserve Currency
  TFTC#34 домаћин Марти Бент
- Money, Sound And Unsound од Џозефа Салерна
- The Ethics Of Money Production од Јерга Гвида Хилсмана

Глава III: Технологија

"Дакле, овај пут ћу боље успети" рече она себи, и поче узимајући мали златни кључ и откључавајући врата која су водила у башту.

Златни кључеви, сатови који раде само случајно, трке да би се решиле чудне загонетке, и зидари који немају имена ни лица. Оно што звучи као бајка из Земље чуда је свакодневна ствар у свету Биткоина.

Као што смо истражили у Глави 2, велики делови садашњег финансијског система су систематски разбијени. Као Алиса, ми се само можемо надати да ћемо овоог пута успети боље. Али, захваљујући изумитељу под псеудонимом, имамо невероватну профињену технологију која ће нас подржавати овога пута: Биткоин.

Решавање проблема у радикално децентрализованом и непријатељском окружењу захтева јединствена решења. Оно што би иначе били тривијални проблеми за решавање сада су све само не то у овом чудном свету чворова. Биткоин се ослања на строгу криптографију за већину решења, барем ако се гледа кроз призму технологије. Колико је баш јака та криптографија биће истражено у једној од следећих лекција.

Криптографија је оно што Биткоин користи да уклони поверење у власти. Уместо ослањања на централизоване институције, овај систем се ослања на коначну власт нашег универзума: физику. Нека зрнца поверења и даље опстају, међутим. Испитаћемо та зрнца у другој лекцији овог поглавља.

- Лекција 15: Снага у бројевима
- Лекција 16: Размишљања о “Не веруј, провери”
- Лекција 17: Одређивање времена захтева рад
- Лекција 18: Крећи се полако и не ломи свари
- Лекција 19: Приватност није мртва
- Лекција 20: Сајферпанкови пишу код
- Лекција 21: Метафоре за будућност Биткоина

Последњих пар лекција истражују етос технолошког развоја у Биткоин, што је, показало се, исто онолико важно као и сама технологија. Биткоин није следећа светлуцава апликација на вашем телефону. То је темељ нове економске реалности, због чега би Биткоин требало третирати као финансијски софтвер најфинијег степена.

Где смо ми у овој финансијској, друштвеној и технолошкој револуцији? Мреже и технологијие прошлости могу да послуже као метафоре за будућност Биткоина, а оне су истражене у последњој лекцији ове главе.

Још једном, вежи се и уживај у вожњи. Као и све експоненцијалне технологије, ми се спремамо да постанемо параболични..

Лекција 15: Снага у бројевима

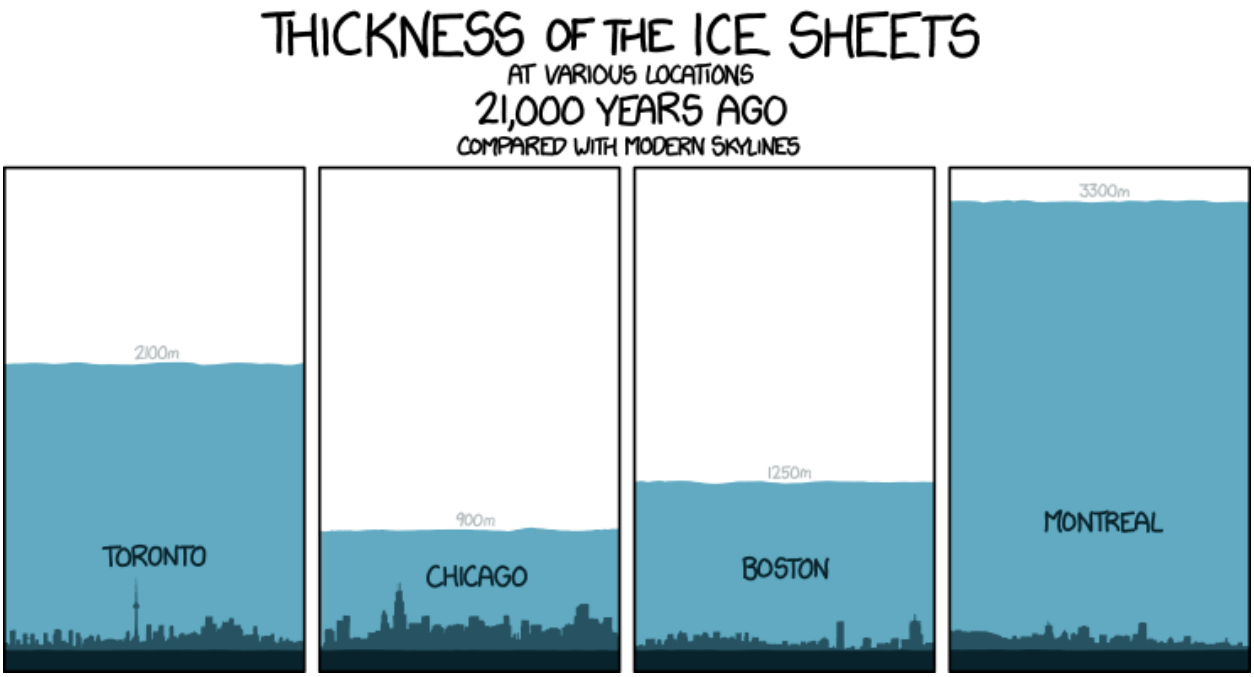
Чекај да видим: четири пута пет је дванаест, а четири пута шест је тринаест, а четири пута седам је четрнаест—ох боже! Никада нећу стићи до двадесет овом брзином!

Бројеви су неопходни део нашег свакодневног живота. Велики бројеви, међутим, нису нешто што је познато већини од нас. Највећи бројеви са којима се можемо срести у свакодневном животу су реда милиона, милијарди или билиона. Можемо читати о милионима људи који живе у сиромаштву, милијардама долара потрошеним на спасавање банака, и билионима државног дуга. Иако је тешко схватити смисао ових наслова, немамо проблем са величином ових бројева.

Иако можда немамо проблем са милијардама и билионима, наша интуиција почиње да попушта већ код бројева ове величине. Да ли имате икакву интуицију колико бисте морали да чекате да прође милион/милијарда/трилион секунди? Ако сте као ја, ви сте изгубљени и пре него што бисте почели да крцкате ове бројке.

Погледајно поближе овај пример: разлика између сваког је повећање за три реда величина: 10^6, 10^9, 10^{12}. Размишљање о секундама није много корисно, зато хајде да претворимо то у нешто што може да нам уђе у главу:

- 10^6: Милион секунди било је пре 1½ седмицу.
- 10^9: Милијарда секунди била је пре скоро 32 године.
- 10^{12}: Пре билион секунди Менхетен је био покривен дебелим слојем леда.



Пре отприлике 1 билион секунди. Source: xkcd #1225

Чим уђемо у изван-астрономско царство модерне криптографије, наша интуиција катастрофално попушта. Биткоин је изграђен око великих бројева и виртуалне немогућности да их погодимо напамет. Ови бројеви су далеко, далеко већи од било чега на шта бисмо могли наићи у свакодневном животу. Много редова величине већи. Разумети колико су ови бројеви истински велики је неопходно да би се разумео Биткоин као целина.

Узмимо SHA-256,једну од хеш функција које се користе у Биткоину, као конкретан пример. Сасвим је природно да се размишља о 256 битова као о "двеста педесет шест", што уопште није велики број. Међутим број у SHA-256 говори о редовима величине — што је нешто са чиме наши мозгови нису добро опремљени да се носе.

Иако је дужина бита погодна за мерење, право значење сигурности од 256-бита је изгубљено у преводу. Слично горепоменутим милионима (10^6) и милијардама (10^9), број у SHA-256 је реда величине око (2^{256}).

Дакле, колико је тачно јак SHA-256?

"SHA-256 је врло јак. То није као прираштајни корак од MD5 до SHA1. Може проћи неколико деценија док не дође до неког крупног пробоја."
Сатоши Накамото

Хајде да испишемо ствари. 2^{256} је једнак следећем броју:

115 дуодецилијарди 792 дуодецилиона 89 ундецилијарди 237 ундецилиона 316 децилијарди 195 децилиона 423 нонилијарди 570 нонилиона 985 октилијарди 8 октилиона 687 септилијарди 907 септилиона 853 секстилијарди 269 секстилиона 984 квинтилијарди 665 квинтилиона 640 квадрилијарди 564 квадрилиона 39 трилијарди 457 трилиона 584 билијарди 7 билиона 913 милијарди 129 милиона 639 хиљада 936.

То је много нонилиона! Утувити овај број је прилично немогуће. Ништа у физичком универзуму не може се упоредити са њим. Он је далеко већи од броја атома у видљивом универзуму. Људски мозак једноставно није направљен да га разуме.

Једна од најбољих визуализација праве снаге SHA-256 је следећи видео Гранта Сандерсона. Одговарајуће назван "Колико је безбедна безбедност 256 бита?" он дивно приказује колики је простор 256-бита.

Учините себи услугу и посветите му пет минута. Као и сваки други видео на каналу 3Blue1Brown он је не само фасцинантан, већ је такође и изузетно добро направљен.

Упозорење: Могли бисте пасти низ математичку зечју рупу.

Одговор: Прилично безбедна.

Брус Шнајер користио је физичке границе рачуна да стави овај број у перспективу: чак и када би могао да направи оптимални компјутер, који би користио било какву обезбеђену енергију да савршено обрће битове, ако би изградио Дајсонову љуску око нашег сунца, и пустио је да ради 100 милијарди милијарди година, ми бисмо и даље имали 25% шансе да нађемо иглу у пласту 256-бит-а.

“Ови бројеви немају ништа са технологијом ових уређаја; они су максимум које ће дозволити термодинамика. И снажно подразумевају да ће напади бруталном снагом против кључева 256-бит-а бити неизводљиви све док компјутери не буду прављени од нечег што није материја и не буду заузимали нешто што није простор.”

Брус Шнајер

Тешко је претерати у описивању дубине свега овога. Моћна криптографија изврће равнотежу сила у физичком свету на који смо навикли. Неломљиве ствари не постоје у стварном свету. Примени довољну силу и моћи ћеш да отвориш свака врата, кутију, или ковчег са благом.

Биткоинов ковчег са благом је веома другачији. Заштићен је снажном криптографијом, која не попушта бруталној сили. И све док важе дубље математичке претпоставке, брутална сила је све што имамо. Признајем, постоји такође опција глобалног изнуђивања. Али мучење неће успети на свим Биткоин адресама, а криптографски зидови Биткоина ће одбити нападе бруталне силе. Чак иако их нападнете снагом хиљаду сунца. Буквално.

Ова чињеница и њене импликације дирљиво су резимиране у позиву на криптографско оружје: "*Никаква количина принудне силе неће никада решити један математички проблем.*"

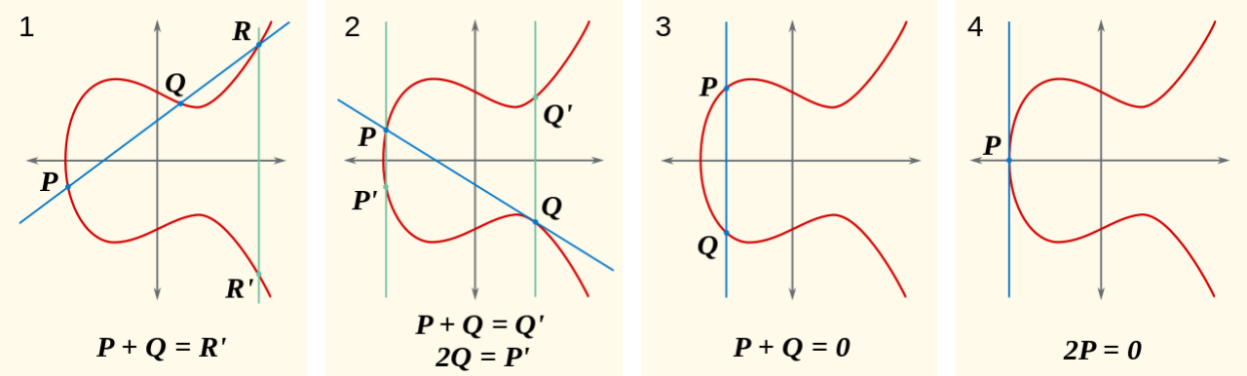
"Није очигледно да свет мора да функционише на овај начин. Али, некако, универзум се осмехује на енкрипцију."
Џулијан Асанж

Нико још не зна са сигурношћу да ли је осмех универзума искрен или није. Могуће је да је наша претпоставка о математичкој асиметрији погрешна и ми откријемо да је P уствари NP, или да откријемо изненађујуће брза решења за специфичне проблеме за које тренутно подразумевамо да су тешки. Ако би се десио такав случај, криптографија какву ми знамо престаће да постоји, а импликације би вероватно промениле свет до непрепознатљивости.

"Vires in Numeris" = "Снага у бројевима"
epii

Vires in numeris није само лако памтљив мото који користе биткоиновци. Дубока је спознаја да постоји недокучива снага у бројевима. Када сам схватио то, као и инверзију постојећих равнотежа сила омогућену тиме, променио се мој поглед на свет и на будућност која лежи пред нама.

Један директан резултат овога јесте чињеница да не морате да тражите дозволу ни од кога да бисте учествовали у Биткоину. Нема листа који треба потписати, нема компаније која је овлашћена, нема владине агенције којој се шаљу пријавни формулари. Једноставно генеришите један велики број и ви сте прилично спремни да кренете. Централна власт над стварањем налога је математика. А само Бог зна ко је власт над њом.



Примери елиптичне криве (cc-by-sa Emmanuel Boutet)

Биткоин је изграђен на нашем најбољем схватању реалности. Иако има још много отворених проблема у физици, компјутерској науци, и математици, прилично смо сигурни у неке ствари. Једна таква ствар је да постоји асиметрија између проналажења решења и вредновања тачности тих решења. Друга је да израчунавање захтева енергију. Другим речима: проналажење игле у пласту сена је теже него проверавање да ли је шпицаста ствар у вашој руци заиста игла или није. А за проналажење игле потребан је рад.

Огромност простора Биткоинове адресе заиста ошамућује. А број приватних кључева још и више. Фасцинантно је колико се много наш модерни свет своди на малу вероватноћу проналажења игле у недокучиво великом пласту сена. Ја сам сада свеснији те чињенице него икада.
Биткоин ме је научио да у бројевима лежи снага.

Низ зечју рупу

- Block hashing algorithm од сарадника Биткоин Викија
- Discrete Logarithm од сарадника Википедије
- Dyson Sphere од сарадника Википедије
- How secure is 256 bit security? од 3Blue1Brown
- Landauer’s Principle од сарадника Википедије
- Last Glacial Maximum од сарадника Википедије
- P versus NP од сарадника Википедије
- SHA-2 од сарадника Википедије
- Fooled By Randomness - The Hidden Role of Chance in Life and in the Markets од Насима Николаса Талеба

Лекција 16: Размишљања о “Не веруј, провери”

"А сада о доказима," рече Краљ, "па онда о пресуди."

Циљ Биткоина је да замени, или бар да представља алтернативу конвенционалним валутама. Конвенционална валута је везана за централизовану власт, без обзира да ли говоримо о законском средству плаћања као што је САД долар или о модерном монополском новцу као што су Фортнајтови V-Buck-ови. У оба примера, морате веровати централној власти која издаје, управља и пушта у циркулацију ваш новац. Биткоин развезује ову везу, и главни проблем који Биткоин решава је проблем *поверења*.

“Основни проблем са конвенционалном валутом је сво то поверење које је потребно да би она функционисала. […] Оно што је потребно је електронски платни систем заснован на криптографском доказу уместо поверења”
Сатоши

Биткоин решава проблем поверења тиме што је потпуно децентрализован, без централног сервера или странака од поверења. Чак не ни *трећих* странака од поверења, већ странака од поверења, тачка. Када нема централне власти, једноставно *нема никога* од поверења. Комплетна децентрализација је иновација. То је корен Биткоинове непобедивости, разлог зашто је још увек жив.
Децентрализација је такође разлог због кога имамо рударење, чворове, хардверске новчанике, и да, блокчејн. Једина ствар у коју треба “имати поверења” је да наше разумевање математике и физике није тотално отишло и да већина рудара поступа поштено (што су они подстакнути да раде).

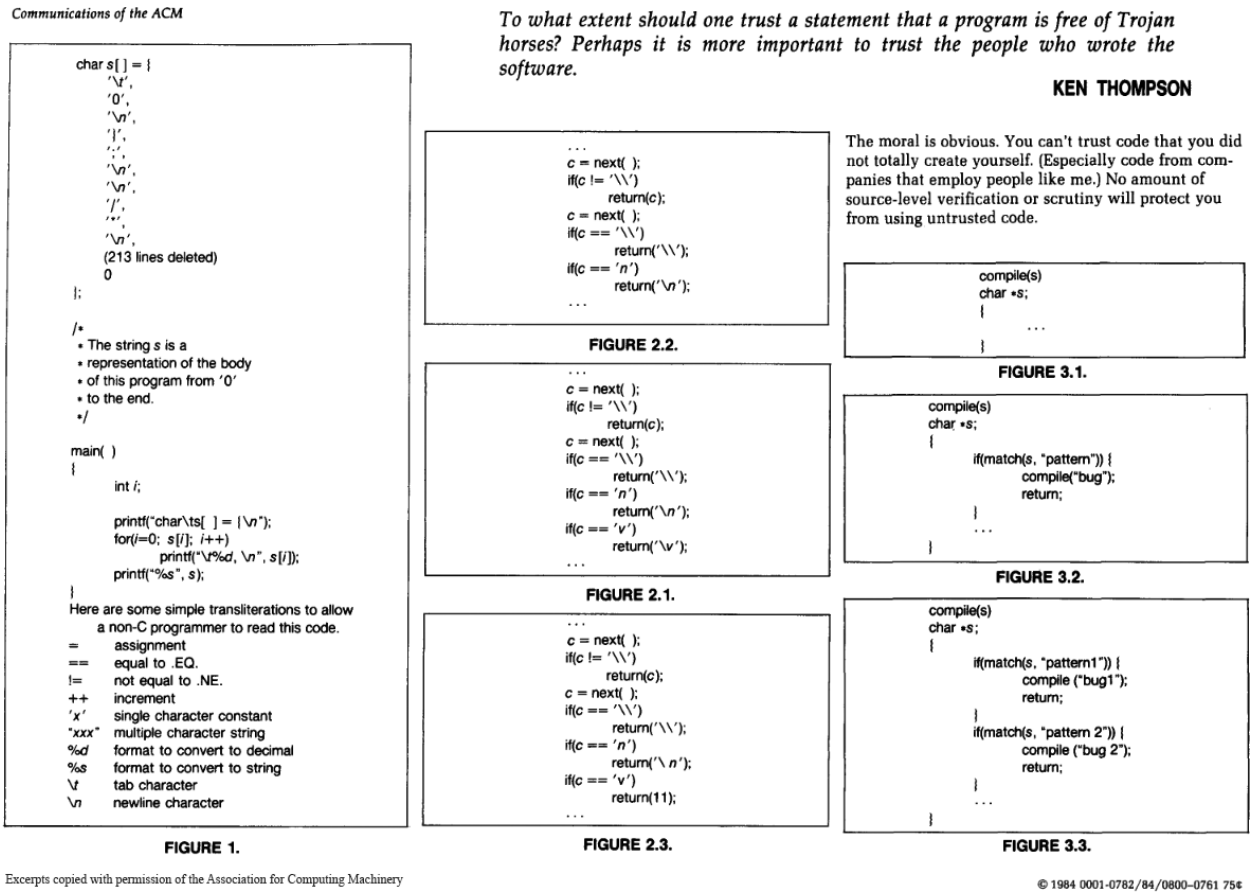
Док обични свет функционише ослањајући се на “*верују, али провери*”, Биткоин се ослања на “*не верују, провери*”. Сатоши је врло јасно истакао значај отклањања поверења и у уводу и у закључку Биткоинове беле књиге.

“Закључак: Ми смо предложили систем за електронске трансакције без ослањања на поверење.”
Сатоши Накамото

Обратите пажњу да се “без ослањања на поверење” овде користи у врло специфичном контексту. Говоримо о трећим странкама од поверења, тј. другим ентитетима којима верујете да ће произвести, чувати и обрађивати ваш новац. Подразумева се, на пример, да можете имати поверење у свој компјутер.

Као што је Кен Томпсон показао у свом предавању поводом Тјурингове награде, поверење је врло пипава ствар у рачунарском свету. Када управљате програмом, морате имати

поверења у све врсте софтвера (и хардвера) који, у теорији, могу да измене, на злонамеран начин, програм којим ви управљате. Како је Томпсон резимирао у својим *Размишљањима о поверљивом поверењу*: “Поука је очигледна. Не можете веровати коду који нисте сами креиралиі.”



Communications of the ACM

```
char s[ ] = {
        '\t',
        '0',
        '\n',
        '}',
        ';',
        '\n',
        '\n',
        '/',
        '*',
        '\n',
        (213 lines deleted)
        0
};

/*
 * The string s is a
 * representation of the body
 * of this program from '0'
 * to the end.
 */

main( )
{
        int i;

        printf("char\ts[ ] = {\n");
        for(i=0; s[i]; i++)
                printf("\t%d, \n", s[i]);
        printf("%s", s);
}
```

Here are some simple transliterations to allow a non-C programmer to read this code.

=	assignment
==	equal to .EQ.
!=	not equal to .NE.
++	increment
'x'	single character constant
"xxx"	multiple character string
%d	format to convert to decimal
%s	format to convert to string
\t	tab character
\n	newline character

FIGURE 1.

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\n');
...
```

FIGURE 2.2.

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\n');
if(c == 'v')
        return('\v');
...
```

FIGURE 2.1.

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\ n');
if(c == 'v')
        return(11);
...
```

FIGURE 2.3.

The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code.

```
compile(s)
char *s;
{
        ...
}
```

FIGURE 3.1.

```
compile(s)
char *s;
{
        if(match(s, "pattern")) {
                compile("bug");
                return;
        }
        ...
}
```

FIGURE 3.2.

```
compile(s)
char *s;
{
        if(match(s, "pattern1")) {
                compile ("bug1");
                return;
        }
        if(match(s, "pattern 2")) {
                compile ("bug 2");
                return;
        }
        ...
}
```

FIGURE 3.3.

Excerpts copied with permission of the Association for Computing Machinery

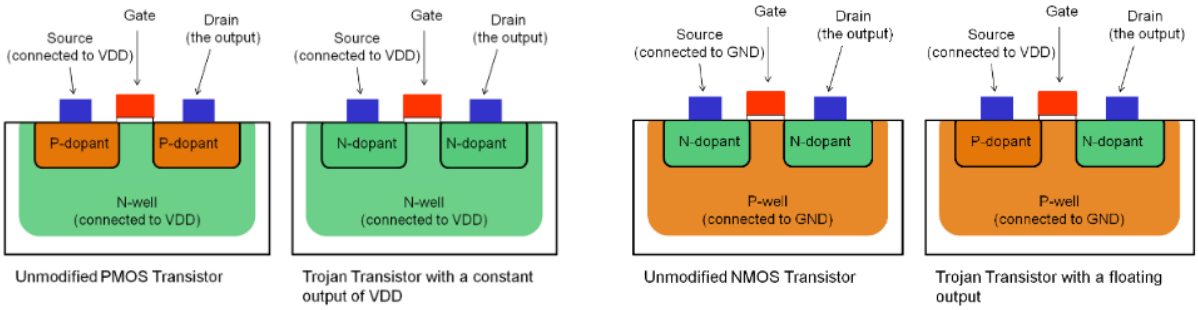
Томпсон је демонстрирао да чак и када имате приступ изворном коду, ваш компајлер – или било који други програм који рукује програмима или хардвером – могао би бити компромитован и детектовање овог тајног приступа било би врло тешко. Дакле, у пракси, систем који истински *не тражи поверење* не постоји. Морали бисте сами да направите сав свој софтвер и сав свој хардвер (асемблере, компајлере, линкере, итд.) од нуле, без помоћи било ког спољашњег софтвера или машине подржане софтвером.

“Ако хоћете да направите питу с јабукама од нуле, морате прво да измислите универзум.”
Карл Саган

Хак Кена Томпсона је посебно довитљив тајни приступ (бекдор), тежак за детектовање, па хајде да бацимо брз поглед на бекдор који је тешко детектовати јер ради без модификовања било каквог софтвера.

Истраживачи су пронашли начин да компромитују хардвер критичан за безбедност измењивањем поларности силикона нечистоћама (допантима). Просто мењајући физичка својства тог материјала од кога су направљени компјутерски чипови, били су у стању да компромитују криптографски безбедан генератор насумичних бројева.

Пошто се ова промена не може видети, бекдор се не може детектовати оптичким испитивањем, које је један од најважнијих механизама за детектовање чачкања по чиповима као што су ови.



(a) p-MOS Transistor (b) n-MOS Transistor

Невидљиви тројанци на допант-нивоу хардвера по Бекеру, Регацонију, Пару, Бурлсону

Звучи застрашујуће? Па, чак и кад бисте били у стању да изградите све од нуле, и даље бисте морали да верујете дубље лежећој математици. Морали бисте да верујете да је secp256k1 елиптична крива без бекдора. Да, злонамерни бекдор може бити убачен у математичке основе криптографских функција и аргументовано је да се то већ десило бар једном. Има добрих разлога да се буде параноичан, и чињеница да све од вашег хардвера, до вашег софтвера, и до елиптичних кривих које користите може имати бекдорове су неки од њих.

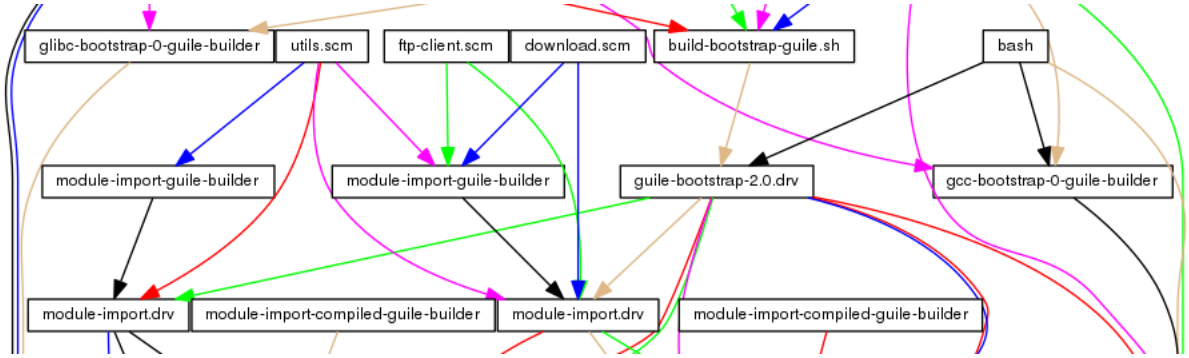
“Не веруј. Провери.”

Горњи примери би требало да илуструју да је рачунарство које *не тражи поверење* утопијско. Биткоин је вероватно систем који се највише приближава утопији, али ипак, он је са *минималним захтевима за поверењем* – са циљем да уклони потребу за поверењем гдегод је то могуће. Показано је да је ланац поверења бескрајан, пошто ћете такође морати да верујете да рачунање захтева енергију, да P није једнако NP, и да сте уствари у приземној реалности а не затворени у симулацији од стране злобних глумаца.

Програмери раде на алатима и процедурама које ће још више свести на минимум сваку преосталу потребу за поверењем. На пример, програмери Биткоина су створили Gitian, који је софтверски метод дистрибуције за стварање детерминистичких билдова. Идеја је да ће, ако више програмера могу да репродукују идентичне бинарне шеме, шансе за злонамерно интервенисање бити смањене. Маштовити бекдорови нису једина средства напада. Једноставна уцена или изнуда су исто тако стварне претње. Као и у главном протоколу, децентрализација се користи да се потреба за поверењем сведе на минимум.

Чине се разнолики напори да се нешто поправи у проблему типа кокошка-или-јаје, у проблему бутстрепинга (коришћења само расположивих ресурса), на који је хак Кена

Томпсона тако бриљантно указао. Такав један напор представља Guix (изговара се Гикс), који користи функционално декларисани пакет менаџмент који доводи до бит-по-бит репродуцибилних билдова по нацрту.
Резултат је да не мораш више да верујеш било ком серверу који обезбеђује софтвер пошто можеш да провериш да ли је на обезбеђеној бинарној шеми било интервенција изграђујући је поново од нуле. Недавно, покренут је zзахтев за промену ради интегрисања Guix-а у процес билдовања Биткоина.



Шта је било прво, кокошка или јаје?

Срећом, Биткоин се не ослања на један алгоритам или део хардвера. Једна последица Биткоинове радикалне децентрализације је расподељен модел безбедности. Иако бекдорове који су претходно описани не треба узимати олако, није вероватно да су угрожени сваки софтверски новчаник, сваки хардверски новчаник, свака криптографска библиотека, свака уградња чвора, сваки компајлер сваког језика. Могуће, али крајње невероватно.

Обратите пажњу да можете генерисати приватни кључ без ослањања на било који рачунарски хардвер или софтвер. Можете бацати новчић, иако зависно од вашег новчића и од вашег стила бацања ова насумичност није довољно насумична. Има разлога зашто протоколи о складиштењу као Glacier саветују да се користи коцкица нивоа оне за казино као један од извора ентропије.

Биткоин ме је присилио да размислим о томе шта неверовање никоме заиста повлачи са собом. Он је појачао моју свесност проблема бутстрепинга, и имплицитног ланца поверења у развијању и вођењу софтвера. Такође је појачао моју свесност о многим начинима на које се софтвер и хардвер могу угрозити.
Биткоин ме је научио да не верујем, већ да проверим.

Низ зечју рупу

- Reflections on Trusting Trust од Кена Томпсона
- Trusted Third Parties Are Security Holes од Ника Сабоа
- The Bitcoin Whitepaper од Сатошија Накамота
- 51% Attack од сарадника Bitcoin Developer Guide (Водич за програмере Биткоина)
- Bootstrapping од сарадника Guix Manual (Приручник Гикса)
- Dual EC DRBG од сарадника Википедије
- ECC Backdoors од сарадника Википедије

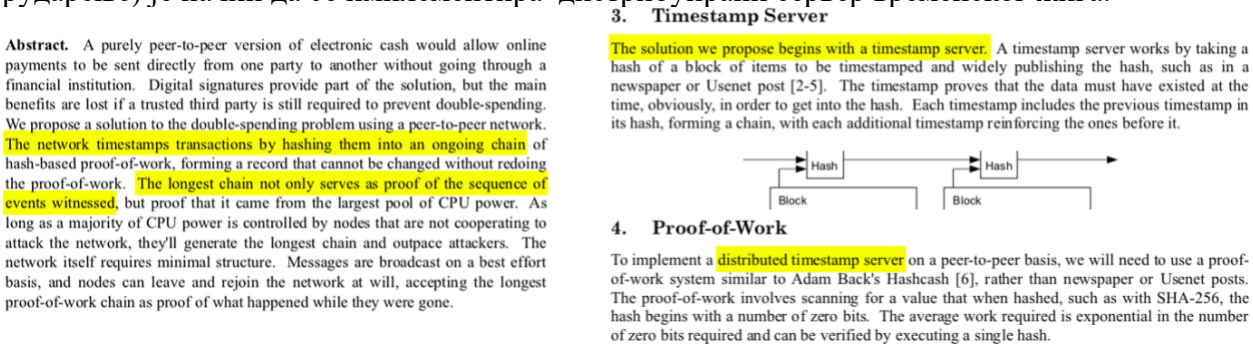
- Secp256k1 од сарадника Биткоин Викија

Лекција 17: Одређивање времена захтева рад

"Боже, боже! Сувише ћу закаснити!"

Често се каже да се биткоини рударе јер хиљаде компјутера ради на решавању *врло сложених* математичких проблема. Одређене проблеме треба решити, и ако израчунате тачан одговор, ви "произведете" биткоин. Иако је овај упрошћен поглед на рударење биткоина можда лакше представити, он помало промашује поенту. Биткоини се не производе нити стварају, и цела мука није баш у решавању одређених математичких проблема. Такође, сама математика није нарочито сложена. Оно што је сложено је *одређивање времена* у једном децентрализованом систему.

Као што је наглашено у белој књизи, систем доказа радом (proof-of-work) (познат и као рударење) је начин да се имплементира дистрибуирани сервер временског жига.



Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

Изводи из беле књиге: Да ли је неко рекао временски ланац?

Када сам први пут сазнао како ради Биткоин и ја сам мислио да је доказ радом неефикасан и сувишан. Мало после, почео сам да мењам своју перспективу о Биткоиновом утрошку енергије. Изгледа да је доказ радом још увек широко несхваћен, у години 13 ПБ (после Биткоина).

Пошто су проблеми који се решавају у доказу радом измишљени, многи људи изгледа мисле да је то *бескористан* посао. Ако је фокус само на израчунавању, ово је разумљив закључак.

Али код Биткоина се не ради о израчунавању. Ради се о независном договору о редоследу *ствари*. Доказ радом је систем у коме свако може да вреднује шта се догодило и којим редом се догодило. Ово независно вредновање је оно што доводи до консензуса, индивидуалног договора од стране многих странака о томе ко шта поседује.

У радикално децентрализованом окружењу, ми немамо луксуз апсолутног времена. Сваки часовник би био увођење треће странке од поверења, централна тачка у систему на коју би се морали ослањати и која би могла бити нападнута. "Тајминг је основни проблем," како то примећује Гриша Трубецкој. А Сатоши је бриљантно решио овај проблем

имплементирајући децентрализовани сат преко блокчејна доказа радом. Свако прихвати унапред да је овај ланац са најкумулативнијим радом извор истине. Он је по дефиницији оно што се заиста десило. Овај договор је оно што се данас назива Накамотов консензус.

“Мрежа удара временски жиг трансакцијама хашујући их у растући ланац што служи као доказ низа догађаја којима је сведочила”
Сатоши Накамото

Без конзистентног начина да се одреди време, нема конзистентног начина да се разликује пре од после.

Немогуће је направити поуздан редослед. Као што је горе поменуто, Накамотов консензус је Биткоинов начин да конзистентно одреди време. Подстицајна структура овог система производи један пробабилистички, децентрализовани часовник, користећи и похлепу и сопствени интерес ривалских учесника. Чињеница да овај часовник није прецизан није релевантна јер је редослед догађаја на крају недвосмислен и свако га може проверити.

Захваљујући доказу о раду, *и* рад *и* вредновање тог рада су радикално децентрализовани. Свако може да се придружи или оде по својој вољи, и свако може да вреднује сваку ствар у било које време. Не само то, већ свако може да вреднује стање система *као појединац*, а да не мора да се ослања на било ког другог ради вредновања..

Да би се схватио доказ о раду треба времена. Он је често супротан интуицији, па иако су правила једноставна, она воде до сасвим сложеног феномена. За мене, помогло је то што сам променио своју перспективу према рударењу. Корисно, а не бескорисно. Вредновање, не израчунавање. Време, не блокови.

Биткоин ме је научио да је одређивање времена пипава ствар, посебно ако сте децентрализовани..

Иза огледала 🔍
Пратите чланке који развијају идеје о којима се расправљало у овој лекцији:

- 🔍 Bitcoin's Energy Consumption - A shift in perspective
- 🔍 Bitcoin Is Time

Низ зечју рупу

- Nothing is Cheaper than Proof of Work од Пола Сторца
- Bitcoin Doesn’t Waste Electricity од Бјутион
- Blockchain Proof-of-Work Is a Decentralized Clock од Грегорија Трубецкоја
- The Anatomy of Proof-of-Work од Хуга Нгујена
- Work is Timeless, Stake is Not од Хуга Нгујена
- Bitcoin Does Not Waste Energy од Паркера Луиса
- Bitcoin Astronomy од Друва Бансала
- The Last Word on Bitcoin’s Energy Consumption од Ника Картера

- Uncovering The Hidden Costs Of The Petrodollar од Алекса Гледстајна
- Controlled Supply од сарадника Биткоин Викија
- Mining од сарадника Биткоин Викија
- 🎧 Trace Mayer on Bitcoin Valuation, Trust, and Energy Consumption
  TIP#252 домаћини Престон Пиш и Стиг Бродерсен
- 🎧 Robert Breedlove on Understanding Bitcoin from First Principles
  CB#52 домаћин Брејди

Лекција 18: Крећи се полако и не ломи ствари

И тако је чамац полако кривудао, под блиставим летњим даном, са својом веселом посадом и својом музиком од гласова и смеха…

Можда је ово мртва мантра, али "крећи се брзо и ломи ствари" је и даље начин на који велики део технолошког света функционише. Идеја да није битно ако ствари успеју из прве је темељни стуб менталитета *греши рано, греши често*. Успех се мери растом, тако да, док растеш, све је одлично. Ако нешто не ради из прве, ти се само окренеш и поновиш. Другим речима: набаци довољно говна на зид и види шта ће се залепити.

Биткоин је веома другачији. Он је по свм нацрту тежак. Он је другачији из нужде. Како је Сатоши указао, е-валута испробана је већ много пута, и сви претходни покушаји су пропали јер је постојала глава која се могла одсећи. Новина Биткоина је у томе што је то звер без глава.

"Многи људи аутоматски одбаце е-валуту као изгубљен случај због свих компанија које су пропале од 1990-тих. Надам се да је очигледно да је централно контролисана природа ових система оно што их је осудило."
Сатоши Накамото

Једна од последица ове радикалне децентрализације је урођена отпорност на промену. "Крећи се брзо и ломи ствари" не функционише и никада неће функционисати на основном нивоу Биткоина. Чак и ако би то било пожељно, не би било могуће без *убеђивања* свакога да промени своје понашање. То је раздељени консензус. То је природа Биткоина.

"Природа Биткоина је таква да, једном када је пуштена верзија 0.1, основни нацрт је уклесан у камен за остатак његовог живота."
Сатоши Накамото

То је једно од многих парадоксалних својстава Биткоина. Сви смо почели да верујемо да је све што је софтвер лако изменити. Али природа ове звери чини сваку промену проклето тешком.

Како Хасу дивно показује у Распакивању Биткоиновог друштвеног уговора, промена правила Биткоина је могућа једино *предлагањем* промене, и даљим *убеђивањем* свих корисника Биткоина да усвоје ту промену. Ово чини Биткоин врло отпорним на промену, иако је софтвер.

Ова непопустљивост је једна од најважнијих особина Биткоина. Критични софтверски системи морају бити не-крхки, а то је оно што однос Биткоиновог друштвеног нивоа и његовог техничког нивоа гарантује. Монетарни системи су по својој природи непријатељски, и као што знамо већ хиљадама година чврсти темељи су неопходни у непријатељском окружењу.

“Киша се спусти, поплаве наиђоше, и ветрови су дували, и ударали на ту кућу; а она не паде, јер је била саздана на стени.”
[Матеј 7:25]

Може се тврдити, у овој параболи о мудрим и глупим градитељима, да Биткоин није та кућа. Он је стена. Непромељива, непокретљива, која обезбеђује основу за један нови финансијски систем.

Баш као и геолози, који знају да се формације стена стално крећу и еволуирају, човек може да види да се и Биткоин стално креће и еволуира. Само треба да знате где да гледте и како да гледате.

Увођење промена pay to script hash (плаћање хашу записа) и segregated witness (издвојени сведок) су доказ да се правила Биткоина могу променити ако довољан број корисника буде уверен да је усвајање те промене од користи за мрежу.

Ова друга промена омогућила је развој lightning network (мућевите мреже), која је једна од кућа које су сграђене на Биткоиновом чврстом темељу. Будуће надградње као што суи Schnorr signatures (Шнорови потписи) повећаће ефикасност и приватност, као и записе (читај: паметне уговоре) који ће бити нераспознатљиви од обичних трансакција захваљујући надградњи Taproot (главни корен). Мудри градитељи заиста граде на чврстим темељима.

Сатоши није био мудар градитељ само у технолошком смислу. Он је такође разумео да би било неопходно да донесе мудре идеолошке одлуке.

“То што је код отворен значи да га свако може независно прегледати. Да је код затворен, нико не би могао да провери безбедност. Мислим да је од суштинског значаја за програм ове врсте да има отворен код.”
Сатоши Накамото

Отвореност је од огромног значаја за безбедност и нераздвојна је од отвореног кода и покрета за бесплатни софтвер.

Како је Сатоши указао, безбедни протоколи и код који их имплементира морају да буду отворени —нема безбедности у скривености. Још једна корист је опет везана за децентрализацију: код који се може користити, проучавати, модификовати, копирати и раздељивати слободно, осигурава да ће бити раширен далеко и широко.

Радикално децентрализована природа Биткоина је оно што га покреће споро и пажљиво. Мрежа чворова, од којих сваким управља суверени појединац, има својство отпорности на промене – злонамерне или не. Без начина да се ажурирања наметну корисницима, једини начин да се промене уведу је да се споро убеди посебно сваки од тих појединаца да прихвати промену.

Тај не-централни процес увођења и развијања промена је оно што чини мрежу невероватно непопустљивом према злонамерним променама. То је такође оно што чини поправку сломљених ствари тежом него у централизованом окружењу, због чега свако пре свега покушава да не ломи ствари.

Биткоин ме је научио да је споро кретање једно од његових својстава, а не баговање.

Низ зечју рупу

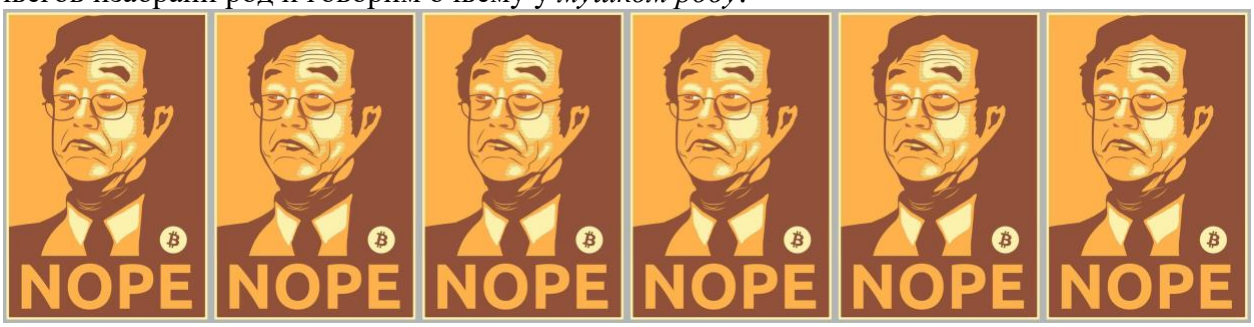
- Bitcoin Is Not Too Slow од Паркера Луиса
- Parable of the Wise and the Foolish Builders од сарадника Википедије
- Segregated Witness (SegWit) од сарадника Биткоин Викија
- Pay to Script Hash (P2SH) од сарадника Биткоин Викија
- Taproot proposal од Грегорија Максвела
- Schnorr signatures BIP од Питера Вуила

Лекција 19: Приватност није мртва

Играчи су играли сви одједном не чекајући свој ред, и свађали су се све време на сав глас, и за само неколико минута Краљица је била сва бесна, и стално је ударала ногом и викала "одрубите му главу!" или "одрубите јој главу!" на сваки минут.

Ако је веровати познаваоцима, приватност је мртва од 80-тих. Изум Биткоина под псеудонимом и други догађаји у новијој историји показују да то није случај. Приватност је жива, иако никако није лако да се избегне ово стање надгледања.

Сатоши је отишао веома далеко да би прикрио своје трагове и сакрио свој идентитет. Тринаест година касније, још увек није познато да ли је Сатоши Накамото био појединац, група људи, мушкарац, жена, или вештачка интелигенција која путује кроз време која је сама себе направила да би преузела свет. Када одбацимо теорије завере, Сатоши је одабрао да идентификује себе као Јапанца, због чега ја не претпостављам већ поштујем његов изабрани род и говорим о њему у *мушком роду*.



Ја нисам Доријан Накамото.

Који год био његов прави идентитет, Сатоши је био успешан у његовом сакривању. Поставио је охрабрујући пример за свакога ко жели да остане анониман: могуће је имати приватност онлајн.

"Енкрипција делује. Правилно имплементирани снажни крипто системи су једна од мало ствари на које се можете ослонити."
Едвард Сноуден

Сатоши није први изумитељ са псеудонимом или који је анониман, а неће бити ни последњи. Неки су директно опонашали овај стил објављивања под псеудонимом, као Том Елвис Једјузор познат као Mimbl Vimbl, док су други објавили усавршене математичке доказе остајући потпуно анонимни.

Чудан је овај нови свет у коме живимо. Свет у коме је идентитет ствар опције, прилози се прихватају на бази заслуге, и људи могу да сарађују и да обављају трансакције слободно.

Биће потребно одређен прилагођавање да навикнемо на те нове парадигме, али ја снажно верујем да све ово има потенцијал да промени свет на боље.

Сви треба да упамтимо да је приватност основно људско право. И докле год људи упражњавају и бране ова права битка за приватност је далеко од завршене.
Биткоин ме је научио да приватност није мртва.

Иза огледала 🔍
Пратите чланке који развијају идеје о којима се расправљало у овој лекцији:

- 🔍 True Names Not Required

Niz zečju rupu

- Digital Cash & Privacy од Хала Финија
- The Case for Privacy од Давида Д. Фридмана
- Protect Your Privacy од Bitcoin.org
- How Lightning Layers Privacy on Top of Bitcoin од Арона ван Вирдума
- Dandelions, and a Bright Future for Bitcoin Privacy од Гаја Свона
- The Case for Electronic Cash од Џерија Бритоа
- We Must Protect our Ability to Transact Privately Online од Џерија Бритоа
- Bitcoin Wiki's Privacy Aritcle од Криса Белчера
- How Private is Bitcoin? од Ерика Вола
- FAQ for Wasabi Wallet од 6102bitcoin
- FAQ for Hodl Privacy од 6102bitcoin
- Bitcoin and Privacy од Едварда Сноудена
- FAQ for Samourai Wallet's Whirlpool од 6102bitcoin
- Universal Declaration of Human Rights од Уједињених Нација
- A lower bound on the length of the shortest superpattern од Anonymous 4chan Poster, Робина Хјустона, Џеја Пејнтона и Винса Ватера
- 🎧 Jameson Lopp on Privacy, Security, and Personal Sovereignty C&G#35 домаћини CryptoDantes i Stigofthepump
- 🎧 6102bitcoin on Bitcoin Privacy, Education, KYC, and Pseudonymity SLP#178 домаћин Стефан Ливера
- American Kingpin - The Epic Hunt for the Criminal Mastermind Behind the Silk Road од Ника Билтона

Лекција 20: Сајферпанкови пишу код

Видим да покушаваш да измислиш нешто.

Као многе велике идеје, Биткоин није дошао ниоткуда. Постао је могућ коришћењем и комбиновањем многих иновација и открића у математици, физици, компјутерској науци, и другим пољима. Иако је без сумње геније, Сатоши не би био у стању да измисли Биткоин без великана на чија рамена се попео.

“Онај ко само жели и нада се не утиче активно на ток догађаја и на обликовање своје сопствене судбине.”
Лудвиг фон Мизес

Један од тих великана је Ерик Хјуз, један од утемељитеља сајферпанк покрета и аутор scајферпанк манифеста. Тешко је замислити да на Сатошија није утицао овај манифест. Он говори о многим стварима које Биткоин омогућава и користи, као што су директне и приватне трансакције, електронски новац и готовина, анонимни системи, и одбрана приватности криптографијом и дигиталним потписима.

“Приватност је неопходна у једном отвореном друштву у електронском добу. […] Пошто прижељкујемо приватност, морамо осигурати да свака странка у трансакцији мора имати сазнање само о ономе што је директно неопходно за ту трансакцију. […]
Према томе, приватност у отвореном друштву захтева анонимни систем трансакције. До сада, примарни такав систем била је готовина. Анонимни систем трансакције није тајни систем трансакције. […]
Ми Сајферпанкови смо посвећени томе да изградимо анонимне системе. Ми бранимо нашу приватност криптографијом, анонимним системима за размени поште, са дигиталним потписима, и са електронским новцем. Сајферпанкови пишу код.”
Ерик Хјуз

Сајферпанкови нису се задовољили надама и жељама. Они активно утичу на ток догађаја и обликују своју сопствену судбину. Сајферпанкови пишу код.

Дакле, у правом сајферпанк стилу, Сатоши је сео и почео да пише код. Код који је узео једну апстрактну идеју и доказао свету да она заиста функционише. Код који је посејао семе нове економске стварности. Захваљујући овом коду, свако може да се увери да овај нови систем заиста ради, а сваких 10 минута или приближно толико Биткоин доказује свету да је још увек жив.

```
map<uint256, CBlockIndex*> mapBlockIndex;
const uint256 hashGenesisBlock("0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f");
CBlockIndex* pindexGenesisBlock = NULL;
int nBestHeight = -1;
uint256 hashBestChain = 0;
CBlockIndex* pindexBest = NULL;
⋮

int64 CBlock::GetBlockValue(int64 nFees) const
{
    int64 nSubsidy = 50 * COIN;

    // Subsidy is cut in half every 4 years
    nSubsidy >>= (nBestHeight / 210000);

    return nSubsidy + nFees;
}

unsigned int GetNextWorkRequired(const CBlockIndex* pindexLast)
{
    const unsigned int nTargetTimespan = 14 * 24 * 60 * 60; // two weeks
    const unsigned int nTargetSpacing = 10 * 60;
    const unsigned int nInterval = nTargetTimespan / nTargetSpacing;

    // Genesis block
    if (pindexLast == NULL)
        return bnProofOfWorkLimit.GetCompact();
```

Изводи кодова из Биткоин верзије 0.1.0

Да би био сигуран да његова иновација превазилази машту и постаје стварност, Сатоши је написао код да имплементира своју идеју пре него што је написао белу књигу. Такође се потрудио да не одлаже заувек његово објављивање. Најзад, "увек ће бити још једна ствар коју треба урадити."

"Морао сам да напишем цео код да уверим себе да могу да решим сваки проблем, онда сам написао књигу."
Сатоши Накамото

У данашњем свету бескрајних обећања и сумњивих извршења, била је очајнички потребна вежба у посвећеном грађењу. Буди решен, убеди себе да можеш заиста да решиш проблеме, и имплементирај решења. Требало би сви да тежимо да будемо мало више сајферпанкови.

Биткоин ме је научио да сајферпанкови пишу код.

Иза огледала 🔍
Пратите чланке који развијају идеје о којима се расправљало у овој лекцији:

- 🔍 Bitcoin Is an Idea

Низ зечју рупу

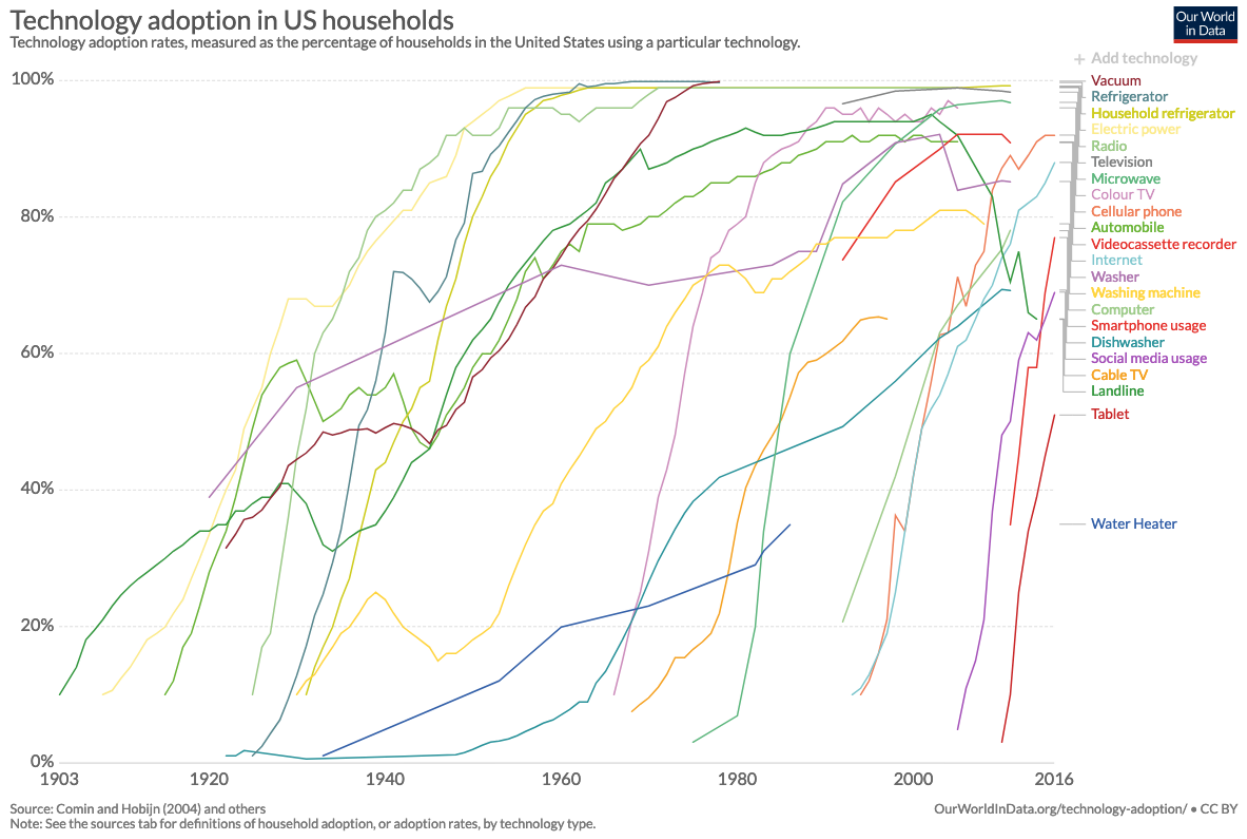
- The Crypto Anarchist Manifesto од Тимотија Ц. Меја
- A Cypherpunk’s Manifesto од Ерика Хјуза
- The Cyphernomicon од Тимотија Ц. Меја
- Bitcoin P2P e-cash paper announcement од Сатошија Накамота
- Bitcoin version 0.1.0 announcement од Сатошија Накамота
- Cypherpunks - Freedom and the Future of the Internet од Јакоба Апелбаума Џулијана Асанжа Ендија Цимермана
- The Book Of Satoshi - The Collected Writings of Bitcoin Creator Satoshi Nakamoto од Фила Чампејна

Лекција 21: Метафоре за будућност Биткоина

Знам да ће се нешто занимљиво сигурно догодити…

У последњих пар деценија, постало је очигледно да технолошке иновације не прате линеарни тренд. Било да верујете у јединство технологије или не, не може се порећи да је напредак експоненцијалан на многим пољима. Не само то, већ се и стопа којом се технологије усвајају убрзава, и пре него што се окренете, ваша деца користе Снепчет радије него да се играју у школском дворишту. Експоненцијалне криве имају обичај да вас тресну у лице још и пре него што видите да наилазе.

Биткоин је експоненцијална технологија изграђена на експоненцијалним технологијама. Our World in Data (Наш свет у подацима) дивно приказује растућу брзину усвајања технологија, почевши од 1903 са увођењем телефонских каблова. Телефонски каблови, струја, компјутери, интернет, паметни телефони; сви они следе експоненцијалне трендове по односу цена-учинак и по прихваћености. И биткоин их прати.



Биткоин је буквално изван мерења.

Биткоин нема један већ [много ефеката мреже](), од којих сви доводе до експоненцијалне шеме раста у својим одговарајућим областима: цена, корисници, безбедност, програмери, удео у тржишту, и прихватање у својству глобалног новца.
Пошто је преживео дечји узраст, Биткоин наставља да расте сваког дана у више од једног аспекта. Признајем, ова технологија није још достигла зрелост. Могла би бити у пубертету. Али ако је технологија експоненцијална, пут од незнаности до свеприсутности је кратак.

Mobile phone, са 1965 vs 2019.

Године 2003 у свом [говору на TED]()-у, Џеф Безос одабрао је струју као метафору за будућност ове мреже. Сва три феномена – струја, интернет, Биткоин – су омогућујуће технологије, мреже које омогућују друге ствари. Оне су инфраструктура за даљу надоградњу, утемељујуће по самој својој природи.

Струја је већ неко време ту. Узимамо је здраво за готово. Интернет је доста млађи, али многи људи га такође већ узимају здраво за готово. Биткоин је стар десет година и ушао је у свест јавности за време последње етапе раста. Само они који су га најраније усвојили узимају га здраво за готово. Како [више времена]() прође, све више и више људи ће препознати Биткоин као нешто што једноставно постоји.

Године 1994, интернет је још збуњујући и тежак за разумевање. Гледајући старе [снимке емисије Today Show]() постаје очигледно да оно што се сматра природним и лаким за схватање данас, у то време уствари није било такво. Биткоин је већини и даље збуњујући и туђ, али баш као што је интернет друга природа за дигиталне урођенике, трошење и [гомилање]() сатова[2] биће друга природа за биткоин урођенике будућности.

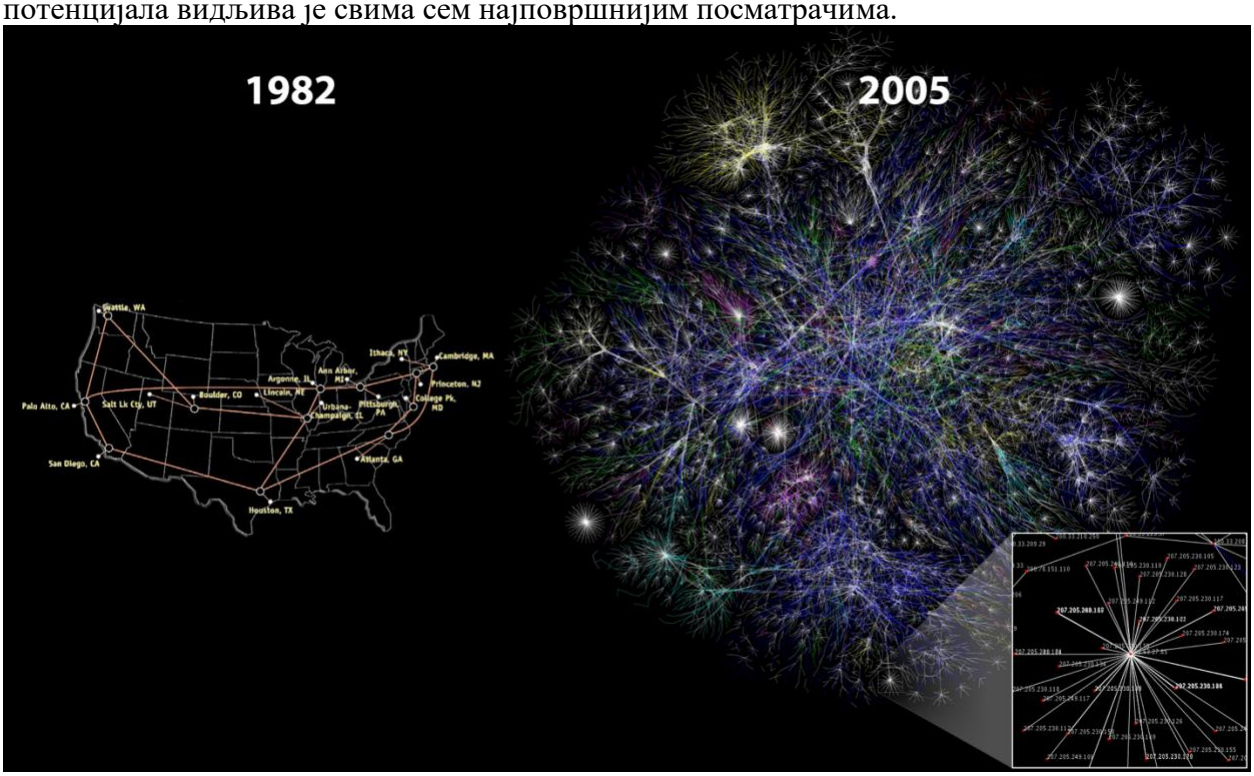
“Будућност је већ овде – само није јако равномерно распоређена”
[Вилијам Гибсон]()

У 1995-ој, око 15% одраслих Американаца користило је интернет. Историјски [подаци из Истраживачког центра Пју]() показују како се интернет уткао у све наше животе. Према

[2] Стомилионити делови биткоина

Prema прегледу корисника од стране Лабораторије Касперски, 13% испитаних користило је Биткоин и његове клонове да плате робу у 2018. Иако плаћање није једини случај коришћења биткоина, то је неки показатељ где смо ми по времену Интернета: у раним до средњим 90-тим.

Године 1997, Џеф Безос је изјавио у свом писму акционарима да "је ово Дан 1 за Интернет," схватајући велики неискоришћени потенцијал интернета и, последично, и његове компаније. Који год ово био дан за биткоин, огромна количина неискоришћеног потенцијала видљива је свима сем најповршнијим посматрачима.

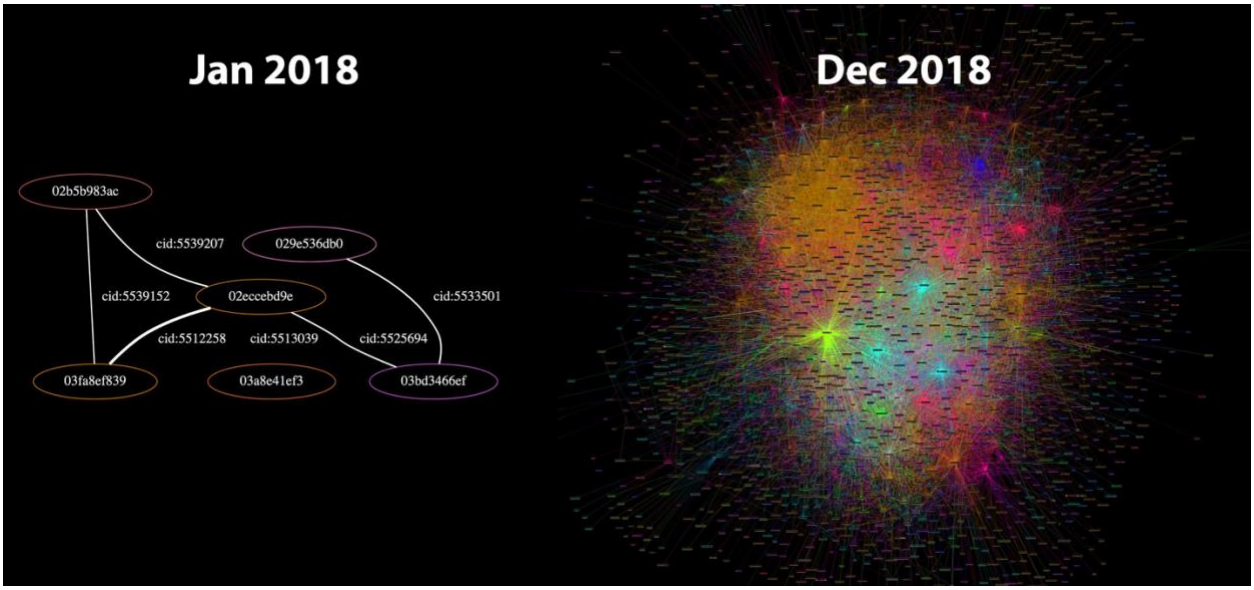


Интернет, 1982 према 2005. Source: cc-by Merit Network, Inc. and Barrett Lyon, Opte Project

Биткоинов први чвор кренуо је онлајн у 2009-ој пошто је Сатоши изрударио блок настанка и пустио софтвер на слободу. Његов чвор није дуго био сам. Хал Фини био је један од првих људи који се ухватио за ту идеју и придружио се мрежи. Десет година касније, када ово пишем, више од 75.000 чворова покрећу биткоин.

Основни ниво овог протокола није једина ствар која расте експоненцијално. Мућевита мрежа, технологија другог нивоа, расте чак и са већом стопом.

У јануару 2018, мућевита мрежа имала је 40 чворова и 60 канала. У априлу 2019, мрежа је нарасла на више од 4000 чворова и око 40.000 канала. Имајте на уму да је ово још експериментална технологија где се може догодити и догађа се губитак фондова. Ипак, тренд је јасан: хиљаде људи је неусттрашиво и жељно да је користи.



Мућевита мрежа, јануар 2018 према децембру 2018. Source: Jameson Lopp

За мене, који сам проживео метеорски успон мреже, паралеле између интернета и Биткоина су очигледне. Оба су мреже, оба су експоненцијалне технологије, и оба обезбеђују нове могућности, нове гране привреде, нове начине живота.

Баш као што је струја била најбоља метафора да се разуме куда иде интернет, интернет би могао бити најбоља метафора да се разуме куда иде Биткоин. Или по речима Андреаса Антонопулоса, Биткоин је *Интернет новца*. Ове метафоре су велики подсетник да иако се историја не понавља, она се често римује.

Експоненцијалне технологије тешке су за схватање и често су подцењене. Иако се јако занимам за те технологије, непрестано сам изненађен стопом напретка и иновација.

Посматрајући како Биткоинов екосистем расте исто је као и посматрати успон интернета у режиму fast-forward. То је веома стимулативно.

Мој пут у покушају да нађем смисао Биткоина водио ме је низ стазе историје на више од једног начина. Разумевање древних друштвених структура, ранијег новца, и начина на који су комуникационе мреже еволуирале, било је део овог путовања. Од секире до паметног телефона, технологија је несумњиво променила наш свет много пута. Мрежне технологије су посебно лаке за трансформацију: писање, путеви, струја, интернет. Све оне су промениле свет. Биткоин је променио мој и наставиће да мења главе и срца оних који се усуде да га користе..

Биткоин ме је научио да је разумевање прошлости неопходно за разумевање будућности. Будућности која упрво почиње.

Иза огледала 🔍
Пратите чланке који развијају идеје о којима се расправљало у овој лекцији:

- 🔍 The World is Waking Up to Bitcoin
- 🔍 Dear Legacy People
- 🔍 Dear Bitcoiners - An optimistic letter to friends and foes around the globe
- 🔍 Dear Family, Dear Friends
- 🔍 On Bitcoin's UX

Низ зечју рупу

- The Electricity Metaphor for the Web's Future од Џозефа Безоса
- How the internet has woven itself into American life од Сузане Фокс и Лија Рејнија
- Hyperbitcoinization од Данијела Кравица
- Speculative Attack од Пјера Рошара
- The 7 Network Effects of Bitcoin од Трејса Мајера
- The Rising Speed of Technological Adoption од Џефа Дежардена
- Hyperbitcoinization - Winner Takes All од Оби Ван Кенобита
- Bitcoin, Not Blockchain од Паркера Луиса
- You Are Not Prepared од Кнута Сванхолма
- Genesis Block од сарадника БиткоинВикија
- Lindy Effect од сарадника Википедије
- Bitcoin and Technology Adoption S-Curves од Биткоин Креза
- 🎧 Murad Mahmudov on The Ultimate Bitcoin Argument
  OTC#25 домаћин Pomp
- 🎧 Bitcoin Tina on Why he is Bullish on Bitcoin
  TFTC#55 домаћин Марти Бент
- 🎧 Pierre Rochard on Hyperbitcoinization and Bitcoin Maximalism
  HF#75 домаћин Деметри Кофинас
- 🎧 Jack Mallers on how Bitcoin Disrupts Payment Clearing Houses
  TIP#BTC007 домаћин Престон Пиш
- 🎧 Jack Mallers on El Salvador's Bitcoin Standard
  WBD#362 домаћин Петер Мек Кормак

Закључак

Научене лекције

"Почни од почетка," рече Краљ, врло озбиљно, "и настави док не дођеш до краја: онда стани."

Као што сам поменуо на почетку, мислим да ће сваки одговор на питање "*Шта сте научили од Биткоина?*" увек бити непотпун. Нешто што се може посматрати као симбиоза више живих система—Биткоин, техносфера и економија—сувише је испреплетано, теме су сувише бројне, а ствари се крећу сувише брзо да би их икада могла потпуно разумети једна особа.

Чак и ако га не разумемо потпуно, и чак са свим његовим ћудима и привидним недостацима, Биткоин без сумње функционише. Он наставља да производи блокове отприлике сваких десет минута и то ради дивно. Што дуже Биткоин настави да ради, то ће више људи одабрати да га користи.

"Истина је да су ствари дивне када раде. Уметност је функција."
Ђанина Браски

Биткоин је дете интернета. Он расте експоненцијално, замућујући границе између разних дисциплина. Није јасно, на пример, где се завршава царство чисте технологије а где почиње друго царство. Иако Биткоин захтева компјутере да би ефикасно функционисао, компјутерска наука није довољна да би се он разумео. Биткоин није само без граница у погледу свог унутрашњег рада већ је такође неограничен у погледу академских дисциплина.

Економија, политика, теорија игара, историја новца, историја, теорија мрежа, финансије, криптографија, информациона теорија, цензура, право и прописи, људске организације, психологија—све ово и више, области су експертизе које би могле помоћи у потрази за разумевањем тога како ради Биткоин и шта је Биткоин.

Није један изум одговоран за његов успех. Он је комбинација већег броја претходно неповезаних делова, слепљених заједно игром теоријских подстицаја, који чине револуцију која је Биткоин. Дивна мешавина многих дисциплина је оно што Сатошија чини генијем.

Као и сваки сложени систем, Биткоин мора да прави компромисе у погледу ефикасности, цене, безбедности, и многих других својстава. Као што и нема савршеног решења да се извуче квадрат из круга, било које решење за ове проблеме које Биткоин покушава да реши биће такође несавршено
.

“Ја не верујем да ћемо више икада имати добар новац док не узмемо ту ствар из руку владе, то јест, не можемо га насилно узети из руку владе, све што можемо да урадимо јесте да неким лукавим заобилазним путем уведемо нешто што они не могу да зауставе.”
Фридрих Хајек

Биткоин је тај потајни, заобилазни пут поновног увођења доброг новца у свет. Он то чини тако што поставља сувереног појединца иза сваког чвора, баш као што је Да Винчи покушао да реши неухватљив проблем квадратуре круга тако што је ставио витрувијанског човека у његов центар. Чворови ефикасно уклањају сваки концепт центра, стварајући систем који је запањујуће не-крхак и кога је јако тешко укинути. Биткоин живи и његови откуцаји срца вероватно ће трајати дуже од свих наших.

Надам се да сте уживали у овој двадесет једној лекцији. Можда је најважнија лекција да би Биткоин требало испитивани холистички, са више углова, ако би човек желео да има нешто што се приближава комплетној слици. Баш као што уклањање једног дела из комплексног система уништава целину, испитивање изолованих делова Биткоина изгледа да затамњује право сазнање о њему.

Ако барем једна особа избрише “blockchain” (блоковски ланац) из свог речника и замени га са “a chain od blocks” (ланац блокова) ја ћу умрети као срећан човек.

У сваком случају, моје путовање се наставља. Намеравам да се усудим још дубље у ову зечју рупу, и позивам вас да се прикачите да вас повезем.

Изјаве захвалности

"Хвала вам," рече Алиса

Хвала безбројним ауторима и стваоцима садржаја који су утицали на моје размишљање о Биткоину и темама које он дотиче. Има их сувише много да би их све набројао, али дађу све од себе да именујем доста њих.

- Хвала Арџуну Балаџију за твит који ме је мотивисао да напишем ово.
- Хвала Мартију Бенту што је обезбедио бескрајно много хране за размишљање и за забаву. Ако нисте претплаћени на билтен Мартија Бента (Marty's Bent) и Tales From The Crypt (Приче из крипте), пропуштате много. Живели Мат и Марти што нас водите кроз зечју рупу.
- Хвала Мајклу Голдстајну и Пјеру Рошару за селекцију и обезбеђивање највеће литературе о Биткоину преко Накамото института. И хвала вам за креирање подкаста Noded Podcast који је значајно утицао на моје филозофске погледе на Биткоин.
- Хвала Питеру Мек Кормаку за његове поштене твитове и за подкаст What Bitcoin Did (Шта је Биткоин учинио), који наставља да пружа сјајне погледе на многе области.
- Хвала Андреасу М. Антонопулосу за сав образовни материјал који је објавио током година.
- Хвала Саифедину Амоусу за његова уверења, бесне твитове, и писање Стандарда Биткоина.
- Хвала Франсису Пулиоу што је поделио своје узбуђење због открића о временском ланцу.
- Хвала Јанику, Брендону, Мату, Камилу, Данијелу, Мајклу и Рафаелу за повратне одговоре на прве верзије неких лекција. Посебно хвала Јанику који је редиговао велики број верзија велики број пута.
- Хвала Друву Бансалу и Мату Оделу што су одвојили време да продискутују неке од идеја са мном.
- Хвала Гају Свону што је направио аудиоверзију 21lessons.com.
- Последње али не и најбезначајније, хвала свим Биткоин максималистима, шиткоин минималистима, преварантима, ботовима и постављачима безвезних постова који обитавају у дивној башти која је Биткоин твитер. И коначно, хвала *вама* што сте ово прочитали. Надам се да сте уживали исто колико и ја док сам га писао. Слободно ме потражите на твитеру. Моје Директне поруке су отворене.