21 Lecke

Mit tanultam meg, miután lemerészkedtem a nyúl üregébe?

Gigi

21 Lessons – What I've Learned from Falling Down the Bitcoin Rabbit Hole, 2019

https://21lessons.com

Magyar fordítás, Hungarian translation: Pásztor Miklós, 2021

https://coincrumb.com

Előszó

A kis Alice esik
le-
felé
a
lyuk-
ba,
beütve a fejét és felhorzsolva a lelkét.

Beleesni a Bitcoin nyúlüregébe furcsa élmény. Sokakhoz hasonlóan én is úgy érzem, az elmúlt pár évben többet tanultam a Bitcoin segítségével, mint előtte két évtizedet eltöltve az iskolarendszerben.
Az itt olvasható sorok az általam megtanult dolgok összegzése. Előzőleg cikksorozatként írtam meg ezt, ami most előtted van, az már az átdolgozott, második változat.

A Bitcoinhoz hasonlóan, ezek a leckék sem statikus dolgok. Időről időre frissítem ezeket, bővítem az új információkkal.
A Bitcoinnal ellentétben viszont ezek a leckék nem kell, hogy visszamenőleg kompatibilisek legyenek. Lehet, hogy néhányat kibővítek, átdolgozok, vagy lecserélek majd. A kézzel fogható, fizikai kiadás is a terveim között szerepel.

A Bitcoin fáradhatatlan tanár, ezért nem mondhatom, hogy a leckék teljesek, és minden téren kielégítőek. Ezek az én személyes tanulási folyamatomra reflektálnak, ezeken kívül pedig rengeteg más dolgot is megtanulhatunk. Mások esetleg egészen különböző dolgokkal találkoznak, amikor belépnek a Bitcoin világába.

Remélem, hasznosnak fogod találni ezeket a leckéket, és az olvasással tanulás nem lesz olyan nehéz és fájdalmas, mint nekem első kézből megszerezni ezeket a tapasztalatokat.

Gigi

– Megmondanád nekem, kérlek, melyik úton tudok innen kijutni?
– Az attól függ, hogy merre szeretnél továbbmenni.
– Nem igazán számít, hogy hová jutok…
– Akkor nem igazán számít, hogy melyik úton indulsz el.

Tartalomjegyzék

Előszó ... 3
Bevezető ... 5
Első rész, filozófia ... 7
Első lecke: A megváltoztathatatlanság és a változtatás ... 9
Második lecke: A korlátozottság hiánya ... 11
Harmadik lecke: Az elhelyezkedés és a másolatok ... 12
Negyedik lecke: Az azonosítás problémája ... 14
Ötödik lecke: Egy hibátlan terv ... 15
Hatodik lecke: A szavak ereje ... 16
Hetedik lecke: A tudás határai ... 18
Második rész, közgazdaságtan ... 19
Nyolcadik lecke: A pénzügyi tudatlanság ... 20
Kilencedik lecke: Infláció ... 22
Tizedik lecke: Érték ... 25
Tizenegyedik lecke: Pénz ... 26
Tizenkettedik lecke: A történelem, és a pénz bukása ... 28
Tizenharmadik lecke: A frakcionált banki tartalék őrültsége ... 33
Tizennegyedik lecke: A stabil pénz ... 36
Harmadik rész, technológia ... 41
Tizenötödik lecke: A számok ereje ... 42
Tizenhatodik lecke: Ne bízz! Bizonyosodj meg! ... 46
Tizenhetedik lecke: Tudnunk kell a pontos időt ... 50
Tizennyolcadik lecke: Mozogj lassan, nehogy valamit összetörj! ... 52
Tizenkilencedik lecke: A magánszféra még nem veszett el ... 55
Huszadik lecke: A cypherpunkok kódokat írnak ... 57
Huszonegyedik lecke: Metaforák a Bitcoin jövőjéről ... 59
Összegzés ... 63

Bevezető

– De én nem akarok őrültek között lenni! – jelentette ki Alice.
– Ezzel nem tudsz mit kezdeni, – szólt a macska – *mi itt mind őrültek vagyunk. Én is őrült vagyok. Te is őrült vagy*.
– Miért gondolod, hogy én is őrült vagyok? – kérdezte Alice.
– Annak kell lenned, – szólt a macska – *különben nem jöttél volna ide.*

2018 októberében megkérdezték tőlem, hogy mit tanultam a Bitcointól. Mikor megpróbáltam egy rövid tweetben válaszolni erre, csúfosan elbuktam. Rájöttem, hogy olyan sok mindent tanultam, hogy erre a kérdésre nem tudok gyorsan és tömören válaszolni, sőt, lehet, hogy egyáltalán nem tudok.
A megtanultak mind a Bitcoinról szólnak, vagy legalább kapcsolódnak hozzá. Ennek ellenére néhány lecke, amely a Bitcoinról szól, nem foglalkozik azzal, hogy hogyan működik a rendszer, vagy, hogy egyáltalán mi a Bitcoin. Inkább azt segíthetnek megérteni, hogy a Bitcoin hogyan fonódik össze a filozófiával, a közgazdaságtannal, és a technológiai innovációkkal.

A 21 Lecke három, egyenként hét fejezetet tartalmazó részre tagolódik. Minden részben más nézőpontból vizsgáljuk meg a Bitcoint, és megnézzük, a különböző irányokból milyen különböző képeket mutat nekünk a hálózat.

Az első részt a filozófiának szenteltem. Mit is jelent a megváltoztathatatlanság, a valódi korlátozottság, a Bitcoin hibátlan felépítése? Mi a baj a személyazonossággal, miért problémás a lokalitás? Miért fontos a szólásszabadság, és miért limitált a tudásunk?

A második rész a gazdaság lencséjén keresztül vizsgálja a dolgokat. Mi a pénzügy, az infláció, az érték, a pénz és a pénz története, hogyan működnek a bankok? Hogyan hozta létre a Bitcoin ismét a stabil, megbízható pénzt, egyfajta kerülőút alkalmazásával?

A harmadik rész a technológiával foglalkozik. Miért bízhatunk a számokban, és miért kell egyáltalán bizalom? Miért kell munka, és hogyan jön be a képbe az idő, hogyan mozogjunk lassan, hogy ne törjünk össze dolgokat, és ez miért nem hiba? Mit mond nekünk a Bitcoin a magánszféráról, kik azok a cypherpunkok, és miért írnak kódokat? Végül pedig mi várhat ránk a Bitcoin jövőjében?

Minden leckében találsz idézeteket, linkeket. Ha egy témáról részletesebben is beszéltem már, az „A tükörben”című részben lévő linkek elirányítanak oda, az angol nyelvű cikkhez. Ha ennél is mélyebbre ásnál, „A nyúlüregnek nincsen alja” szekcióban pedig további releváns anyagokat találhatsz, angol nyelven.

Könnyebb dolgod lesz, ha van már némi előzetes tudásod a Bitcoinról, de a leckéket úgy írtam, hogy bármely érdeklődő olvasó élvezhesse azokat. A leckék között lehet összefüggés, de egyenként, önmagukban is megállják a helyüket. Igyekeztem kerülni a szakzsargont, de néhány kifejezést mindenképpen használni kell.
Remélem, ezek a sorok inspirációként szolgálnak mások számára, hogy még mélyebbre merüljenek, ha kérdéseik lennének, ne csak a felszínt kapargassák. Én számos tartalomkészítőtől és szerzőtől kaptam ihletet, és mindegyiküknek örök hálával tartozok.

Végül pedig fontosnak tartom megjegyezni, hogy nem azért írom ezeket a sorokat, hogy bármiről is meggyőzzelek. Az a lényeg, hogy elgondolkodtassalak, és megmutassam, a Bitcoinban sokkal több rejtőzik, mint amennyit elsőre láthatunk. Még csak meg sem tudom mondani neked, hogy mi a Bitcoin, vagy, hogy mit taníthat számodra. Erre magadnak kell rájönnöd.

„Innen nincs visszaút. Ha a kék pirulát választod, a mesének vége, reggel felébredsz az ágyadban, és éled tovább az életed, ahogyan eddig. Ha a piros pirulát választod, akkor itt maradsz Csodaországban, én pedig megmutatom, milyen mély a nyúl ürege."

Morpheus

Első rész, filozófia

Az egér kérdőn nézett rá, és mintha kacsintott volna az egyik apró szemével, de nem mondott semmit.

Ha csak egy futó pillantást vetünk a Bitcoinra, akkor azt láthatjuk, hogy lassú, pazarló, túlbiztosított, és elképesztően paranoid. De ha valódi kíváncsisággal fordulunk felé, észrevehetjük, hogy a dolgok nem olyanok, mint első ránézésre.

A Bitcoinnak van az a tulajdonsága, hogy fogja az emberek feltevéseit, és a feje tetejére állítja azokat. Mikor kicsit képbe kerülsz, és úgy érzed, megértetted az összefüggéseket, a Bitcoin megint beront a szobába, mint az elefánt a közmondásos porcelánboltba, és szétzúzza az elméleteket, ismét.

Vak szerzetesek próbálják értelmezni, hogy milyen egy elefánt

A Bitcoin számos tudományágra épül. Mint ahogyan a régi kínai mesében a vak szerzetesek az egyes testrészek alapján próbálják elképzelni, hogy hogyan is néz ki egy elefánt, úgy a Bitcoint tanulmányozók is egy-egy speciális nézőpontból indulnak ki. Ezért pedig mindenki más következtetésre jut, hogy miféle bestia is ez.

Az itt következő leckék azokról a feltevéseimről szólnak, amelyeket a Bitcoin darabokra szedett. Filozófiai gondolatok négy fejezetben a megváltoztathatatlanságról, a szűkösségről, a

lokalitásról és a személyazonosságról. Az ötödikben a Bitcoin létrehozásának a lenyűgöző történetét vesszük át, a két utolsó lecke pedig a szólásszabadságról és az egyéni tudás korlátairól szól, ezek a nyúlüreg feneketlen mélységére reflektálnak. Szóval vesd bele magad a lyukba, és élvezd a zuhanást!

Első lecke: A megváltoztathatatlanság és a változtatás

„Azon tűnődöm, hogy megváltoztam-e az éjszaka során? Hadd gondolkozzak! Ugyanaz voltam, mint aki ma reggel felébredt? Úgy gondolom, emlékeznék rá, ha valaki más lettem volna. De ha mégsem vagyok ugyanaz, akkor ki vagyok valójában?
Ez ám az igazi kérdés!”

Nagyon nehéz meghatározni, hogy mi a Bitcoin. Nagyon új dolog, és minden jellemzés megpróbálja valami régi, ismert dologhoz hasonlítani, így hívták már digitális aranynak és az internet pénzének is. Mindegy, hogy kinek mi a kedvenc hasonlata, két dolog alapvetően létfontosságú a Bitcoinhoz, a decentralizáció és a megváltoztathatatlanság.

Úgy is lehet gondolkodni a Bitcoinról, hogy az egyfajta automatizált társadalmi szerződés. A szoftver maga csak egy része az összképnek, és ha úgy akarjuk megváltoztatni a Bitcoint, hogy megváltoztatjuk a programkódot, hasztalan próbálkoznánk. Minden változtatásról meg kellene győznünk a hálózat összes többi résztvevőjét, hogy fogadják el. Ez pedig pszichológiai kérdés, nem technológiai. A következő kijelentés esetleg abszurdnak tűnhet, mint sok minden más is a Bitcoinnal kapcsolatban, de attól még igaz: nem fogod megváltoztatni a Bitcoint. Az fog megváltoztatni téged.

„A Bitcoin jobban meg fog változtatni minket, mint amennyire mi meg tudjuk változtatni a Bitcoint.”

Marty Bent

Sokáig tartott, mire elfogadtam ennek a valóságát. A Bitcoin csak egy program, ráadásul nyílt forráskódú, tehát bármikor megváltoztathatod, nem igaz? Nem, nem igaz. Nagyon nem. Nem meglepő módon a Bitcoin létrehozója is tisztában volt ezzel.

„A Bitcoin természete olyan, hogy már a 0.1-es verzió kiadásakor kőbe lettek vésve a fő működési szabályok, véglegesen.”

Satoshi Nakamoto

Rengetegen próbálták már megváltoztatni a Bitcoint. Mindegyikük elbukott. Végtelen mennyiségben sorakoznak a forkok és az altcoinok, a Bitcoin mégis itt van, és ugyanúgy teszi a dolgát, mint az első csomópont elindulásakor. Hosszú távon az altok nem fognak számítani. A forkok kihalnak. A Bitcoin számít. Addig, amíg az univerzumunk matematikai és fizikai törvényei nem változnak meg, addig a Bitcoin itt lesz és működni fog.

„A Bitcoin olyan, mint egy új életforma. Az interneten él, azzal együtt lélegzik. Azért él, mert fizetni tud az embereknek, hogy életben tartsák. Nem lehet megváltoztatni. Nem lehet vitatkozni vele. Nem lehet manipulálni. Nem lehet korrumpálni. Nem lehet leállítani. Ha egy atomháború elpusztítaná a bolygó felét, a Bitcoin akkor is itt lenne, és tovább működne.”

Ralph Merkle

A Bitcoin hálózata túl fog élni mindannyiunkat. Mikor ezt megértettem, az jobban megváltoztatott engem, mint előtte a világon bármi. Megváltozott az időperspektívám, megváltoztak a pénzügyi ismereteim, a politikai nézeteim, és még sok minden más is. Vannak, akiknek még az étrendjét is megváltoztatta. Neked is őrültségnek hangzik, mint nekem? Az is, őrültség, de mégis ez történik.

Megtanultam, hogy a Bitcoin nem fog változni. Én fogok.

***

A tükörben:

Bitcoin's Gravity - How idea-value feedback loops are pulling people in

Proof of Life – Why Bitcoin is a Living Organism

The Bitcoin Journey

Második lecke: A korlátozottság hiánya

Ez már elegendőnek tűnik – remélem, nem kell még nagyobbra nőnöm…

Általánosságban véve, a technológia bőséget hoz az emberiség számára. Egyre több és több ember élvezheti a modern világ előnyeit, olyan módon, amely azelőtt luxusnak számított. Hamarosan úgy élhetünk majd, ahogyan régen a királyok, és néhányunk már most is úgy él. Ahogyan Peter Diamandis írta az Abundance, Bőség című könyvében, „a technológia felszabadítja az erőforrásokat, és amiből régen kevés volt, az most bőségesen a rendelkezésünkre áll".

A Bitcoin, mint fejlett technológia, megtöri ezt a trendet, és létrehoz egy olyan dolgot, amely viszont ténylegesen korlátozott. Egyesek azt mondják, hogy az egész univerzumban ez a dolog a legkorlátozottabb. Egyszerűen nem lehet növelni a készletet, nem számít, mekkora erővel próbálkozunk.

„Mindössze két dolog létezik, amelyik ténylegesen korlátozott. Az idő és a bitcoin."

Saifedean Ammous

Önellentmondásnak tűnik, hogy a Bitcoin ezt a másolás segítségével éri el. A tranzakciókat kihirdetik a hálózaton, a blokkokat mindenki rögzíti a saját főkönyvébe, ez az elosztott főkönyv pedig, nos, tényleg elosztott. Csinos szakkifejezések, amelyek valójában azt jelentik, hogy mindenki lemásolja magának az adatokat. A Bitcoin annyi számítógépre másoltatja fel magát, amennyire csak lehetséges, és pénzügyileg motiválja a felhasználókat, hogy bányásszanak vagy csomópontot futtassanak. Ez a rengeteg másolás pedig kitűnően biztosítja a szűkösséget.

A bőség korában a Bitcoin megtanította, hogy mit jelent a korlátozottság.

Harmadik lecke: A lokáció

Egyszer csak egy dühös hang hallatszott, a nyúlé – *Pat, Pat! Merre vagy?*

Ha nem vesszük számításba a kvantum-mechanikát, a fizikai világban könnyű meghatározni, hogy mi hol van. A kérdés, hogy „Hol van X?”, egyszerűen megválaszolható, függetlenül attól, hogy X egy személy, vagy esetleg egy hely. A digitális világban a lokáció, az elhelyezkedés már kicsit trükkösebb dolog, de nem lehetetlen válaszolni rá.

Hol vannak az emailjeink például? Az, hogy a felhőben, az rossz válasz, hiszen csak annyit jelent, hogy valaki más gépén. Persze, ha nagyon akarod, be lehet azonosítani minden egyes készüléket, amely a leveleidet tárolja, és meghatározni azok földrajzi helyét. A bitcoin esetében az elhelyezkedés viszont nagyon trükkös. Hol is van a bitcoinod?

„Kinyitottam a szemem, körülnéztem, és feltettem a legegyértelműbb, hagyományos, legvalószínűbb kérdést: Hol vagyok?”

Daniel Dennett

Itt két féle probléma is felmerül. Az elosztott főkönyv ténylegesen elosztott, tehát minden egyes gépen megtalálható a teljes, hiánytalan másolata. Másodszor pedig bitcoin nem létezik. Nem fizikálisan nem létezik, hanem technikailag sincs olyan dolog, hogy bitcoin.

A Bitcoin, mint elosztott főkönyv, nyilvántartást vezet az úgynevezett elköltetlen tranzakciós kimenetekről, az UTXO-król, és szót sem ejt semmiről, amely akár csak hasonlítana bitcoinra. A bitcoin létezését úgy állapítjuk meg, hogy az UTXO-k csoportjának minden 100 milliós egységét bitcoinként definiáljuk.

„Hol van a bitcoin ebben a pillanatban? Nos, nincs bitcoin. Egyszerűen csak nincs ilyesmi. Nem létezik. Bejegyzések vannak az elosztott főkönyvben, amelynek nincs meghatározott földrajzi lokációja. De azt is mondhatjuk, hogy valójában mindenhol ott van. Földrajzilag ennek nincs sok értelme, és abban sem segít, hogy rájöjj, mit is csinálsz itt.”

Peter Van Valkenburgh

Szóval, ha nincs is bitcoin, akkor mit birtokolsz, amikor azt mondod, hogy van bitcoinod? Mikor létrehozol egy tárcát, kapsz egy seed-sort, egy tucatnyi fura szót, amelyet a meghatározott sorrendben kell leírni. Ezek hozzák létre a privát és a publikus kulcsod, és úgy működnek, mint egy varázsige, lehetővé teszik számodra, hogy bitcoint „küldj” másoknak. Azaz bejegyzést hozz létre az elosztott főkönyvben. Ilyen értelemben nézve a privát kulcsod maga a bitcoinod.

Ha szerinted ezt rosszul gondolom, nyugodtan küldd el nekem a privát kulcsaidat.

A Bitcoin megtanította nekem, hogy az elhelyezkedés kérdése tényleg trükkös dolog.

***

A tükörben:

The magic dust of cryptography

Negyedik lecke: Az azonosítás problémája

Ki vagy te? – kérdezte a hernyó.

Nic Carter írt egy nagyon jó filozófiai értekezést, amelyben megpróbálta megválaszolni a kérdést, hogy vajon milyen lehet Bitcoinnak lenni? Ahogy rávilágított, a nyílt, publikus blokkláncok, mint amilyen a Bitcoin is, szembekerülnek a Tézeusz hajója néven ismert talánnyal. Felmerül tehát a kérdés, melyik az igazi Bitcoin?

„Elég csak arra gondolni, hogy a Bitcoin alkotóelemei közül mennyire kevés az eleve benne lévő. A teljes kódbázisa újra lett írva. Meg lett változtatva. Ki lett bővítve. Így már alig hasonlít az első, az eredeti verzióra. A főkönyv maga, hogy ki mit birtokol, ténylegesen az egyetlen eleme az egész hálózatnak, amely a kezdetek óta változatlan. Hogy a Bitcoin valóban irányítás nélkül működhessen, ellen kell állni a kísértésnek, hogy bárki olyan pozícióba kerüljön, hogy meghatározhassa, melyik lánc az igazi, máshogyan kell ezt megoldani."

Nic Carter

Úgy tűnik, a technológia fejlődése rákényszerít minket, hogy komolyan vegyük ezeket a filozófiai kérdéseket. Előbb vagy utóbb az önvezető autók is szembesülni fognak azzal, hogy egy balesetet csak egy másik baleset árán tudnának elkerülni. Nem fognak tudni megállni, és el kell dönteniük, kit ütnének el inkább, ki élhet, és ki hal meg.

A kriptopénzek az első szándékosan előidézett hard fork óta rákényszerítik az embereket, hogy igenis foglalkozzanak ezekkel a kérdésekkel. Érdekes, hogy az eddigi két legnagyobb jelentőségű hard fork esetén két különböző válasz született ebben a kérdésben. 2017 augusztus elsején a Bitcoin két táborra szakadt, mikor a láncot kettéválasztották. A piac úgy döntött, hogy a módosítatlan, változatlan lánc lesz az eredeti Bitcoin. Egy évvel korábban, 2016 októberében az Ethereum vált kétfelé. A piac akkor viszont úgy döntött, a módosított láncot fogja eredeti Ethereumként folytatni.

Ha egy rendszer ténylegesen decentralizált, akkor időről időre fel kell merülnie a „Tézeusz hajója" kérdéskörnek, egészen addig, amíg a hálózat létezik.

A Bitcoin megtanította, hogy a decentralizáció nem teszi könnyebbé a dolgok meghatározását.

Ötödik lecke: Egy hibátlan terv

Elvesztették a fejüket, – kiáltották vissza a katonák…

Mindenki szereti a jó történeteket. A Bitcoin eredetmítosza különösen lenyűgöző, és az egyes részletek fontosabbak, mint elsőre gondolhatnánk. Kicsoda Satoshi Nakamoto? Egyetlen személy, vagy esetleg egy csoport? Férfi vagy nő? Időutazó földönkívüli, esetleg egy fejlett mesterséges intelligencia? Elméleteink lehetnek, de valószínű, hogy az igazságot sosem fogjuk megtudni. Ez pedig nagyon fontos tényező!

Satoshi szándékosan maradt névtelen. Elültette a Bitcoin magját, a környékén maradt, hogy megbizonyosodjon, a rendszer nem fog leállni rögtön a kezdeti fázisban. Végül nyomtalanul eltűnt. Ez furcsa, ködösítő viselkedésnek tűnhet, de valójában szükségszerű ahhoz, hogy egy rendszer ténylegesen decentralizált lehessen.

Nincs központi irányító. Nincs felügyelő hatóság. Nincs feltaláló. Nincs senki, akit le lehetne tartóztatni, megkínozni, megzsarolni, bebörtönözni. Hibátlan koncepció egy technológia számára.

„Az egyik legnagyobb dolog, amit Satoshi tett, az eltűnése volt."

Jimmy Song

A Bitcoin létrehozása óta ezernyi más kriptopénz született meg. Egyik ilyen klón sem osztozik a Bitcoin eredet-történetén. Ha valaki túl akarja szárnyalni a Bitcoint, az eredetmítosszal kell kezdenie. Az ötletek harcában pedig minden a körítésről, a narratíváról szól.

„Az arany eredetileg csak az ékszerekhez volt használva, aztán pedig a cserekereskedelemben vett részt az elmúlt 7000 évben. A magával ragadó csillogása miatt az volt a meggyőződés, hogy az istenek ajándéka az emberiség számára."

Arany: A különleges fém

Ahogyan régen az arany, most a Bitcoin is lehetne az istenek ajándéka. Az arannyal ellentétben a Bitcoin eredete viszont kifejezetten emberi történet. Azt is tudjuk, hogy kik a fejlesztés istenei: átlagemberek szerte a világról, ismert szakértőként, vagy névtelenül.

A Bitcoin megtanította a narratíva fontosságát.

Hatodik lecke: A szavak ereje

Elnézésedet kérem, – mondta az egér, mogorván bár, de nagyon udvariasan, – *te szóltál?*

A Bitcoin egy ötlet. Egy olyan ötlet, amelyik a jelenlegi formájában nem más, mint egy szavakkal irányított gép. A Bitcoin minden egyes része szavakkal működik. A white paper szavakból áll. A szoftver, amely a működését kódolja, szavakból épül fel. A főkönyv szavakból áll. A tranzakciókhoz is szavakat használunk, valamint a publikus és privát kulcsaink is szavak. A Bitcoin szavakból áll, és ezért tulajdonképpen olyan, mint a beszéd.

„A Kongresszus nem hozhat törvényt a vallások ellen, és nem tilthatja meg a szabad vallásgyakorlást. Nem korlátozhatja a szólásszabadságot, a sajtószabadságot, a gyülekezéshez való jogot, és azt, hogy az emberek petíciót nyújthassanak be a kormányzat számára, változtatásokat követelve."

Az Amerikai Egyesült Államok Alkotmányának első kiegészítése

A Bitcoin háborújának a végső harcaira még nem került sor, de azt tudni kell, hogy egy ötletet nagyon nehéz megállítani. Főleg egy olyan ötletet, amely nem más, mint szavak küldözgetése egymás között. Minden alkalommal, mikor egy kormányzat megpróbálja korlátozni a beszédet és a szavakat, még mélyebbre merülnek a nevetségesség és az abszurditás mocsarában, amely olyan ostobaságok lelőhelye, mint az illegális számok, vagy az illegális prímek.

Egészen addig, amíg a világnak van olyan része, ahol a szólásszabadság ténylegesen szabadságot jelent, addig a Bitcoin megállíthatatlan.

„Nincs olyan része a bitcoin tranzakcióknak, ahol nem szavakat használunk. Mindig szavakkal működik. A Bitcoin szavakból áll. A Bitcoin beszéd. Nem lehet szabályozni az olyan szabad országokban, mint amilyen az USA, hiszen az állampolgároknak elidegeníthetetlen jogaik vannak, amelyeket az Alkotmány is szavatol."

Beautyon

A Bitcoin megtanított rá, hogy egy szabad országban a szólászabadság és a nyílt forráskódú programok megállíthatatlanok.

***

A tükörben:

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

Hetedik lecke: A tudás határai

Egyre csak lefelé, lefelé. Sosem fog véget érni a zuhanás?

Belemerülni a Bitcoin világába megrendítő élmény lehet. Azt hittem, tudok ezt-azt. Azt hittem, jó oktatást kaptam. Azt hittem, értek a számítástechnikához, ha máshoz nem is. Évekig tanultam, szóval mindent tudnom kell a digitális aláírásokról, hashelésről, titkosításról, a hálózatról és a biztonságról, nem igaz?
Nem.
Megtanulni az alapokat, amelyekre a Bitcoin működése épül, nehéz. Teljes mélységében megérteni mindegyiket pedig nem egyszerűen nehéz, hanem valószínűleg lehetetlen.

„Senki sem találta még meg a Bitcoin nyúlüregének az alját."

Jameson Lopp

A könyvek listája, amelyeket el szeretnék olvasni, gyorsabban bővül, mint amilyen gyorsan olvasni tudok. Az esszék, cikkek listája pedig gyakorlatilag végtelen. Több podcast létezik, mint amennyit meg tudnék hallgatni. Ez elképesztő, tényleg. Ráadásul a Bitcoin fejlődik is, és majdnem lehetetlen lépést tartani az innovációval, követni az újdonságokat. Még el sem igazán ült a por, amelyet a Bitcoin főhálózatának a létrehozása felvert, de az emberek már második réteget építettek rá, és a harmadikon dolgoznak.

A Bitcoin megtanított rá, hogy a tudásom korlátozott. Megtanította, hogy a nyúl ürege feneketlen.

***

A tükörben:

Bitcoin's Eternal Struggle – How Bitcoin thrives on the Edge between Order and Chaos

Második rész, közgazdaságtan

Egy hatalmas rózsafa állt nem messze a kert bejáratától. Fehér rózsák nőttek rajta, de három kertész azon igyekezett, hogy vörösre fesse az összeset. Alice ezt kifejezetten érdekesnek találta…

A pénz nem a fákon terem. Ostobának kell lenni, hogy ezt higgyük, a szüleink pedig biztosra mentek, hogy megtanuljuk ezt a nagy igazságot, ezért mantraként ismételgették nekünk egész gyerekkorunkban. Arra bátorítottak, hogy bölcsen osszuk be a pénzt, ne szórjuk el felelőtlenül, és takarékoskodjunk a jó időkben, hogy könnyebben átvészelhessük a nehéz időket. Hiszen a pénz nem a fákon terem.

A Bitcoin többet tanított a pénzről, mint amennyiről úgy gondoltam, hogy tudnom kellene. Rákényszerültem, hogy foglalkozzak a pénz történetével, a bankok működésével, a közgazdaságtannal, és sok más dologgal is. Az út, amely a Bitcoin megértéséhez vezet, számtalan irányba ágazik el, és ebben a részben néhányat közelebbről is szemügyre veszünk.

Az első hét leckében filozófiai kérdéseket jártunk körbe. Ebben a hét leckében viszont a pénzt és a gazdaságot vesszük górcső alá. Ahogyan már említettem korábban, csak a felszínt tudjuk megkapargatni. A Bitcoin olyan, mint egy szélesen elterülő folyó, amely ráadásul mély is. Nincs rá mód, hogy minden aspektusát érinthessük egyetlen cikkben, esszében, vagy akár könyvben. Kétlem, hogy egyáltalán lehetséges lenne ez.

A Bitcoin a pénz következő evolúciós lépcsőfoka. Emiatt a megértéséhez érteni kell a közgazdaságtanhoz is. A helyén kell kezelni az emberi tevékenységeket és a résztvevőket a gazdaságnak nevezett hatalmas kirakósban, márpedig a gazdasági vonatkozások adják a Bitcoin saját kirakósának talán a legnagyobb részét.

Hadd mondjam el ismét, ezek a leckék azt tükrözik, hogy én miket tanultam meg a Bitcointól. Az én saját utazásom a nyúl üregébe, és az, amit felhoztam onnan. Márpedig én nem vagyok közgazdász. Határozottan kiléptem a komfortzónámból, és szinte biztos, hogy a tudásom, a megértésem hiányos. Megpróbálom kihozni a maximumot abból, amit elértem, még ha ezzel nevetségessé is válhatok. Végülis eleve a választ keressük arra, hogy mit tanultam a Bitcointól?

A hét filozófiai lecke után jöjjön hát a hét pénzügyi lecke. A mai ajánlat egy kis közgazdaságtan, a célállomás pedig a megbízható pénz.

Nyolcadik lecke: A pénzügyi tudatlanság

Tudatlan kislánynak fog hinni, ha rákérdezek. Nem fogom ezt tenni, talán itt találom valahol, felírva.

Számomra az volt a legmeglepőbb dolog, hogy az, ami elsőre egy tisztán technológiai jellegű dolognak tűnt, egy számítógép-hálózatnak, valójában mekkora tudást igényel a megértéshez a pénzügy, a gazdaság, és a pszichológia terén. Ha egy fantasztikus irodalmi hasonlattal akarnám jellemezni, ez az az érzés, amelyet így írtak le:

„Veszélyes dolog beszállni a Bitcoinba, Frodó. Elolvasod a white papert, és aztán ha nem figyelsz oda, hová lépsz, könnyen beszív a mélység."

Ha meg akarsz érteni egy új pénzrendszert, ahhoz ismerned kell a régit. Én nagyon hamar rájöttem, hogy az oktatási rendszerben eltöltött időm alatt kapott pénzügyi ismereteim mennyisége gyakorlatilag nulla. Elkezdtem feltenni magamnak a kérdéseket, mintha csak öt éves lennék. Hogyan működnek a bankok? Hogyan működik a tőzsde? Mi a pénz? Mi a rendes pénz? Miért van annyi adósság? Honnan jön a pénz, és ki dönti el, mennyi van belőle? Hamar pánikba estem, hogy mennyire tudatlan is vagyok, de aztán rájöttem, hogy jó társaságba keveredtem.

„Ironikus, hogy a Bitcoin miatt többet tanultam a pénzről, mint a pénzintézeteknél eltöltött hosszú évek során. Ráadásul egy bankban kezdtem a karrieremet."

aarontaycc

„Az elmúlt három hónapnyi kriptózás alatt többet tanultam a pénzről, gazdaságról, technológiáról, titkosításról, pszichológiáról, politikáról, jogról, játék-elméletről, és saját magamról, mint előtte három és fél év alatt a főiskolán."

bitcoindunny

Számtalan ilyen vallomással találkozhatunk. A Bitcoin, ahogyan az első leckében említettem, egy élő dolog. A híres közgazdász, Mises szerint maga a gazdaság szintén egy élő rendszer. Azt pedig mindannyian tudjuk, hogy az életet kifejezetten nehéz megérteni.

„A tudomány nem más, mint egy állomás a tudásért folyó végtelen versenyben. Az emberi tevékenység minden apró mozzanata hatással van rá, sokszor rossz irányba. Ez nem azt jelenti, hogy a világgazdaság ma visszafejlődik. Egyszerűen annyit jelent, hogy a gazdaság egy élő rendszer, és mint ilyen, tökéletlen, és folyton változik."

Ludwig von Mises

Mindannyian olvashattunk már a hírekben több pénzügyi, gazdasági válságról is, elcsodálkozva, hogy ezek a mentőcsomagok hogyan működnek, és hogy lehet, hogy a sok billió

dolláros veszteségekért soha senki nem felelős. Még én is csak kapkodom a fejem, de mostanra már van valami fogalmam arról, hogy mi is történik a pénzügyi világban.

Néhányan viszont olyan messzire mennek, hogy az általános tudatlanságból inkább a rendszerszintű, szándékos tagadás fázisába lépnek. A történelem, fizika, biológia, matematika, nyelvtan mind szerepel az iskolai tantervekben, a pénz és a gazdaság viszont meglepő módon rendkívül kis súllyal szerepel, ha egyáltalán bekerül valahol. Csodálkoznék rajta, ha akkor is ennyi adósságot halmoznának fel az emberek, ha az oktatásunkban szó lenne a gazdaság és a pénz működéséről is. Persze, néha azon is elgondolkodok, hogy vajon hány réteg alufólia kell egy jó kis alufóliasisakhoz. Lehet, hogy három már elég.

„Ezek a válságok, a mentőcsomagok, nem véletlen történnek így. Az sem véletlen, hogy nem tanítanak a pénzről az iskolában. Ez szándékos. Az amerikai polgárháború előtt illegális volt a rabszolgák tanítása. Nekünk most az nincs engedélyezve, hogy a pénzről tanuljunk az iskolában."

Robert Kiyosaki

Mint ahogyan Óz történetében, nekünk is azt mondják, ne foglalkozzunk azzal a fickóval a függöny mögött. Ózzal ellentétben nekünk viszont most elérhető a valódi varázslat: egy cenzúra-ellenálló, nyílt, határokon átívelő pénzrendszer. Nincs függöny, és a varázslatot bárki megnézheti közelebbről.

A Bitcoin rávett, hogy lessek be a függöny mögé, és szembesüljek a saját pénzügyi tudatlanságommal.

Kilencedik lecke: Infláció

Kedvesem, itt nekünk olyan gyorsan kell futnunk, ahogyan csak bírunk, így tudunk egy helyben maradni. Ha pedig előrébb szeretnél jutni, akkor kétszer olyan gyorsan kell futnod.

Mikor elkezdtem a közgazdasággal foglalkozni, az első, amit tanulmányozni kezdtem, a monetáris infláció, és az azzal ellenétesen működő Bitcoin hatása volt a cselekedeinkre. Annyit tudtam, hogy az infláció nem más, mint az új pénzkészlet létrehozásának az aránya, semmi többet.

Néhány közgazdász úgy véli, az infláció jó dolog. Mások viszont azt a nézetet vallják, hogy az egészséges gazdasághoz létfontosságú egy stabil pénz, amelyet nem lehet könnyen elinflálni. Az aranystandard idején ez utóbbi működött is. A bitcoin teljes készlete 21 millióban van maximalizálva, a stabil pénz táborát erősítve.

Az infláció hatásai a legtöbbször nem azonnaliak. Az inflációs rátától függően, meg persze még egy sor egyéb faktort figyelembe véve a hatás és a következmény között akár több év is eltelhet. Ráadásul az infláció bizonyos társadalmi csoportokat jobban érint, mint másokat. Henry Hazlit közgazdász rávilágított, „a közgazdaságtan nem a rövid távú következmények figyeléséről szól, hanem a hosszú távú hatások feltérképezéséről bármilyen beavatkozás esetén, ehhez pedig nem csak az egy-egy csoportra gyakorolt hatást, hanem a teljes társadalomban, minden csoportban fellépő következményeket kell vizsgálnunk”.

Az én személyes megvilágosodásom az volt, mikor rájöttem, az új pénz kibocsátása, a jegybanki pénznyomtatás olyan gazdasági tevékenység, amely nagyban eltér az összes többitől. Az áruk és a szolgáltatások termelése, áruba bocsátása valódi értéket teremt a valódi emberek számára, a pénznyomtatás gyakorlatilag ennek az ellenkezőjét éri el. Mindenki, aki az adott fajta pénzzel rendelkezik, veszít a vagyonából.

„A puszta infláció, az új pénz kinyomtatása nagyobb bérekhez, és drágább árukhoz vezet. Ez úgy tűnhet, hogy az igények növekedése miatt történik. A termelés és az árucsere szempontjából viszont ez egyáltalán nem így van.”

Henry Hazlitt

Az infláció valódi pusztító ereje akkor válik nyilvánvalóvá, mikor a kis infláció nagy inflációba csap át. Mikor a hiperinfláció színre lép, a dolgok hamar eldurvulhatnak. A pénz ekkor értékét veszti, és már nem is tud értéktárolóként működni, az emberek pedig igyekeznek átváltani bármire, amihez hozzájutnak.

A másik következménye a hiperinflációnak az, hogy az emberek megtakarításai, amelyeket esetleg egy életen át gyűjtöttek, semmivé válnak. A papírpénz természetesen még mindig ott lesz a pénztárcákban, de már tényleg csak annyi lesz. Egy darab értéktelen papír.

Hiperinfláció a Weimar Köztársaságban, 1921-23

A pénz az úgynevezett enyhe inflációval is veszthet az értékéből, lassan. Ilyenkor annyira lassú a változás, hogy az emberek többségének fel sem tűnik a vásárlóerő csökkenése. Viszont ha a pénznyomtató beindul, a valuta könnyen inflálódhat, és a lassú értékcsökkenés gombnyomásra átcsaphat nagyon durva értékcsökkenésbe. Friedrich Hayek, ismert közgazdász is erre jutott az esszéjében, hogy az infláció általában mindig felerősödik.

„Az sem segít semmin, ha enyhe az infláció. Onnan csak nőni tud."

Friedrich Hayek

Az infláció különösen káros hatású is lehet, hiszen azoknak kedvez, akik közelebb vannak a pénznyomtatóhoz, a közmondásos húsosfazékhoz. Időbe telik, míg a frissen nyomtatott pénz bekerül a gazdaság körforgásába, és az árak hozzáigazodnak a megnövekedett készlethez. Szóval, ha meg tudod oldani, hogy még azelőtt rátedd a kezed a pénzre, hogy elkezdődne az értéktelenedés, az inflációs görbe előtt maradhatsz. Ezért is nevezik az inflációt rejtett adónak, hiszen a kormányzat jól jár vele, mindenki más viszont pénzt veszít.

„Nem érzem túlzásnak azt mondani, hogy a világtörténelem valójában az infláció történelme. Az inflációt pedig a kormányok idézik elő, a saját vagyonuk növelésére."

Friedrich Hayek

A történelem során eddig kivétel nélkül az összes, kormányok által kibocsátott pénz lecserélődött, vagy teljesen összeomlott. Nem számít, mennyire kicsi az infláció, az sem számít, ha egyenletes növekedésnek nevezzük, valójában azt jelenti, hogy exponenciálisan növekszik. A természetben és a gazdaságban pedig, ha valami exponenciálisan növekszik, akkor vagy megáll a növekedése egy ponton, vagy katasztrofális összeomlás következik be.

Persze, gondolhatod azt, hogy a te országodban ez nem fog megtörténni. De nem gondolod ezt, ha egy venezuelai lakos vagy, mert abban az országban éppen hiperinfláció van. Az infláció egymillió százalék fölötti, a pénzük gyakorlatilag értéktelen papírfecnivé vált.

Lehet, hogy nem fog ugyanezt történni a következő pár évben, vagy nem fog megtörténni azzal a valutával, amely a te országodban van használatban. De a történelemből tudjuk, hogy elég hosszú időtávon nézve elkerülhetetlenül bekövetkezik. Gyerekkorunkból még akár emlékezhetünk is ilyen pénzekre, az osztrák schilling, az olasz líra, a horvát dínár, mind értéktelen. Az én nagyszüleim még használták az Osztrák-Magyar Monarchia pénzét, a koronát is. Ahogy telik az idő, minden egyes valuta elértéktelenedik. Vagy lecserélik, vagy összeomlik a hiperinfláció miatt. Történelmi, antik pénzzé válik, és mi tesszük ezzé.

„A történelemből láthatjuk, hogy a kormányok végül mind engednek az infláció csábításának."

Saifedean Ammous

Miért más a bitcoin? Az államok által kibocsátott, állami rendeletekkel, törvényekkel szabályozott pénzekkel ellentétben azok a pénzek, amelyek a fizika törvényein alapulnak, túlélő típusok, és az értéküket is tartják. Messze a legjobb példa erre az arany, amelyről tudjuk, hogy nem évszázadokon, de évezredeken keresztül tartja az értékét. Természetesen nem tökéletesen stabil – és amúgy is, mi alapján döntjük el, hogy stabil-e valami –, de a kilengései meghatározott tartományban maradnak. Ha egy pénz hosszú időn keresztül tartani tudja az értékét, akkor stabil, megbízható pénznek, úgymond kemény valutának nevezzük. Ha pedig könnyű elinflálni, és így nem tartja az értékét, akkor bizony nem stabil, és nem is megbízható. A megbízhatóság létfontosságú eleme a bitcoinnak, és ezért ennek majd egy önálló leckét is szentelek a későbbiekben.

Egyre több és több országban üti fel a fejét a hiperinfláció, ezért pedig egyre több ember szembesül a pénz megbízhatatlanságával. Ha szerencsénk van, talán néhány központi bank észhez tér, és újragondolják a pénzpolitikájukat. Bármi történjék is, a bitcoinnak köszönhetően már annyit tanultam a pénzről, hogy megérte foglalkozni vele, mindentől függetlenül.

A bitcoinnak köszönhetően az inflációnak nevezett rejtett adóról, és a hiperinfláció katasztrófájáról is tanultam.

***

A tükörben:

Bitcoin Boots ont he Ground – Venezuela

Tizedik lecke: Érték

A fehér nyúl volt az, lassan jött visszafelé, és közben aggódva nézelődött, mint aki elvesztett valamit…

Az érték fogalma mindig is paradoxonnak tűnt, és számos elmélet létezik, amely azt próbálja megmagyarázni, miért értékelünk bizonyos dolgokat többre, mint valami mást. Az emberiség valójában évezredek óta elmélkedik ezen. Ahogy Platón is írta a dialógusaiban, sokszor azért értékelünk valamint, mert ritka, nem pedig azért, mert szükséges a túlélésünkhöz.

„Ha körültekintő vagy, ugyanezt tanácsolod a tanítványaidnak is – ne beszéljenek senkivel, csak veled, és egymással. Ha valami ritka, Euthydemus, akkor értékes is. A víz bőséges, ezért olcsó, pedig létszükségletünk, ahogyan Pindar is mondta."

Platón

Az érték paradoxona valami érdekesre világít rá velünk, emberekkel kapcsolatban. Úgy tűnik, szubjektíven is értéket tulajdoníthatunk dolgoknak, de nem önkényesen választott kritériumok alapján. Egy bizonyos dolog sok különböző okból számíthat értékesnek, de minden, amit értékesnek tekintünk, meghatározott tulajdonságokkal bír. Ha valamit könnyen sokszorosíthatunk, vagy természeténél fogva bőségesen rendelkezhetünk vele, akkor nem tekintjük értékesnek. A jelek szerint viszont értékesnek gondolunk olyasmit, ami ritka (például a nemesfémek, drágakövek, vagy éppen az idő), amit nehéz, bonyolult előállítani, vagy amit nem lehet pótolni (például egy régi fényképet valamely szerettünkről), vagy éppen azért, mert lehetővé tesz számunkra valamilyen fontos dolgot. De akár ezek kombinációja is lehetséges, ahogyan a műalkotások esetében tapasztalhatjuk.

A bitcoin mindezt biztosítja. Elképesztően ritka, csak 21 millió fog létezni belőle. Egyre nehezebb előállítani a blokkjutalom-felezések miatt. Nem lehet lecserélni, ha egy privát kulcs elveszett, a rajta lévő bitcoin örökre elérhetetlen. Lehetővé tesz számunkra néhány nagyon fontos dolgot. Vitathatatlanul a legjobb értéktovábbító a határokon átnyúló pénzküldéshez. Nem lehet cenzúrázni, sem pedig lefoglalni, ráadásul lehetővé teszi az emberek számára, hogy bankok, kormányok nélkül, önállóan tudják tárolni, biztonságban tartani a vagyonukat.

A bitcoin megtanította, hogy az érték lehet szubjektív, de nem önkényes döntéseken alapul.

Tizenegyedik lecke: Pénz

Fiatal koromban – mondta a bölcs*, – nagyon odafigyeltem rá, hogy az izületeim rugalmasak maradjanak. Ez a kenőcs segített, öt schilling egy doboz. Engedd meg, hogy eladjak neked párat!*

Mi a pénz? Minden nap használjuk, erre a kérdésre mégis meglepően nehéz válaszolni. Minden téren függünk a pénztől, és ha kevéssel rendelkezünk, az életünk hamar bonyolulttá válhat. Mégis alig gondolkodunk el ezen, pedig állítólag e körül forog a világ. A Bitcoin hamar rákényszerített, hogy újra meg újra feltegyem magamnak a kérdést, mi is valójában a pénz?

A mai modern világban a legtöbb embernek a tárcájában lévő bankjegyek jutnak az eszébe, ha szóba kerül a pénz, még akkor is, ha valójában a legtöbbünk pénze inkább csak néhány szám, egy bankszámlán. Már most egyeseket és nullákat használunk a pénzünkhöz, miért más mégis a bitcoin? A bitcoin azért más, mert működését tekintve nagyon is különbözik a jelenleg használt pénzeinktől. Ezt úgy tudjuk könnyen megérteni, ha megnézzük, mi is a pénz, hogyan jön létre, és miért az arany és az ezüst volt a történelem során a kereskedelemhez használva.

„Ha úgy vesszük, a bitcoin inkább a nemesfémekre hasonlít. Nem változik a készlete csak azért, hogy tartani tudja az értékét. A készlete előre meg van határozva, ezért az értékének kell változnia."

Satoshi Nakamoto

Kagylók, ezüst, arany, papír, bitcoin, igazából mindegy. Az számít pénznek, függetlenül az alakjától és a megjelenésétől, amelyről az emberek úgy döntenek, hogy pénzként használják.

A pénz, mint találmány, zseniális dolog. Egy pénz nélküli világ őrülten bonyolult lenne. Vajon hány halat kell adnom egy új pár cipőért? Hány tehénnel tudok venni egy házat? Mi van, ha éppen nincs szükségem semmire, de meg kellene szabadulnom a romlandó almáimtól? Nem kell nagy képzelőerő ahhoz, hogy rájöjjünk, a barteren, cserekereskedelmen alapuló gazdaság nem a leghatékonyabb megoldás.

A pénzben az a legjobb, hogy bármire elcserélhető, emiatt ekkora jelentőségű találmány. Ahogyan Nick Szabo a Shelling Out című esszéjében kifejtette, az emberiség már rengeget dolgot használt pénzként. Gyöngyöket, kagylókat, faragott csontot, ékszereket, és olyan ritka fémeket, mint az ezüst és az arany.

Az emberek lusták, és nem nagyon gondolkodunk el azon, hogy az általunk használt dolgok hogyan működnek. A pénz működik, tudjuk használni. Ahogyan az autók vagy a számítógépek esetén is, a legtöbben csak akkor gondolkodnak el valaminek a működésén, ha az a valami éppen tönkremegy. Azok az emberek, akiknek az összes megtakarítása semmivé vált a hiperinfláció miatt, pontosan ismerik a megbízható, stabil pénz értékét. Azok az emberek, akiknek a rokonai, barátai tűntek el a náci Németország, vagy a kommunista Szovjetunió atrocitásaiban, pontosan ismerik a magánszféra értékét.

A pénzzel az a helyzet, hogy mindennel kapcsolatban áll. Minden tranzakció felét a pénz adja, hiszen pénzért cserébe veszünk vagy adunk valamit, így aki a pénzt kontrollálja, hatalmas befolyásra tehet szert.

„A kereskedelmi tranzakciók egyik fele a pénz mozgása, és teljes civilizációk emelkednek fel, vagy buknak el a pénzük minőségétől függően. Egy rendkívüli erőről beszélünk, amely gyakorlatilag az éj leple alatt működik. Egy olyan erőről, amely valóságnak tűnő illúziókat képes teremteni, és fenntartani. Ez a Szövetségi Tartalékbank, a FED valódi hatalma."

Ron Paul

A Bitcoin véget vet ennek, hiszen megszünteti a pénznyomtatást, mégpedig békésen, erőszak nélkül.

A pénz rengeteg megjelenési formát öltött már. Néhány ezek közül jó volt. Így vagy úgy, de javítottak a pénzünk minőségén. Nemrégiben azonban a pénzünk működési szabályait korrumpálták. Manapság szinte minden pénz parancsszóra jön létre, fedezetlenül. Hogy ezt megértsem, tanulmányoznom kellett a történelmet, és a pénzek bukását.

Hogy ezt mások is megérthessék, vagy hatalmas erőfeszítések kellenek az oktatásban, vagy sorozatos pénzügyi katasztrófák. Reménykedjünk, hogy az első változat fog bekövetkezni.

Nekem mindenesetre megtanította a Bitcoin, hogy mi a pénz.

Tizenkettedik lecke: A történelem, és a pénz bukása

Még arra a pár szabályra sem fognak emlékezni, amelyeket a barátaik mondtak nekik. Például, hogy ha belenyúlsz a tűzbe, megégeted magad, vagy, ha megvágod az ujjad késsel, vérezni fog. Ha pedig meg akarsz inni valamit, amire az van írva, hogy méreg, emlékezz erre, biztos, hogy nem fognak egyetérteni veled.

A legtöbben úgy hiszik, a pénznek aranyfedezete van, ezt az aranyat pedig hatalmas széfekben őrzik, vastag falak mögött. Ez már évtizedek óta nem így van. Arra nem emlékszem, hogy én mit gondoltam erről, mert nekem elsőre az is nehéz volt, hogy megértsem az összefüggést az arany és a papírpénz között, vagy azt, hogy egyáltalán miért kellene fedezet a pénz mögé?

Ha tanulni akarsz a bitcoinról, tanulnod kell a fiat pénzekről is. Mit jelent ez a kifejezés? Hogyan jött létre, és miért nem a legjobb ötlet így működtetni a pénzünket? Szóval mi a fiat pénz? És miért használjuk mégis azt?

Ha valamit úgy jellemzünk, hogy fiat, az annyit jelent, hogy egy hatóság vagy más szervezet rendelete alapján számít valaminek. Tehát a fiat pénz azért pénz, mert valaki törvényt hozott róla, hogy pénznek számít. Ez a valaki pedig az országod kormányzata, hiszen ma a világ összes országa fiat pénzt használ. Sajnos nem tekinthetsz el ettől a törvénytől, és ha úgy érzed, ez kényszerítésnek hangzik, akkor jól érzed. Ha megtagadod, hogy ezt a pénzt használd a vállalkozásodban, vagy az adófizetéshez, hamarosan már csak a cellatársaiddal beszélgethetsz a pénz működéséről.

A fiat valuták értéke nem a belső tulajdonságaikból fakad. Hogy egy fiat pénz mennyit ér, azt az dönti el, hogy a kibocsátója, az adott ország pénzügyileg mennyire stabil, mennyit ér. Ezt az értéket tulajdonképpen önkényesen határozzák meg.

A latin „fieri”, azaz „legyen így” kifejezésből származik az angol fiat szó.

Egészen a közelmúltig, az emberiség két típusú pénzt használt. Az egyik az árucikk-pénz, amely valamilyen értékes dologból, például aranyból készül. A másik az úgynevezett képviseleti pénz, amely tulajdonképpen egyfaja igazolás, a mögöttes fedezetről, legtöbbször szintén valami értékes dologról.

Az árupénzekről már beszéltünk, a faragott csontok, gyöngyök, aranyérmék kapcsán. A nemesfémekből régóta vernek pénzérméket, és ezek a mai napig értékesek. A legrégebbi

arany és ezüstötvözetből készült érme nagyjából 2700 éves. A bitcoin esetén nem maga a coin, az érme fogalma az újdonság.

Perzsa érme elektrumból (80-90% arany, 10-20% ezüst), Classical Numismatic Group Inc.

Az érmék felhalmozása, gyűjtése, vagy talán ismerősebb szóhasználattal mondva, a „hodl" pedig egyidős az érmékkel. A legkorábbi gyűjtögető majdnem száz érmét tett egy edénybe, amelyet aztán egy templom alapzatához ásott el. 2500 évvel később találták meg, ez elég jó hidegtárcának számít, ha engem kérdezel.

A fém érmék egyik legnagyobb hátránya viszont az, hogy le lehet vágni belőlük kisebb darabokat, így csökkentve az érme értékét. A levágott darabokból aztán új érméket lehet létrehozni, tulajdonképpen inflációt előidézve.

Az emberek szó szerint annyit csiszoltak le az ezüstdollárok pereméből, amennyit csak lehetett, mintha valamiféle Dollárvágó Klub működött volna annak idején. A kormányzatok viszont csak akkor kedvelik az inflációt, ha ők csinálják, így természetesen megpróbálták megakadályozni az efféle magán-leértékelést. Ez a klasszikus macska-egér harchoz vezetett, az érmevágók egyre kifinomultabbak és kreatívabbak lettek, rákényszerítve az államok pénzverdéit, hogy ők is még nagyobb erőfeszítéseket tegyenek ennek a megakadályozására.

Isaac Newton, a modern fizikai atyjának arcképe is felkerült az ilyen érmékre, egy rövid idézettel, amely körbefutott az érme szélén. Ez a módszer a mai napig használatban van, alaposan megnehezítve az érmevágók dolgát.

Az ilyen leértékelési problémák mellett az érmékkel kapcsolatban más nehézségekkel is számolni kellett. Nehezek, és nem szállíthatók könnyen, főleg nagy mennyiségben, ha nagy értékű tranzakciót hajtanánk végre. Egy nagy zsák ezüstpénzt vinni a kereskedésbe, ha venni akarunk egy új Mercedest, nem hangzik túl praktikus dolognak.

Ha már szóba kerültek a német dolgok, egy kis érdekesség a dollárról. Az USA pénze a német Thaler szóról kapta a nevét. A Thaler pedig a Joachhimsthaler rövidítése. Ezt a pénzt Sankt Joachimsthal városában verték, ezüstből. A Thaler szót pedig arra a személyre vagy dologra használták, amely abból a völgyből jött, amelyben a város feküdt, és ahol az ezüstérméket készítették. Az emberek ezután egyszerűen Thalerként kezdtek hivatkozni az ezüstpénzekre. A szó átkerült a holland nyelvbe, „daalders” formában, majd ebből lett az angol dollár szó.

Az „ős-dollár”, rajta a szent képe, a pálcájával és a varázslókalappal; Berlin-George

A képviseleti pénzek megjelenésével elkezdődött a megbízható, stabil, kemény valuták fokozatos eltűnése. Az arany-certifikátok 1863-ban jelentek meg, és tizenöt évvel később megkezdődött az ezüstpénzek lecserélése is papír-igazolásokra. Az első ezüst-certifikát megjelenése után 50 évvel az a bizonyos darab papír már majdnem úgy nézett ki, mint egy mai egydolláros bankjegy.

1928-as ezüstdollár, „A névértékre beváltható”; National Numismatic Collection, Smithsonian Institution

Érdemes megfigyelni, hogy ez a papír még mindig „ezüst-certifikát” a felirat alapján, tehát egyértelműen nem más, mint egy igazolás arról, hogy a tulajdonosa adott mennyiségű ezüstre jogosult. Az idők során ez a felirat természetesen eltűnt a bankjegyekről, és csak annyi állt már ott, hogy a Federal Reserve bankjegye.

Ugyanez történt az arannyal is. A világ nagy részén az aranyat és az ezüstöt használták a pénzveréshez. Az arany-certifikátok megjelenése, amelyeket fizikai aranyra lehetett beváltani, technológiai szempontból fejlődésnek számított. A papír használata sokkal kényelmesebb, kisebb a súlya, és sokkal jobban felosztható, hiszen könnyen tudunk kisebb címletet nyomtatni belőle. Hogy az embereket, a felhasználókat emlékeztessék a mögöttes fedezetre, a megfelelő színeket használták a nyomtatáshoz, és egyértelműen feliratozták ezeket a certifikátokat:

„Ez az igazolás bizonyítja, hogy az Amerikai Egyesült Államok kincstárában letétbe lett helyezve 100 dollár értékű aranyérme, amely az igazolás birtokosának a részére igény szerint kifizethető.”

Arany-certifikát; National Numismatic Collection, National Museum of American History

1963-ban lekerült az újonnan nyomtatott bankjegyekről a felirat, amely szerint a fedezetül szolgáló arany az igazolás birtokosának részére kifizethető. Öt évvel később pedig teljesen megszüntették a beváltási lehetőséget. A szavak, amelyek a papírpénzek eredetét, az egész ötletet jelképezték, végleg eltűntek. Az arany színt nem használták már. Nem maradt más, csak egy darab papír, amelyből a kormány annyit nyomtatott, amennyit csak akart.

Az aranystandard 1971-es megszüntetésével véget ért az évszázados bűvészmutatvány. A pénz azzá az illúzióvá vált, amelyet ma ismerünk, fiat pénzzé. Azért ér valamit, mert egy hadsereggel és börtönőrökkel rendelkező hatalom azt mondja, hogy márpedig ér valamit. Ma minden egyes dolláron az olvasható, hogy „Ez a hivatalos pénznem”. Más szóval megfogalmazva, azért ér valamit, mert rá van írva.

Egy ma is használatban lévő, 2004-es kiadású húszdolláros, a „hivatalos pénznem”.

Van egy másik érdekes dolog is, amely szintén a bankjegyekre van nyomtatva, ugyanis azt olvashatjuk rajta, hogy „For all debt, public and private”, azaz minden adósságot szimbolizálhat. Ez lehet, hogy nem újdonság a közgazdászoknak, engem viszont meglepett. A pénz tehát adósság. Nekem még mindig zúg a fejem az egésztől, de arra bátorítalak, hogy nézz utána a kapcsolatnak a pénz és az adósság között.

Ahogy láthatjuk, az arany és az ezüst évezredeken keresztül működött pénzként. Idővel aztán papírra cserélték ezeket, végül ezek a papírok szolgáltak fizetőeszközként. Ez hozta létre azt az illúziót, hogy magának a papírnak van bármiféle értéke.

A Bitcoin megtanított a pénz történetére, és megmutatta, leleplezte a gazdaság legnagyobb bűvészmutatványát, a fiat pénzeket.

Tizenharmadik lecke: A frakcionált banki tartalék őrültsége

Aztán egyszer csak már késő lett. Egyre nagyobbra és nagyobbra nőtt, és hamarosan le kellett térdelnie. Egy perc múlva viszont már nem volt elég helye így sem, és megpróbált lefeküdni, az egyik karját az ajtó felé, a másikat a feje alá téve. De még tovább nőtt, így utolsó erejével kidugta a kezét az ablakon, az egyik lábát pedig a kéményen, és így szólt, *„nem tudok már mit tenni, mi lesz így velem?”*

A pénz kérdése nem számít túl egyértelmű témának, főleg manapság nem. Már a pénz létrehozásának a banki folyamata sem egyértelmű, és nem tudok szabadulni az érzéstől, hogy ez szándékosan van így. Az, amit előzőleg csak az oktatásban, vagy a jog nyelvezetében tapasztaltam, úgy tűnik, a pénz világában is ugyanúgy érvényes. Semmit sem magyaráznak el világos, érthető módon, és nem azért, mert a téma bonyolult. Minden dolog a szakzsargon újabb és újabb rétegei alatt bújik meg, és nagyon bonyolultnak látszik. Kiterjesztett monetáris politika, mennyiségi lazítás, fiskális stimulus, és hasonló kifejezések vannak mindenfelé. A hallgatóság pedig mintegy hipnotizálva van a komoly szakszavak által.

A frakcionalizált banki tartalék és a mennyiségi lazítás is ilyen kifejezés, és valójában arra szolgálnak, hogy elfedjék a lényeget, bonyolultnak, és nehezen érthetőnek beállítva. Viszont ha el akarod magyarázni ezeket egy öt éves gyereknek, hamar kiderül, hogy miről is van szó. Az Európai Parlament egyik vitáján Godfrey Bloom nagyon is egyértelműen kimondta ezt, jobban, mint ahogyan én tudnám megfogalmazni.

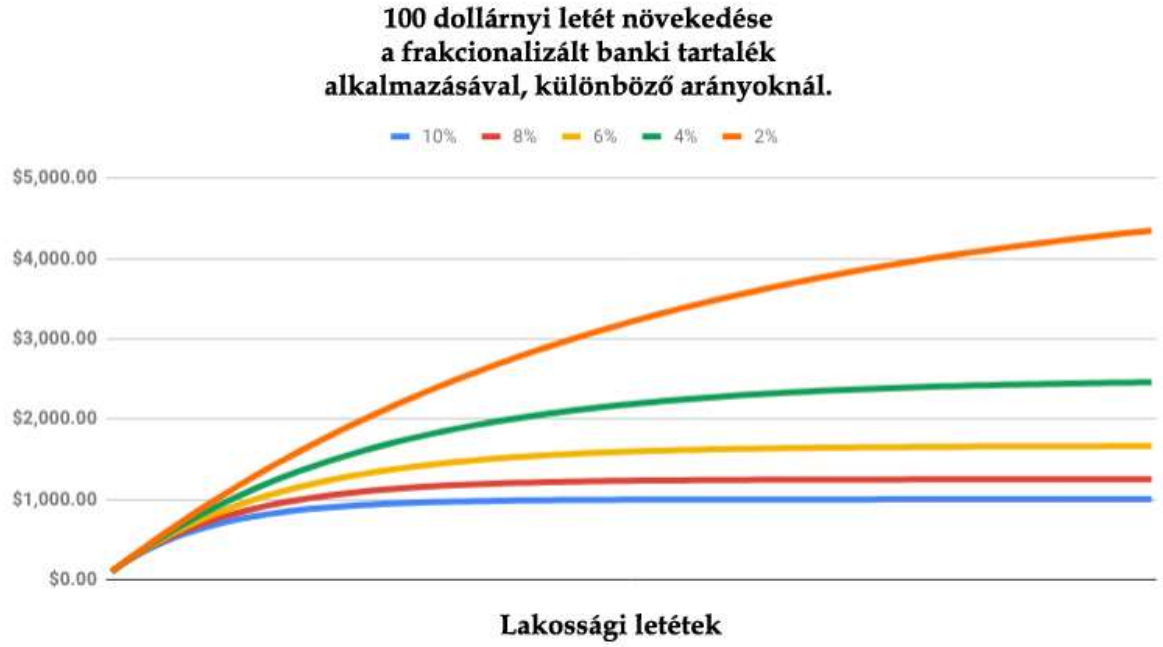
„Úgy látom, nem igazán értitek a bankrendszer működését. Minden bank rosszul működik. A Santander, a Deutsche Bank, a Skót Királyi Bank, az összes hibás! Hogy miért? Nem Isten keze van a dologban. És nem is valami szőkőár tarolta le a rendszert. Azért működnek hibásan, mert az úgynevezett frakcionalizált banki tartalékok módszerét használják. Ez azt jelenti, hogy olyan pénzt is kihelyeznek hitelbe, amellyel nem is rendelkeznek! Ez bűncselekmény, és már túl régóta folyik! Ez pénzhamisítás, bár néha mennyiségi lazításnak nevezik, de valójában pénzhamisítás. Ha egy átlagember ezt teszi, nagyon hosszú időre börtönbe kerül. Amíg nem kezdjük el a bankárokat is börtönbe küldeni – igen, ide értem a politikusokat és a központi bankok vezetőit is –, addig ez az őrültség tovább folytatódik!

Godfrey Bloom

Ismételjük meg a legfontosabb részt: a bankok olyan pénzt is kihelyeznek hitelként, amellyel nem is rendelkeznek. Vegyük sorra egy példán, hogy hogyan is működik ez a gyakorlatban! Számoljunk 10%-kal, mert ez kerek szám, és egyszerűbb követni a gondolatmenetet.

Szóval beteszel a bankba 100 dollárt, mert nem akarod a matracod alatt tartani. A banknak viszont csak a 10%-át kell letétben tartania ennek, tehát 10 dollárt. A 100 dollár 10%-a az 10 dollár. Mit csinálnak a többi pénzzel, mi lesz a maradék 90 dollároddal? Azt csinálják, amit a bankok szoktak, kölcsönadják másnak. Ez viszont megsokszorozza a körforgásban lévő pénz mennyiségét. Befizettél 100 dollárt, ebből a számládon 100 dollár látszik (még ha nincs itt ott a bankban, csak a 10%-a), és hitelként kihelyeztek 90 dollárt. A gazdaságban tehát 100 dollár

helyett már 190 dollár van. Az újonnan „létrejött” 90 dollárból ismét csak 10%-ot kell letétben tartani, a többit ki lehet helyezni hitelként, így már 271 dollár van a körforgásban. A következő körben ez már 343,9 dollár. A pénzkészlet minden lépéssel növekszik, mivel a bankok szó szerint nem létező pénzt adnak ki hitelként, és ezután létezőként tartják nyilván. Bonyolult abrakadabra nélkül is 1000 dollárt tudnak varázsolni a bankok, alig 100 dollárból. Könnyű tízszeres nyereség, és csak néhány hitelezési kör kell hozzá.



Félre ne érts, szerintem semmi gond nincs a hitelezéssel. Semmi gond nincs a kamatokkal. Semmi gond nincs a hagyományos kereskedelmi bankokkal, amelyek tárolják a pénzedet, egy olyan helyen, amely biztonságosabb, mint a párnaciha.

A központi bankok viszont már másik állatfaj. Ezek a pénzügyi szabályozás anomáliái, félig magáncégek, félig közintézmények, és egy olyan dologgal játszadoznak, amely a világon mindenki számára létfontosságú. Mindezt kizárólag a rövid távú haszonra koncentrálva, és a jelek szerint teljesen felelősségmentesen, ellenőrizetlenül.

A bitcoin is inflációs, ez viszont ideiglenes. A szigorúan meghatározott maximális készlet mindössze 21 millió, és mire a rendszer ezt eléri, az infláció végleg eltűnik. Mostanra két különálló pénzrendszerünk lett. Az egyik inflációs, ahol a pénzkészletet bármikor önkényesen megváltoztathatják. A másik pedig a Bitcoin világa, ahol a készlet véges, és bárki számára ellenőrizhető. Az egyiket ránkkényszerítik, a másikhoz viszont bárki önként csatlakozhat, ha úgy kívánja. Nincs korlát, amely előttünk állhatna, senkinek sem kell engedélyt kérnie senkitől. Kizárólag az önkéntességen alapul. Ez a Bitcoin szépsége.

Azt is mondhatjuk, hogy a közgazdászok keynesi és osztrák iskolát követő táborai között a vita immár nem csak akadémiai szinten folyik. Satoshi a pénzrendszerek szteroidozott változatát hozta létre, amely biztosítja számunkra a valaha létezett legmegbízhatóbb, legstabilabb pénzt. Ilyen vagy olyan módon, de egyre több ember fog rájönni a központi bankok által használt frakcionalizált tartalékrendszer visszásságaira. Ha ugyanarra a következtetésre jutnak, mint a

bitcoinerek, vagy az osztrák iskolát követő közgazdászok, vélhetően becsatlakoznak a bitcoin-használók gyorsan növekvő csoportjába. Senki sem tudja megállítani őket, ha ezt szeretnék tenni.

A Bitcoin megtanította, hogy a frakcionalizált banki tartalék nem más, mint színtiszta őrültség.

Tizennegyedik lecke: A stabil pénz

Az első dolog, amit tenni fogok, – gondolta Alice, miközben a fák között bandukolt, – *hogy visszanyerem a megfelelő méretem, a második dolog pedig az, hogy megtalálom a kaput ahhoz a csodás kerthez. Így lesz a legjobb.*

Az egyik legfontosabb lecke, amelyet a Bitcoin megtanított nekem, az az, hogy hosszú távon a stabil pénz sokkal jobb, mint a manipulálható pénz. A stabil pénzek, vagy ahogyan a köznyelv sokszor hivatkozik ezekre, a kemény valuták, olyan pénznemek, amelyek világszerte elismertek, és jó értéktárolónak számítanak.

A bitcoin fiatal és volatilis. A kritikusai szerint nem jó értéktároló. A volatilitás emlegetése viszont eltereli a figyelmet a lényegről. A volatilitás eleve várható volt. A piacnak időre van szüksége, hogy kitalálja, mennyit ér ez a viszonylag új pénzeszköz. Viccesen még azt is szokták mondani, hogy a volatilitás csak egyfajta mérési hiba, hiszen nem kell dollárban számolnunk, mert 1 bitcoin mindig is 1 bitcoint fog érni.

„A lefixált készlet, vagy a csak és kizárólag előre meghatározott, objektív és kikalkulálható mértékben módosítható készlet, mindenképpen szükséges ahhoz, hogy a pénz érdemben pénzként tudjon működni.”

Fr. Bernard; W. Dempsey; S. J.

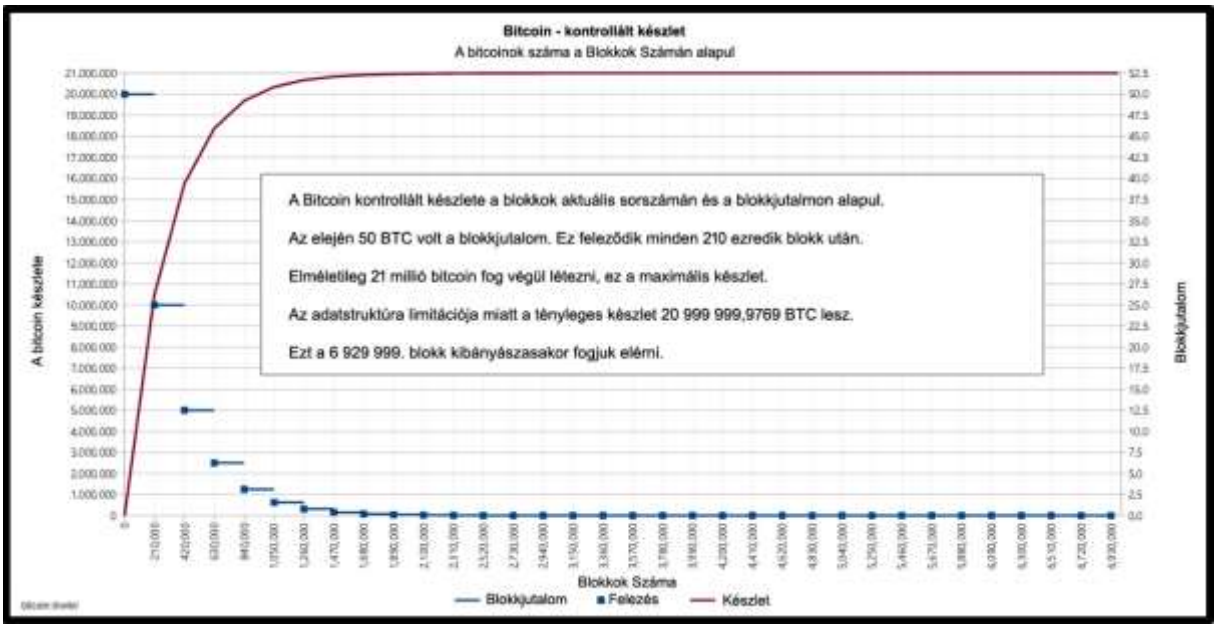
Ha átfutjuk az egykor létező, de mára már elbukott pénzek listáját, azonnal láthatjuk, hogy amelyet korlátlanul lehetett nyomtatni, azzal pontosan ezt is tették. Az emberiség történelme során nem volt kormányzat, amely ellen tudott volna állni ennek a kísértésnek.

A Bitcoin viszont megálljt parancsol ennek a kísértésnek, mégpedig zseniális módon. Satoshi pontosan tisztában volt az emberek kapzsi és esendő természetével, ezért olyasmit választott, amely megbízhatóbb az embereknél. A matematikát.

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

A bitcoin készletének a képlete

Ez a csinos képlet pontosan leírja az új bitcoinok kibocsátásának a képletét, a Bitcoin kódjában viszont sehol sem szerepel. A kódban az algoritmus által meghatározott kibocsátási ütem van rögzítve, amely ráadásul négy évente megfelezi a blokkokért járó jutalmat. Ez a képlet tulajdonképpen az egyszerűsített formula. Hogy egészen pontosan mi történik, az egy grafikonon látható a legjobban, amely megmutatja nekünk a nagyjából 10 percenként létrejövő új blokkokért járó jutalom alakulását.



Készlet és blokkjutalom; jelenleg, 2021 őszén már elkerültük a 700 ezredik blokkot

Az ilyen képletek, matematikai funkciók, és exponenciális formulák általában nem túl magától értetődőek a többség számára. Hogy egy adott pénz mennyire stabil, mennyire kemény, könnyebben megérthető egy másik nézőpontból. Ha tudjuk, hogy valamiből mennyi áll rendelkezésre, és ebből a valamiből milyen könnyen lehet még többet létrehozni, azonnal meg tudjuk határozni az értékét. Ez ugyanúgy igaz Picasso festményeire, Elvis gitárjára, a Stradivari-hegedűkre, ahogyan igaz a fiat pénzekre, az aranyra, és a bitcoinra is.

A fiat pénzek stabilitása attól függ, ki a főnök a pénznyomtató mellett. Néhány kormányzat jobban szereti a nyomtatást, mások viszont kevésbé, így a pénzek egymáshoz viszonyított értéke is eltér, az egyik megbízhatatlan pénz, a másikra viszont úgy tekinthetnek, hogy kemény valuta.

A fiat pénzek előtt a keménységet az határozta meg, hogy a pénzként használt dolog milyen tulajdonságokkal rendelkezett. A bolygón található arany készletét a fizika törvényei határozzák meg. Az arany, mint kémiai elem, ritka, mert a kialakulását előidéző szupernovák vagy neutroncsillag-összeomlások is ritkák. Az arany „kibocsátása” is lassú, hiszen a bányászat rendkívül energiaigényes folyamat. Az arany egy nehézfém, mélyen eltemetve a föld felszíne alatt. Mikor megszűnt az aranystandard, egy új kor vette kezdetét. Az új pénz létrehozásához már nem kellett semmi, csak egy kis tinta. A modern kor bankszámláin néhány plusz nulla hozzáadása egy egyenleghez pedig még ennél is egyszerűbb, hiszen pár kattintással megoldható a bank számítógépein.

„Fontos aspektusa ennek az új valóságnak, hogy az olyan intézmények, mint a Fed, nem tudnak csődbe menni. Bármennyi pénzre is lenne szükségük, egyszerűen kinyomtatják maguknak, nulla költséggel.”

Jörg Guido Hülsmann

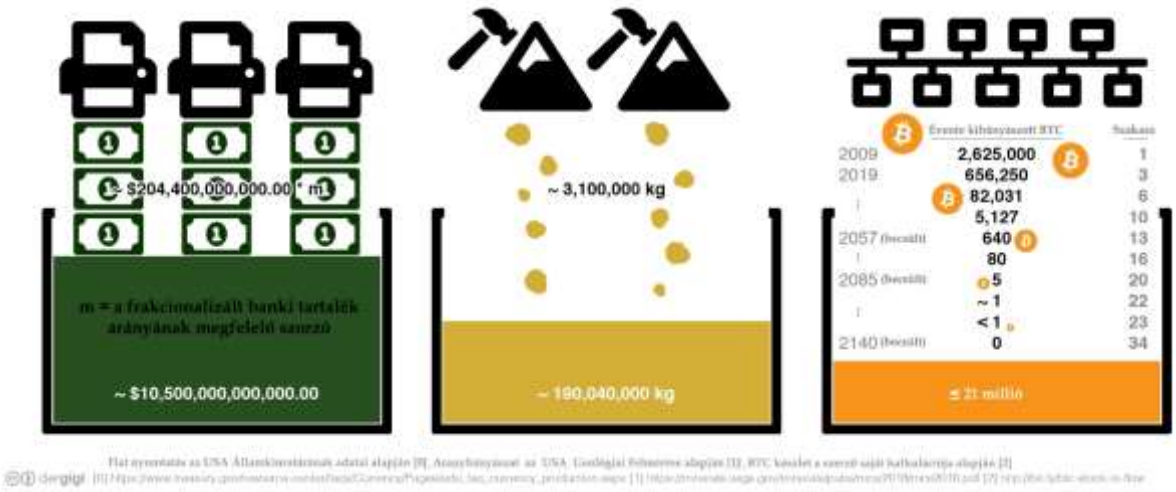
A különböző pénzeszközök keménységének a meghatározására az úgynevezett „stock to flow”, S2F arányt használják. A stock, az S az a jelenleg rendelkezésre álló készlet. A pénz esetében ez az aktuálisan forgalomban lévő készlet. A flow, az F pedig az, hogy adott időszak, például egy év alatt mennyivel növekszik ez a készlet. Ha megértjük az S2F arányt, megértjük, hogy egy pénz mennyire kemény, mennyire stabil.

A fiat pénzek esetén nehézkes az S2F meghatározása, hiszen nem mindegy, hogy mit tekintünk fiat pénznek. Mondhatjuk azt, hogy csak a bankjegyek és az érmék számítanak (ez az M0 készlet), vagy hozzáadhatjuk a bankszámlákon, csak digitálisan létező pénzt is (M1), de ide számíthatnak a különböző takarékszámlák, megtakarítási eszközök is (M2), vagy akár még a letétigazolások (M3) is. Ráadásul az, hogy ezekben a kategóriákban pontosan mi is szerepel, országonként eltérhet. A világ tartalékvalutája az USA dollár, de a Fed valamiért abbahagyta az M3 számainak a publikálását, így teljes készletként az M2 használható. Az ember szívesen lellenőrizné ezeket a számokat maga is, de ehelyett meg kell bíznunk a Fed közleményeiben.

Az arany, mint legritkább fém a Földön, jelenleg a legmagasabb S2F aránnyal rendelkezik. A geológiai adatok alapján eddig összesen 190 ezer tonnát bányásztak ki. Az előző pár év átlaga pedig évente 3100 tonnányi arany. Ezekből a számokból könnyen kikalkulálhatjuk, hogy a 190 ezer tonna osztva a 3100 tonnával, durván 61-gyel egyenlő. Az arany S2F értéke tehát 61.

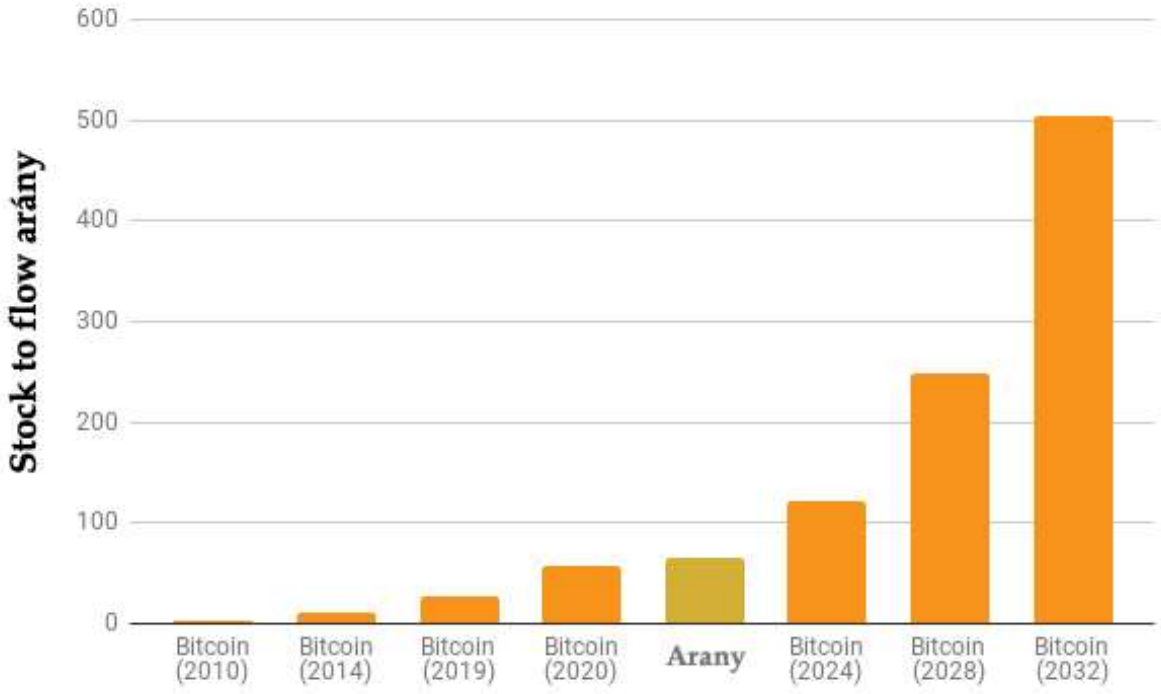
Ezzel az arany vezeti a mezőnyt. Érthető hát, miért számított az arany a világtörténelem során a legkeményebb, legmegbízhatóbb pénznek. A becslések alapján a világ összes aranya elférne pár Olimpiai méretű versenymedencében.

Aztán jött a bitcoin. Lehet, hogy hallottál róla már, a bitcoin bányászata rengeteg hírverést kapott az elmúlt években. Ennek az az elsődleges oka, hogy a bányászat korai szakaszában járunk, tehát minden egyes blokk viszonylag nagy jutalmat ér a létrehozásához szükséges munkáért cserébe. Jelenleg a negyedik szakaszban járunk, amely 2020 májusában kezdődött. A pontos dátumokat nehéz előre meghatározni a Bitcoin hálózatán, mivel a 10 perces blokkidő egy átlag, nem pedig kőbe vésett szabály. Az mindenesetre biztosra vehető, hogy a bitcoin S2F értéke növekszik. Hogy meddig? Nos, igazából szó szerint a végtelenségig.



Stock to flow arányok vizualizálva, a szerző saját ábrája

A bányászati jutalom exponenciálisan csökken, az új bitcoinok forgalomba kerülése lassul, az S2F arány ennek köszönhetően rakétaként tör felfelé. 2020-ban megközelítette az aranyét, és alig négy évvel később ráduplázz erre az arányra. Ez a duplázódás pedig összesen 64 alkalommal fog lejátszódni. Az exponenciális görbe alapján ötven év múlva már kevesebb, mint 100 új bitcoin kerül majd forgalomba évente, hetvenöt év múlva pedig kevesebb, mint 1. A blokkjutalom a 2140-es évek környékén végleg eltűnik, és gyakorlatilag nem fog új bitcoin létrejönni. Ez a hosszú távú berendezkedés. Te, aki ezt olvasod, kifejezetten korán érkeztél a területre.



S2F arány a bitcoin és az arany esetében

A bitcoin a végtelen S2F arányhoz közelít, így a valaha létező legkeményebb valuta lesz. Ezt nehéz túlszárnyalni. Ha a pénzügy lencséjén keresztül nézzük, a Bitcoin úgynevezett nehézségi igazítása valószínűleg a legfontosabb összetevő a rendszerben. Hogy milyen gyorsan jön létre új bitcoin, az attól függ, hogy mennyire nehéz a bányászat. Elméletileg igazából a blokktalálattól függ, de a mi szempontunkból ez a bányászatot jelenti, és 2140-ig ezt is fogja. A hálózat a résztvevőktől függően dinamikusan változtatja a bányászati nehézséget, és ezzel lehetővé teszi, hogy előre jelezhessük a készlet jövőbeli alakulását.

A nehézségi igazítás egyszerűsége esetleg azt a képzetet keltheti, hogy jelentéktelen dolog. A nehézségi igazítás viszont az einsteini alapelvek forradalmi alkalmazása. Ez biztosítja, hogy a bitcoin előre meghatározott készlete és kibocsátási rátája a túl sok vagy a túl kicsi bányászati erő alkalmazásával sem borul fel. Ellentétben a világ összes többi „nyersanyagával”, a bitcoin esetében nem számít, hogy mekkora mértékben növeljük meg a bányászatra fordított energiát, a jutalom mértéke nem fog változni.

Ahogyan az $E=mc^2$ képlet megszabja, hogy az univerzumunkban mekkora lehet a maximális sebesség, úgy a nehézségi igazítás megszabja a bitcoin korlátait. Ha nem létezne ez az igazítás, már rég kibányászták volna az összes bitcoint. A bitcoin valószínűleg túl sem élte volna az első pár évet. A nehézségi igazítás oldja meg, hogy az adott jutalmazási szakaszban a hálózat a megfelelő módon biztosítva legyen. Ez biztosítja, hogy folyamatosan, a meghatározott sebességgel jöjjön létre minden új blokk, és kerüljön forgalomba az új bitcoin. Egyfajta termosztátként működik, amely a Bitcoin monetáris berendezkedését szabályozza.

Einstein rámutatott valami fontosra: nem számít, mennyire erősen tolsz valamit, egy bizonyos ponton túl már nem lehet jobban felgyorsítani. Satoshi is valami hasonlót mutat nekünk, hiszen nem számít, mennyire keményen kutatsz ez után a digitális arany után, egy bizonyos szint után már nem tudsz többet szerezni. Az emberiség történelme során először van egy olyan pénzeszközünk, amelyből egyszerűen nem lehet többet előállítani, bármilyen erősen is próbálkozunk.

A bitcoin megtanította, hogy a stabil pénz létfontosságú.

Harmadik rész, technológia

Ezúttal jobban fogom csinálni! – mondta magának, miközben elővette a kis aranykulcsot, és kinyitotta a kertbe vezető ajtót.

Aranykulcsok, órák, amelyek nem úgy működnek, ahogyan megszoktuk, versenyek furcsa rejtvényekkel, és névtelen, arctalan építők. Ez úgy hangzik, mintha egy tündérmese lenne Csodaországból, de ez valójában a Bitcoin napi valósága.

Ahogyan a Második részben olvashattad, a jelenlegi pénzrendszerünk nagyobb része alapjaiban hibás. Ahogyan Alice, mi is csak abban reménykedhetünk, hogy másodszorra már jobban csináljuk majd. Köszönhetően viszont egy ismeretlen alkotónak, most a rendelkezésünkre áll egy kifinomult technológia, a Bitcoin. A problémamegoldás egy decentralizált, ellenséges környezetben, egyedi megoldásokat kíván. A csomópontok világában a problémákra minden jellemző, csak az nem, hogy egyszerűen megoldhatók. A Bitcoin sok esetben alapoz az erős titkosítási megoldásokra, főleg, ha a technológia szemszögéből nézzük. Hogy ez a titkosítás mennyire erős, arról is szót ejtünk majd.

A kriptográfia segítségével távolítja el a rendszerből a közvetítőket a Bitcoin. Ahelyett, hogy egy központi szereplőben kellene megbíznunk, a hálózat az univerzum legnagyobb erejét hívja segítségül, a fizikát. Persze, egy leheletnyi bizalom azért még szükséges ezután is, erről is beszélni fogok az egyik leckében.

Az utolsó pár lecke a Bitcoin mögötti technológiai fejlesztések világába kalauzol el, a mögöttes filozófiához. Ez ugyanolyan fontos, mint a technológia maga. A Bitcoin nem egyszerűen egy új, trendi app a telefonodon. A Bitcoin egy teljesen új pénzügy valóság alapja, pontosan ezért kellene úgy kezelni, mint egy atombiztos pénzügyi rendszert.

Hol állunk most ebben a pénzügyi, társadalmi, technológiai forradalomban? A már létező technológiák és hálózatok akár összehasonlítási alapként is szolgálhatnak a Bitcoin jövője számára, az utolsó leckében ezért pontosan ezt fogjuk közelebbről szemügyre venni.

Szóval kösd be magad, és élvezd az utazást! Ahogyan minden exponenciális technológia esetében, most is parabolikus emelkedés következik.

Tizenötödik lecke: A számok ereje

Lássuk, tehát négyszer öt az tizenkettő, négyszer hat az tizenhárom, és négyszer hét az tizennégy… ó jajj! Sosem fogok így eljutni húszig!

A számok létfontosságúak a mindennapi életünkben. A nagy számokkal viszont kevesen vannak jó viszonyban. A legnagyobb számok, amelyekkel találkozhatunk, a milliós, millárdos, esetleg a billiós tartományba esnek. Olvashatunk az újságokban arról, hogy milliók élnek nyomorban, milliárdos mentőcsomag kell a bankoknak, vagy éppen valahány billió az államadósság. Ezek a főcímek nem nagyon ragadják meg a lényeget, de az emberek többsége mégis viszonylag kényelmesen át tudja gondolni az ekkora számokat.

Viszont hiába tudjuk kezelni ezt a nagyságrendet, az intuíciónk itt azért már kezd rendetlenkedni. Például van elképzelésed arról, hogy mennyi ideig tart, míg eltelik egymillió, egymilliárd, vagy egybillió másodperc? Ha hasonlítasz rám ebben, akkor valójában fogalmad sincs arról, hogy mit is jelentenek ezek a számok. Szóval nézzük meg közelebbről!

A különbség ezek között három nagyságrend, tehát 10^6, 10^9, 10^{12} másodpercről beszélünk. A másodpercek használata nem túl praktikus, szóval fogalmazzuk meg kicsit hétköznapibb mértékegységgel:

- 10^6, tehát egymillió másodperc másfél hetet jelent.
- 10^9, egymilliárd másodperc 32 évnyi idő.
- 10^{12}, egybillió másodperccel ezelőtt Manhattan szigetét elég vastag jégréteg borította.

1 billió másodperccel ezelőtt; xkcd #1225

Ahogyan belépünk a modern kriptográfia asztronómiai léptékű számainak a világába, a képzeletünk felmondja a szolgálatot. A Bitcoin hatalmas számokra épül, és arra, hogy ezeket

nem lehet kitalálni. Ezek a számok pedig sokkal, de tényleg sokkal nagyobbak, mint azt el tudnánk képzelni. Nagyságrendekkel nagyobbak. Hogy megérthesd a Bitcoin egészét, érdemes ezeket a számokat is megérteni.

A Bitcoin az SHA-256 algoritmust használja a hasheléshez, az adatok titkosításához. Azt gondolhatnánk, hogy a 256 az nem olyan nagy szám, de az SHA-256 elnevezésében a 256 valójában a nagyságrendet jelenti. Ekkora nagyságrend már megdolgoztathatja az agyunkat. A 256 bites biztonság esetében félrevezető lehet, ha a kétszázötvenhatra gondolunk. Ez nagyságrendet jelent, ahogyan a millió az annyi, mint tíz a hatodikon, a milliárd pedig tíz a kilencediken. Az SHA-256 az azt jelenti, hogy a használt szám az 2^{256}, tehát kettő a kétszázötvenhatodikon.

Ez mennyire erős titkosítás?

„Az SHA-256 nagyon erős. Nem olyan, mintha csak egy következő lépcsőfok lenne, mint az SHA1 az MD5 után. Évtizedekig használható marad, hacsak nem történik valami hatalmas jelentőségű áttörés a területen."

Satoshi Nakamoto

Nézzük meg pontosan, hogy miről is beszélünk! Ez egészen pontosan 78 számjegyet jelent a tizes számrendszerben.

2^{256} = 115.792.089.237.316.195.423.570.985.008.687.907.
853.269.984.665.640.564.039.457.584.007.913.129.639.936

Ez sokkal több, mint a létező atomok száma az ismert univerzumban, igazából nincs is mihez hasonlítanunk ekkora számot. Hogy ezt teljes valóságában felfogjuk, szinte lehetetlen. Az emberi agy nem erre van tervezve.

Ha van kedved, egy videót is megnézhetsz erről, Grant Sanderson nagyon jól vizualizálta, hogy mekkora léptékekről van szó. A „How secure is 256 bit security?" című, angol nyelvű videót a https://www.youtube.com/watch?v=S9JGmA5_unY oldalon tekintheted meg. Ahogyan az alkotó többi videója, ez is egyszerre lenyűgöző, és hihetetlenül informatív. Az embernek kedve támad még jobban belemerülni utána a matematika világába.

Bruce Schneier a számítógépek fizikai korlátai segítségével is elmagyarázta, hogy mekkora számokat kell magunk elé idéznünk. Ha sikerülne építeni egy hatalmas számítógépet, és a bolygónk központi csillaga, a Nap összes energiáját fel is használnánk, százmilliárdszor százmilliárd évnyi kalkuláció után is mindössze 25%-os esélyünk lenne megtalálni egy tűt a 256 bites szénakazalban.

„Ezek a számok nem a számítógépek, mint eszközök technológiájától függnek. Ezeket a termodinamika törvényei maximalizálják. A 256 bites kulcsok feltörése nyers erővel azután válik lehetségessé, ha a számítógépeket már nem anyagból készítik, és nem a fizikai térben léteznek."

Bruce Schneier

Nehéz ennél egyértelműbben megfogalmazni ezt. Ráadásul a kriptográfia erőssége felborítja a valódi, fizikai világban tapasztalható erőviszonyokat. A való világban nincs törhetetlen dolog. Ha elég keményen próbálkozol, kinyitható bármely ajtó, széf, kincsesláda. A Bitcoin kincsesládája viszont máshogyan működik. Kriptográfia védi, az pedig nem törhető fel nyers erővel. Márpedig amíg a matematikai törvényszerűségek működnek, nincs más, csak a nyers erő. Van esély persze az emberi oldal „feltörésére", de a fizikai erőszak alkalmazása nem old fel minden bitcoin-címet, a nyers erő pedig elvérzik a Bitcoin titkosítási sáncain. Akkor is, ha valaki ezernyi csillag erejét használja. Mármint szó szerint, akkor is. Ahogyan a cypherpunkok körében ismert mondás tartja, „a matematikai problémákat nem lehet kényszerítő erővel megoldani".

„Nem annyira magától értetődő, hogy a világnak így kellene működnie. De valahogy mégis, az univerzum rámosolyog a titkosításra."

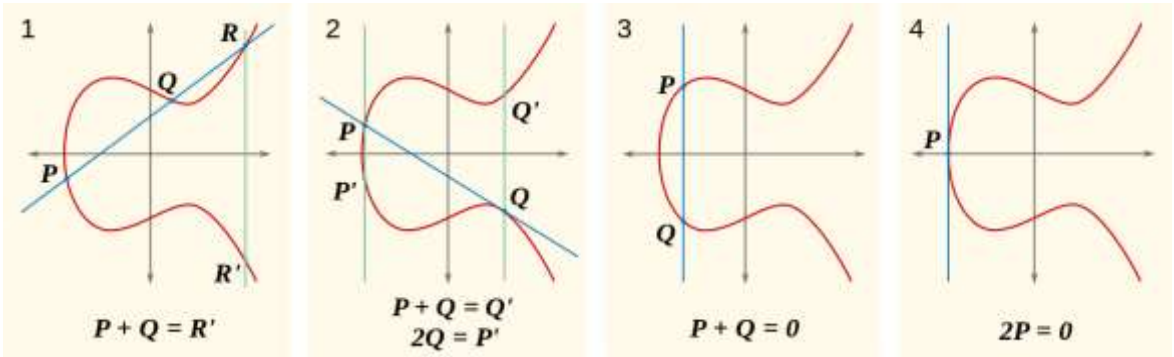
Julian Assange

Azt még senki sem tudja, hogy az univerzum mosolya vajon őszinte-e. Lehetséges, hogy a matematikai feltevéseink helytelenek, és valahogy rájövünk, hogy X egyenlő Y-nal, vagy esetleg valamely nagyon nehéz, speciális problémáról derül ki, hogy egyáltalán nem nehéz. Ha ez a helyzet, akkor a kriptográfia a jelenlegi formájában megszűnik létezni, a világunk pedig a felismerhetetlenségig megváltozik ennek következményeként.

„Vires in Numeris = Számokban az erő"

epii

Ez a kifejezés nem egyszerűen egy jól hangzó mottó, amelyet a bitcoinerek mantráznak. A felismerés, hogy egyfajta legyőzhetetlen erő van a számokban, a megvilágosodással érhet fel. Mikor megértettem ezt, és a hatását a világ jelenlegi erőviszonyaira, az megváltoztatta a világnézetemet, és azt, ahogyan a jövőbe tekintek. A számok erejének legegyszerűbb bizonyítéka az, hogy senkitől sem kell engedélyt kérned a Bitcoin használatára. Nincs weboldal, ahol regisztrálni kellene. Nincs cég, amely irányítaná a rendszert, nincs állami hatóság, és nincs formanyomtatvány, amelyen be kell adni a kérvényt. Generáltass a számítógépeddel egy jó nagy számot, és kész is vagy. A számok mögötti hatóságot úgy hívják, hogy matematika. És csak Isten tudja, hogy ott ki a főnök.



Elliptikus görbék; Emmanuel Boutet

A Bitcoin a valóságról alkotott jelenlegi ismereteinkre épül. Számos nyitott kérdés létezik még a fizika, számítástechnika, és a matematika terén, de vannak dolgok, amelyekben már eléggé biztosak vagyunk. Aszimmetria van aközött, hogy mennyire nehéz megoldani egy problémát, és leellenőrizni, hogy tényleg megoldottuk-e. Az is biztos, hogy a számításokhoz energia kell. Más szóval megfogalmazva, sokkal nehezebb megtalálni egy tűt a szénakazalban, mint megmondani, hogy az a hosszú, hegyes dolog a kezdben tű, vagy szénaszál. A tű megtalálása pedig munkával jár.

A bitcoin-címek lehetséges változatainak a száma szinte leolvasztja az ember agyát. A privát kulcsok száma is. Lenyűgöző, hogy az egész modern világ elhasal a tűkeresés feladata előtt, akkora elképzelhetetlenül nagy a szénakazal. Most már sokkal jobban értem ezt, mint régebben.

A Bitcoin megtanított a számok erejére.

Tizenhatodik lecke: Ne bízz! Bizonyosodj meg!

Előbb lássuk a bizonyítékot, – mondta a király, – *aztán ítélkezünk.*

A Bitcoin arra lett létrehozva, hogy lecserélje a jelenlegi pénzrendszerünket, vagy legalábbis azzal párhuzamosan működjön. A hagyományos pénznemeket központi szereplők bocsátják ki, az olyan tartalékvaluták esetében is, mint az USA dollár, vagy említhetjük akár a népszerű lövöldözős játék, a Fortnite V-Bucks nevű, játékon belüli virtuális pénzét. Mindkét esetben meg kell bíznod a kibocsátókban, akik létrehozzák, menedzselik, kezelik a pénzt. A Bitcoin megszünteti ezt a bizalmat, ez a legfőbb probléma, amelyet a hálózat kezelni tud.

„A legfőbb probléma a jelenlegi pénzrendszerünkkel az, hogy bíznunk kell a működtetőkben. Egy olyan elektronikus fizetési megoldásra van szükségünk, amely nem a bizalmon, hanem a kriptográfián alapul."

Satoshi

A Bitcoin úgy oldja meg a bizalom problémáját, hogy teljesen decentralizáltan működik, bármiféle központi szereplő nélkül. Nem egyszerűen harmadik felek kikerülésével, hanem szó szerint központ nélkül. Ha pedig nincs központ, nincs kiben megbízni. A Bitcoin innovációja a teljes decentralizációban rejlik. Ez az ellenálló-képesség alapja, az ok, hogy miért működik még ma is. A decentralizáció az indok, amiért bányászni kell, csomópontokra van szükség, hardvertárcákat használunk, és igen, egymáshoz láncolt blokkokban tároljuk az adatokat. Az egyetlen dolog, amelyben bíznunk kell, az az, hogy a matematika és a fizika nem fog egyszer csak gyökeresen megváltozni, és az, hogy a bányászok többsége rendesen viselkedik. Erre pénzügyi ösztönzők is vannak a rendszerben, hiszen blokkjutalmat csak a szabályos blokkokért lehet kapni.

A világ úgy működik, hogy „Bízzál, de azért bizonyosodj is meg.", a Bitcoin viszont a „Ne bízz, hanem mindenképpen bizonyosodj meg!" elvet követi. Satoshi nagyon is világossá tette a bizalom kiiktatásának a fontosságát. A white paper bevezető szekciója mellett az végkövetkeztetések között is megemlítette.

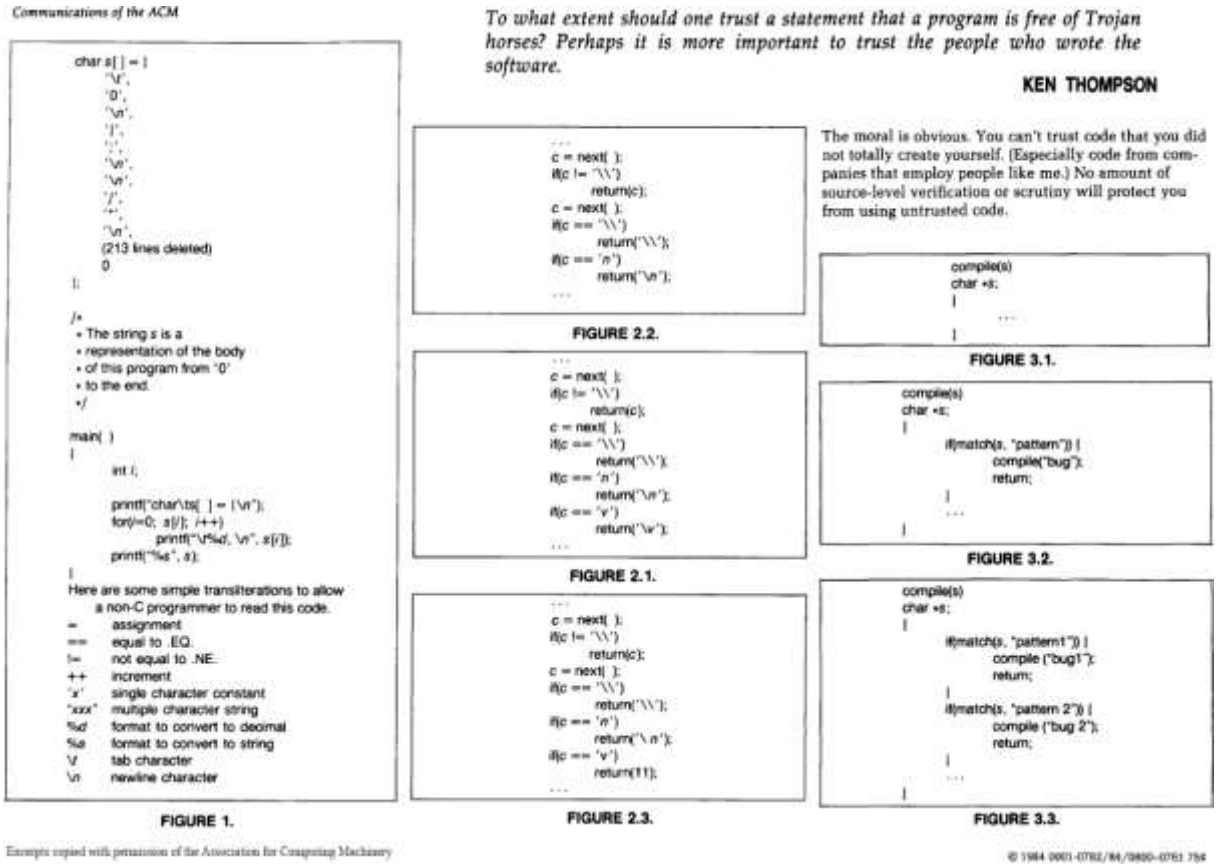
„Létrehoztunk tehát egy rendszert az elektronikus tranzakciókhoz, amely nem a bizalmon alapul."

Satoshi Nakamoto

A bizalom pedig itt egy nagyon specifikus kontextusban kerül elő. Megbízható harmadik felekről beszélünk, tehát olyan szervezetek, közvetítők kerülnek szóba, akik létrehozzák, őrzik, és kezelik a pénzedet. Emellett feltételezhetjük azt is, hogy az ember megbízhat a saját számítógépében is.

Ahogyan Ken Thomson a Turing-díjas értekezésében rámutatott, a számítástechnika világában nagyon trükkös dolog a bizalom. Amikor egy programot futtatsz, meg kell bíznod egy sor szoftverben, ráadásul a hardvereidben is, hiszen a használni kívánt programodat mindegyik

befolyásolni tudja, rosszindulatú módon is akár. Ahogyan végül Thomson összegzi ezt, „az ember nem bízhat meg teljesen semmilyen kódban, hacsak nem ő írta az egészet”.


Communications of the ACM

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

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.

FIGURE 1.

FIGURE 2.2.

FIGURE 2.1.

FIGURE 2.3.

FIGURE 3.1.

FIGURE 3.2.

FIGURE 3.3.

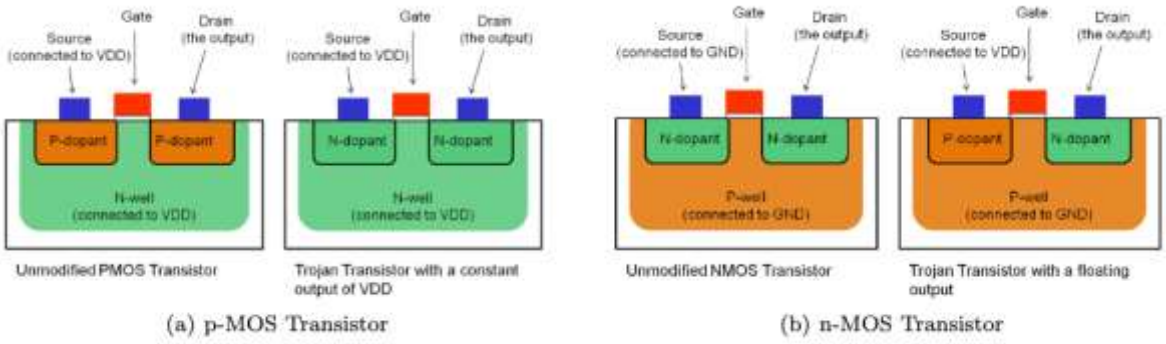
Kód; Association of Computing Machinery

Thomson rámutatott, hogy ha hozzáférésed is van a forráskódhoz, bármely program vagy hardver módosított lehet, és ezeket a hátsú kapukat elképesztően nehéz észrevenni. Éppen emiatt gyakorlatilag nem létezik bizalommentes rendszer. Ehhez neked magadnak kellene megírnod a programjaid kódját, és megépítened fizikailag az összes hardvert, gépalkatrészt, bármiféle külső segítség nélkül.

„Ha a nulláról akarsz nekiállni almáspitét sütni, ahhoz újra meg kell teremteni az univerzumot.”

Carl Sagan

A Ken Thomson Hack néven ismert hátsó kapu egészen zseniális megoldás. Nézzük meg egy kicsit közelebbről, hiszen ezt észrevenni sem lehet, ráadásul a szoftverek megváltoztatása nélkül működik. A kutatók rájöttek, hogyan tudják kompromittálni a biztonsági szempontból fontos hardvereket, az áramkörök polaritásának a megváltoztatásával. Fizikailag meg lehet változtatni a számítógép-csipek alkotóelemeinek a tulajdonságait, így befolyásolhatjuk a titkosítás felelős véletlenszám-generátor működését. Ezt a változtatást pedig nem lehet észrevenni, hiszen nem lehet látni. Márpedig a csipek legfőbb ellenőrzési metódusa az, hogy alaposan átnézik azokat, optikai eszközökkel.



Láthatatlan, hardveres trójai; Becker, Regazzoni, Paar, Burleson

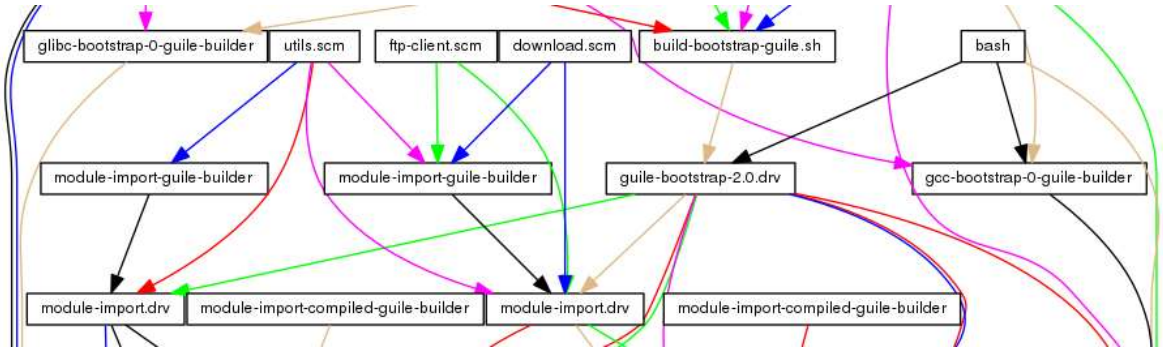
Ijesztően hangzik, igaz? Szóval, ha képes is vagy mindent megépíteni teljesen a nulláról, akkor is bíznod kell abban, hogy a matematika alapvető szabályai kitartanak. Hinnünk kell, hogy a secp256k1 függvény, amelyet a titkosításhoz használnak, egy hátsó kapuk nélküli elliptikus görbe. A rosszindulatú hátsó kapuk még ezen a szinten is lehetségesek, a kriptográfia alapjait adó matematikai funkciókban is feltűnhetnek, ahogy ez már legalább egyszer meg is történt. Jó okunk lehet hát a paranoiára, hiszen szó szerint bármi, szoftver, hardver, és még a használt algoritmusok is kompromittálódhatnak.

„Ne bízz, bizonyosodj meg!”

Látható tehát, hogy a tényleges bizalommentesség csak egy álom a számítástechnikában. A Bitcoin az a rendszer, amely valószínűleg a legközelebb van ehhez az állapothoz, de még így is inkább minimalizálja csak a bizalmat, nem pedig teljesen kiiktatja. Valójában számos más ponton szükség van a bizalomra, hiszen el kell fogadnunk, hogy a számítási kapacitáshoz energia kell, hogy X nem egyenlő Y-nal, és, hogy te a valóságban tartózkodsz, nem pedig egy rosszindulatú összeesküvés által fenntartott szimulációban.

A fejlesztők azon dolgoznak, hogy még nagyobb mértékben eltávolíthassák a bizalmat a rendszerből. Létrehoztak például egy szoftver-megosztó kezdeményezést Gitian néven, ezzel előre meghatározott építési utakat lehet követni. Ha több fejlesztő egymástól függetlenül ugyanazokat az eredményeket kapja a meghatározott útvonalakon, akkor nagyobb a valószínűsége, hogy nem történt rosszindulatú beavatkozás. De nem a hátsó kapuk jelentik az egyedüli támadási vektort. Az egyszerű zsarolás és fizikai kényszerítés ugyanúgy működhet. A decentralizáció alapvetően csak csökkenti a bizalmat.

Nagy erőfeszítések történnek, hogy túljuthassunk a „tojás-vagy-a-tyúk” problémán, és az egyik ilyen például a Guix. Ezzel úgymond le tudsz ellenőrizni bármilyen kódot, hogy úgy néz-e ki, ahogyan eredetileg kellene neki. Tehát ha valaki ártó szándékkal beleírt valamilyen plusz dolgot, azt észre lehet venni. Így nem vagy ráutalva, hogy különböző szoftver-megosztó platformokban kelljen megbízni, hogy a letöltött kódod a kívánt módon működik. Ha a Bitcoin fejlesztésével foglalkozik valaki, akkor a jó hír, hogy nemrégiben felvetődött az ötlet, a Guix megoldása kerüljön bele a fejlesztési környezetbe.



Melyik volt előbb, a tyúk vagy a tojás?

Szerencsére a Bitcoin nem egyetlen algoritmuson vagy hardveren alapul. A Bitcoin nagymértékű decentralizációjának az egyik pozitív következménye az elosztott biztonsági modell használata. A fent említett sebezhetőségeket nem szabad könnyelműen venni, valószínűtlen, hogy minden szoftvertárca, minden hardvertárca, minden titkosítási megoldás, minden csomópont-szoftver, és minden programnyelv kompromittálódott. Lehetséges, viszont nagyon valószínűtlen.

A privát kulcsok létrehozhatók számítógép és szoftver nélkül is. Egyszerű érmefeldobálással is végig lehet menni a karaktereken, bár a saját dobálási stílusod, vagy éppen az érmétől függően a véletlenszerűség nem biztos, hogy 100%-os. Ez az egyik oka, hogy például a Glacierhez hasonló tárolási szolgáltatók például kaszinókban alkalmazható minőségű dobókockákat is használnak a véletlenszám-generátoraikban.

A Bitcoin rákényszerített, hogy átgondoljam, mit is jelent megbízni másokban. Felhívta a figyelmem, hogy a hibakeresés vagy a szoftverfejlesztés során milyen bizalmi láncolaton kell végigmennünk, és rámutatott, hányféle különböző módon lehet befolyásolni a programokat és a hardvereket.

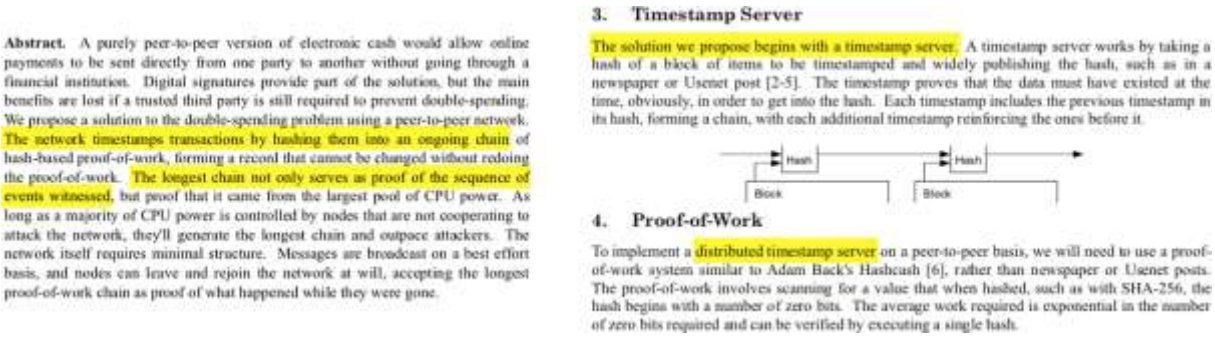
A Bitcoin megtanította, hogy ne bízzak, hanem bizonyosodjak meg.

Tizenhetedik lecke: Tudnunk kell a pontos időt

Kedveském, így el fogok késni!

Sokszor lehet hallani, hogy a bitcoin bányászattal jön létre, mivel számítógépek ezrei dolgoznak nagyon bonyolult matematikai problémák megoldásán. Meghatározott problémákra kell megoldást találni, és ha sikerül, akkor azzal hozod létre az új bitcoint. Ez egy nagyon leegyszerűsített nézőpont, és figyelmen kívül hagyja a lényeget. A bitcoint nem kell létrehozni, és a rendszer nem a matematikai problémák megoldásáról szól. Valójában a matematikai része nem is nehéz. Ami valójában nehéz, az a pontos idő meghatározása egy decentralizált rendszerben.

Ahogyan a white paper kiemeli, a proof of work (a bányászat) ahhoz kell, hogy egy elosztott időbélyegző-szerver működhessen a hálózaton.



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.

Kivonat a white paperből. Valaki azt mondta, hogy időlánc?

Mikor először hallottam a Bitcoinról, azt hittem, hogy a PoW nem hatékony, és pazarló megoldás. Egy idő után viszont elkezdtem máshogyan tekinteni az energiafelhasználás kérdésére. A jelek szerint a proof of work még ma, egy évtizeddel a Bitcoin megszületése után is teljesen félre van értelmezve.

A matematikai „problémák”, amelyet a PoW megold, úgymond kitaláltak, ezért sokan úgy vélik, az a munka haszontalan. Ha kizárólag a számítási teljesítményre fókuszálunk, akkor ez a nézet igaz. De a Bitcoin nem a számításokról szól. A Bitcoin arról szól, hogy egymástól függetlenül egyetértésre juthassanak a résztvevők az események sorrendjében.

A proof of work az a metódus, amely használatával bárki meg tud bizonyosodni arról, hogy mi minden történt, és milyen sorrendben történt. Ez az egyéni megbizonyosodás vezet a konszenzushoz, a több résztvevő közötti egyetértéshez, hogy ki mit birtokol.

Egy végletekig decentralizált környezetben nincs meg az a luxus, hogy valaki megmondja nekünk a pontos időt. Bármely harmadik fél, aki üzembe állítana egy órát, egyben központi sebezhetőséget is hozna a rendszerbe, amely mentén az támadhatóvá válna. Márpedig ahogyan Grisha Trubetskoy megfogalmazta, minden az időzítésen múlik. Satoshi pedig pontosan ezt a problémát oldotta meg, egy decentralizált óra létrehozásával, amely egy proof

of work blokklánc segítségével működik. Mindenki elfogadja tényként, hogy az a lánc a valódi lánc, amely a legtöbb munkát összesíti, amely ezért a legértékesebbnek számít. Így van meghatározva az, hogy valójában mi történt, és ez a megegyezés az, amelyet a számítástechnika-tudományban Nakamoto-konszenzusnak neveznek.

„A hálózat időbélyegzővel látja el a tranzakciókat a hashelés során, ezután pedig ezek lánc-szerűen kerülnek összefűzésre. Ezzel lehet bizonyítani a tapasztalt események pontos sorrendjét."

Satoshi Nakamoto

Ha nincs egy következetesen használható módszerünk, amellyel megmondhatjuk a pontos időt, akkor nem tudjuk meghatározni, hogy mi történt előbb, és mi később. Lehetetlen megmondani a pontos sorrendet. A Nakamoto-konszenzus segítségével a Bitcoin megbízhatóan tudja mérni az időt. A hálózat pénzügyi motivációt használ, hogy fenntartsa ezt a decentralizált órát, az emberi kapzsiságra és az önérdek érvényesítésére a versengő felek között. Hogy maga az óra nem pontos, igazából nem számít. Az események sorrendje a valódi információ, ezt pedig bárki önállóan le tudja ellenőrizni.

A proof of work konszenzusnak köszönhetően a munka és a megbizonyosodás egyaránt teljes mértékben decentralizált. Bárki csatlakozhat, bárki kiléphet, önként, bárki megbizonyosodhat bármiről, bármikor. Ráadásul bárki önállóan, egyedül képes leellenőrizni a teljes rendszert, anélkül, hogy meg kellene bízni másokban.

A proof of work megértése időbe telik. Nem túlságosan magától értetődő, és hiába egyszerűek a szabályok, egy nagyon összetett rendszert működtetnek. Nekem az segített, mikor máshogy kezdtem gondolkodni a bányászatról. A hasznosságot láttam benne, nem a pazarlást. Megbizonyosodást, nem pedig üres számításokat. Időt, nem pedig blokkokat.

A Bitcoin megtanította, hogy nem egyszerű megmondani a pontos időt, főleg, ha decentralizált vagy.

***

A tükörben:

Bitcoin's Energy Consumption – A shift in perspective

Bitcoin is Time

Tizennyolcadik lecke: Mozogj lassan, nehogy valamit összetörj!

A hajó lassan körözött a vizen a melengető nyári napsütésben, a legénység vidám hangjait, nevetését hallatva.

Mostanra már idejétmúlt mantrának számíthatna, de a „csináld gyorsan, nem baj, ha összetörsz valamit" mottó még mindig jellemző a technológiai szektorra. Az ötlet, hogy nem baj, ha valami elsőre nem sikerül, a korai és sűrű hibázás mentalitásának az egyik pillére. A növekedés jelenti a sikert, ezért amíg növekedni tudsz, minden rendben van. Ha valami nem megy elsőre, akkor újrakezded, újragondolod. Más szavakkal megfogalmazva ez azt jelenti, hogy ha elég sok szart dobálsz a falra, valamennyi csak rajta marad.

A Bitcoin nem így működik. Nem is ilyenre lett megtervezve. Nem is szükséges, hogy így működjön. Ahogyan Satoshi rámutatott, az elektronikus pénzekkel sokszor próbálkoztak már, de minden kezdeményezés elbukott, mert le tudták állítani a központot, le tudták vágni a fejet. A Bitcoin viszont egy fej nélküli bestia.

„Az emberek többsége automatikusan elutasítja az e-pénzek témáját, mivel minden egyes ezzel foglalkozó cég bedőlt a '90-es évek óta. Remélem egyértelmű, hogy ez kizárólag a centralizált berendezkedésük miatt történt meg velük."

Satoshi Nakamoto

A teljes decentralizáció egyik következménye, hogy a rendszer nagymértékben ellenáll a változtatásnak. A „csináld gyorsan, nem baj, ha összetörsz valamit" nem működik a Bitcoin esetében, és soha nem is fog. Ha akarnánk, se lenne lehetséges anélkül, hogy szó szerint minden résztvevőt meggyőznénk a szükségességéről. Ez az elosztott konszenzus. Így működik a Bitcoin.

„A Bitcoin természete olyan, hogy már a 0.1-es verzió kiadásakor kőbe lettek vésve a fő működési szabályok, véglegesen."

Satoshi Nakamoto

A Bitcoin számos ellentmondó tulajdonsága közül ez az egyik Azt hihetnénk, hogy egy programot, egy szoftvert könnyű megváltoztatni, hiszen csak át kell írni a kódot. De a Bitcoin megváltoztatása elképesztően nehéz az alapvető természete miatt.

Hasu, „A Bitcoin társadalmi szerződése" című esszé szerzője nagyon jól rávilágított, hogy a Bitcoin szabályait úgy lehet megváltoztatni, ha először megszületik egy beadvány, egy fejlesztési javaslat, majd sikerül meggyőzni minden felhasználót, hogy elfogadja ezt a javaslatot. Ez a jellegzetesség kifejezetten ellenállóvá teszi a Bitcoint a változtatásokkal szemben, pedig a Bitcoin is egy szoftver.

Ez az ellenállóképesség a Bitcoin egyik legfontosabb tulajdonsága. A fontos szoftver-rendszereknek üzembiztosnak kell lenniük, a Bitcoin szociális és technológiai működési szabályosságai pedig képesek ennek megfelelni. A pénzügyi rendszerek a természetüknél fogva legtöbbször ellenséges környezetben működnek, azt pedig évezredek óta tudjuk, hogy ilyenkor különösen fontosak az erős, megbízható alapok.

„Megérkezett az eső és az áradás, és a feltámadó szelek ostromolták a házat, de az nem dőlt le, hiszen sziklára építették."

Máté evangéliuma, 7:24

Ebben a hasonlatban, amely a bölcsről és a bolondról szól, a Bitcoint nem a ház jelképezi, hanem a szikla. Megváltoztathatatlan, megmozdíthatatlan alap, amelyen egy új pénzrendszer nyugszik. A geológusok persze azt mondják, a sziklaformációk folyton mozognak és változnak, és igazából a Bitcoin is változik és fejlődik. Csak éppen tudni kell, hogy hová nézzünk, és mit keressünk.

Már vezettek be olyan fejlesztést, például a SegWit frissítést, amely bizonyítja, hogy a Bitcoin is tud változni, ha elegendő felhasználó érzi úgy, az újítás hasznos a hálózat számára. A SegWit teszi lehetővé például a Lightning Network működését, amely olyan, mint egy ház, a Bitcoin erős alapjaira épülve. A jövőben várhatók olyan fejlesztések is, amelyek a magánszférát hivatottak jobban védeni (Schnorr aláírások), vagy éppen olyan kódok, amelyeknek köszönhetően az okosszerződéseket nem lehet majd megkülönböztetni a hagyományos tranzakcióktól (Taproot). A bölcs építők erős alapokat választanak maguknak.

Satoshi nem csak technológiai szempontból számított bölcs építőnek, hanem az ideológiai döntések szükségszerűségét is felismerte.

„Ha nyílt forráskóddal dolgozunk, bárki átnézheti a kódot, önállóan. Ha zárt forráskódot használnánk, senki sem tudná leellenőrizni a biztonságosságot. Úgy gondolom, egy ilyen program esetében létfontosságú, hogy nyílt forráskódú legyen."

Satoshi Nakamoto

A nyitottság nagyon fontos a biztonsághoz, és az ingyenes, nyílt forráskódú szoftverek mozgalmának is nagy mozgatórugója. Ahogyan Satoshi rámutatott, a biztonsági protokolloknak nyitottaknak kell lenni, hiszen a titkolózásban nincs biztonság. Egy másik előny pedig ismét csak a decentralizációhoz kapcsolódik. Egy olyan program, amely szabadon futtatható, tanulmányozható, módosítható, másolható, továbbítható, biztosan széles körben elterjed.

A Bitcoin decentralizált természete miatt kell lassan, megfontoltan haladni. A csomópontok hálózatának mindegyikét független szereplők futtatják, akik alapvetően ellene vannak bármiféle változtatásnak, legyen az hasznos vagy rosszindulatú. Nem lehet kényszeríteni senkit semmire, a javaslatok felvetése után mindenkit egymás után meg kell győzni arról, hogy a javasolt változtatás jó és el kellene fogadni. Ez a központosítatlan folyamat, amely a változtatások felvetésének és bevezetésének egyetlen útja, elképesztően ellenállóvá teszi a hálózatot a rosszindulatú módosításokkal szemben. Persze, a hibák kijavítását is ugyanennyire

megnehezíti, ezért van az, hogy inkább mindenki eleve igyekszik elkerülni a hibázást, és senki sem akar összetörni semmit.

A Bitcoin megtanította, hogy a lassú haladás nem hiba, hanem követelmény.

Tizenkilencedik lecke: A magánszféra még nem veszett el

A játékosok mind egyszerre kezdtek neki, anélkül, hogy kivárták volna a sorukat, és hamar veszekedésbe torkollt az egész. A Királynő nemsokára dühbe jött, a lábával dobolt, és percenként kiáltotta, hogy „vágjátok le a fejét”, és „az ő fejét is vágjátok le!”.

Sokan hiszik, hogy a magánszférának valamikor a ’80-as években szakadt vége. A Bitcoin pszeudonim létrehozása, és még néhány esemény a közelmúltból rávilágított, hogy ez egyáltalán nem így van. A magánélet, a magánszféra létezik, bár az tény, hogy nehéz megszabadulni a mindent megfigyelő állami szemektől.

Satoshi komoly erőfeszítéseket tett, hogy elfedje a nyomait, és titokban tarthassa a személyazonosságát. Egy évtized múltán sem tudjuk, hogy ki volt Satoshi, egyetlen személy, vagy egy csoport, férfi vagy nő, esetleg egy időutazó mesterséges intelligencia, amely a Bitcoin segítségével akarja elfoglalni a világot. Az összeesküvés-elméleteket félretéve, Satoshi úgy döntött, hogy az internetes személyiségének egy japán férfinevet választ, így bár nem tudunk erről megbizonyosodni, férfiként és egyetlen személyként hivatkozhatunk rá.

„Nem Dorian Nakamoto vagyok.”

Függetlenül a valódi személyazonosságától, el kell ismernünk, hogy Satoshi sikeresen megőrizte a magánszféráját. Mindenki számára egyértelműen megmutatta, hogy lehetséges online is névtelennek maradni.

„A titkosítás működik. A megfelelően beállított erős kriptográfiai rendszerek azon kevés dolgok közé tartoznak, amelyekben meg lehet bízni.”

Edward Snowden

Nem Satoshi az első pszeudonim vagy anonim feltaláló a világon, és biztos, hogy nem is az utolsó. Van, aki már le is másolta az ő névtelen módszerét, mint Tom Elvis Yedusor a MimbleWimble projekt bemutatásakor, mások pedig emelt szintű matematikai bizonyításokat tesznek le az asztalra, teljesen anonim módon.

Furcsa világban élünk. Egy világ, ahol a személyazonosság választható, az együttműködés alapja a kiválóság, az emberek pedig szabadon tudnak tranzaktálni, összedolgozni. Meg kell

szokni ezeket az új paradigmákat, de hiszem, hogy ezek mindegyike képes jó irányba megváltoztatni a világot.

Mindannyiunknak észben kellene tartani, hogy a magánélethez való jog az alapvető emberi jogok közé tartozik. Amíg az emberek harcolnak ezekért a jogokért, addig a magánszféráért vívott csata nem dőlt el.

A Bitcoin megtanította, hogy a magánszféra nagyon is létezik.

***

A tükörben:

True Names Not Required

Huszadik lecke: A cypherpunkok kódokat írnak

Látom, próbálsz valamit létrehozni.

Hasonlóan a többi korszakalkotó ötlethez, a Bitcoin sem a semmiből került elő. Matematikai, fizikai, számítástechnikai és egyéb innovációk, felfedezések kombinációjának köszönhetően jöhetett létre. Bátran kimondhatjuk, hogy Satoshi egy zseni, de nem tudta volna létrehozni a Bitcoint, ha nem tud óriások vállára állni.

„Aki csak reménykedik és vágyakozik, sosem fogja aktívan irányítani az eseményeket, sem pedig formálni a végzetét."

Ludwig Von Mises

Az egyik ilyen óriás Eric Hughes, a cypherpunk mozgalom alapítója, a Cypherpunk Manifesztum szerzője. Nehéz elhinni, hogy Satoshi nem merített volna ihletet az ő munkásságából. Rengeteg dolog szerepel benne, amelyet a Bitcoin lehetővé tesz, például a felhasználók közötti közvetlen tranzakciók, az elektronikus pénz, az anonim hálózatok, és a magánélet védelme titkosítás valamint digitális aláírások segítségével.

„A magánszféra létfontosságú minden társadalom számára az elektronikus korban. Mi pedig magánszférát akarunk, tehát biztosítanunk kell, hogy a tranzakciók minden résztvevője csak annyi információval rendelkezik, amennyi ténylegesen szükséges az adott tranzakció lebonyolításához.

Ennélfogva egy társadalomban akkor létezik a magánszféra, ha lehetőségünk van anonim tranzakciókra. Mostanáig a készpénz biztosította ennek a lehetőségét. Egy anonim pénzrendszer nem jelent titkos pénzrendszert.

Mi, a cypherpunkok, elköteleztük magunkat az anonim rendszerek létrehozása mellett. Megvédjük a magánszféránkat titkosítással, anonim email-küldéssel, digitális aláírással és elektronikus pénzzel.

A cypherpunkok kódokat írnak."

Eric Hughes

A cypherpunkoknak nem elég a vágyakozás és a remény. Aktívan részesei akarnak lenni az eseményeknek, és formálni a saját végzetüket. Ezért kódokat írnak.

Ezért, akár egy vérbeli cypherpunk, Satoshi leült, és nekiállt kódolni. Egy absztrakt ötletet formált kóddá, és bebizonyította a világnak, hogy a dolog működhet. Egy kóddá, amely aztán egy teljesen új gazdasági realitás alapja lett. A kódnak köszönhetően erről bárki saját maga megbizonyosodhat, és átlagosan 10 percenként a Bitcoin is bebizonyítja ezt a világnak egy új blokk létrehozásával.

```
23  map<uint256, CBlockIndex*> mapBlockIndex;
24  const uint256 hashGenesisBlock("0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f");
25  CBlockIndex* pindexGenesisBlock = NULL;
26  int nBestHeight = -1;
27  uint256 hashBestChain = 0;
28  CBlockIndex* pindexBest = NULL;
 :
675 int64 CBlock::GetBlockValue(int64 nFees) const
676 {
677     int64 nSubsidy = 50 * COIN;
678
679     // Subsidy is cut in half every 4 years
680     nSubsidy >>= (nBestHeight / 210000);
681
682     return nSubsidy + nFees;
683 }
684
685 unsigned int GetNextWorkRequired(const CBlockIndex* pindexLast)
686 {
687     const unsigned int nTargetTimespan = 14 * 24 * 60 * 60; // two weeks
688     const unsigned int nTargetSpacing = 10 * 60;
689     const unsigned int nInterval = nTargetTimespan / nTargetSpacing;
690
691     // Genesis block
692     if (pindexLast == NULL)
693         return bnProofOfWorkLimit.GetCompact();
```

Kódrészlet a Bitcoin 0.1-es verziójából

Hogy megbizonyosodjon az ötlet életképességéről, működőképességéről, Satoshi megírta a kódot, létrehozva a Bitcoin szoftverét, mielőtt nyilvánosságra hozta volna a white papert. Abban is biztos akart lenni, hogy a frissítéseket nem fogják folyton elhalasztani, hiszen „mindig van valami, amit még lehetne fejleszteni”.

„Meg kellett írnom a kódot, hogy meggyőzzem magamat, képes vagyok megoldani a felmerülő problémákat. Csak ezután írtam meg a white papert.”

Satoshi Nakamoto

A mai világ tele van ígéretekkel, amelyek nem, vagy alig valósulnak meg, így hatalmas az igény az elkötelezett alkotókra. Győzd meg magadat, hogy tényleg képes vagy kezelni a problémákat, és megoldásokat találni! Egy kicsit mindannyiunknak cypherpunknak kellene lennie.

A Bitcoin megtanította, hogy a cypherpunkok kódokat írnak.

***

A tükörben:

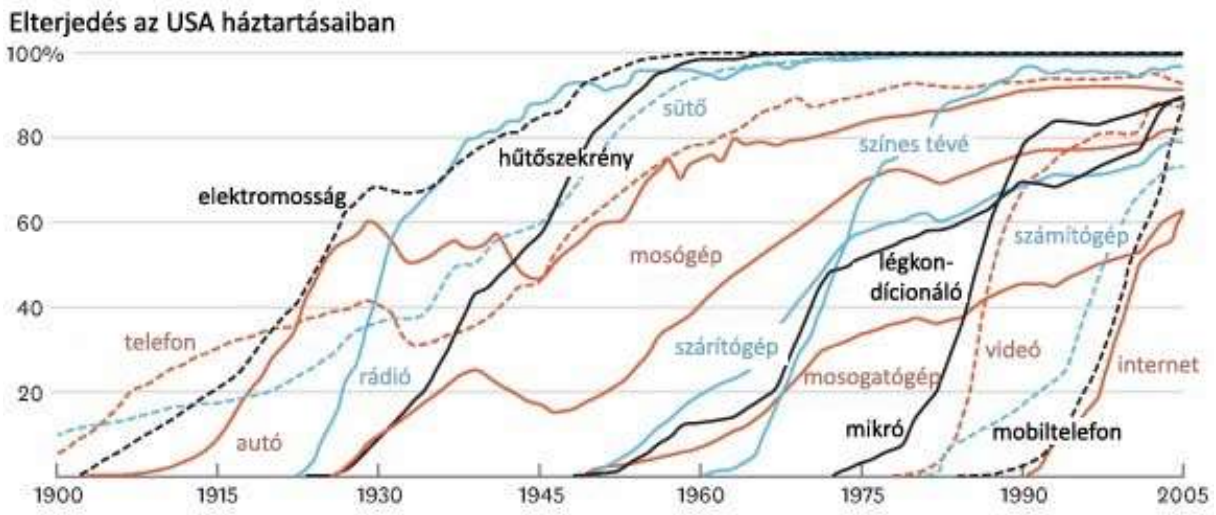
Bitcoin is an Idea

Huszonegyedik lecke: Metaforák a Bitcoin jövőjéről

Tudom, hogy valami érdekes biztosan történt itt…

Az elmúlt évtizedekben egyértelművé vált, hogy a technológiai fejlődés nem lineáris utat követ. Hogy hiszel-e a technológiai szingularitás elméletében vagy sem, attól függetlenül is látható, hogy számos területen exponenciális a növekedés. Ráadásul az elfogadási ütem is gyorsul, az iskolaudvar mögötti bringapálya már rég eltűnt, a gyerekeink generációja Snapchat-en tartja a kapcsolatot. Ez a növekedési görbe még azelőtt gyomron vágja az embert, hogy egyáltalán észrevennénk a közeledtét.

A Bitcoin pedig egy olyan exponenciális technológia, amelyet más exponenciális technológiákra építettek fel. Az Our World in Data grafikonjából jól látható, hogyan gyorsul az egyes technológiák elterjedési sebessége (az USA-ban), kezdve 1903-tól, az elektromosság bevezetésével. Elektromos áram, számítógépek, internet, okostelefon, mindegyik exponenciális trendet követ az elterjedésben és az árban is. A Bitcoinra ugyanez igaz.



Egyre meredekebb az emelkedés; a Bitcoin szó szerint rá sem fér a grafikonra.

A bitcoin ráadásul több szinten is hálózati hatás alatt áll, mindegyik hatalmas növekedést eredményez. Az árfolyam, a felhasználók száma, a biztonság, a fejlesztések, a piaci részesedés, és a világszintű elterjedés tekintetében mind növekedést mutat. Miután sikeresen túlélte a kezdeti éveket, a Bitcoin minden egyes nappal növekszik, mégpedig több területen is. Az is biztos, hogy még nem érte el a teljes kifejlődést a rendszer, talán egyfajta serdülőkorban lehet. De mivel a technológia exponenciális, az árnyékokból a rivaldafénybe vezető út nagyon rövid.

Mobiltelefon 1965-ből és 2019-ből

2003-ban Jeff Bezos a híres TED-talk előadásában az internet jövőjéhez az elektromosság terjedéséből vont párhuzamokat. Mindhárom dolog, az elektromosság, az internet, és a Bitcoin is, hálózati technológia. Olyan technológiák, amelyek lehetővé tesznek más technológiákat. Természetüknél fogva alapzatnak számítanak, infrastruktúrának, amelyre építeni lehet. Az elektromosság már köztünk van egy ideje, alapvetőnek tekintjük. Az internet sokkal fiatalabb, de a többség már most ugyanúgy alapdolognak gondolja, mint az áramot. A Bitcoin alig tíz éves, és a köztudatba csak néhány éve, a legutóbbi tőzsdei bikaciklusban került be. Csak a legkorábbi felhasználói tekintik alapvetőnek a létezését. Ahogy viszont telik az idő, egyre több és több ember fogja ugyanezt gondolni róla.

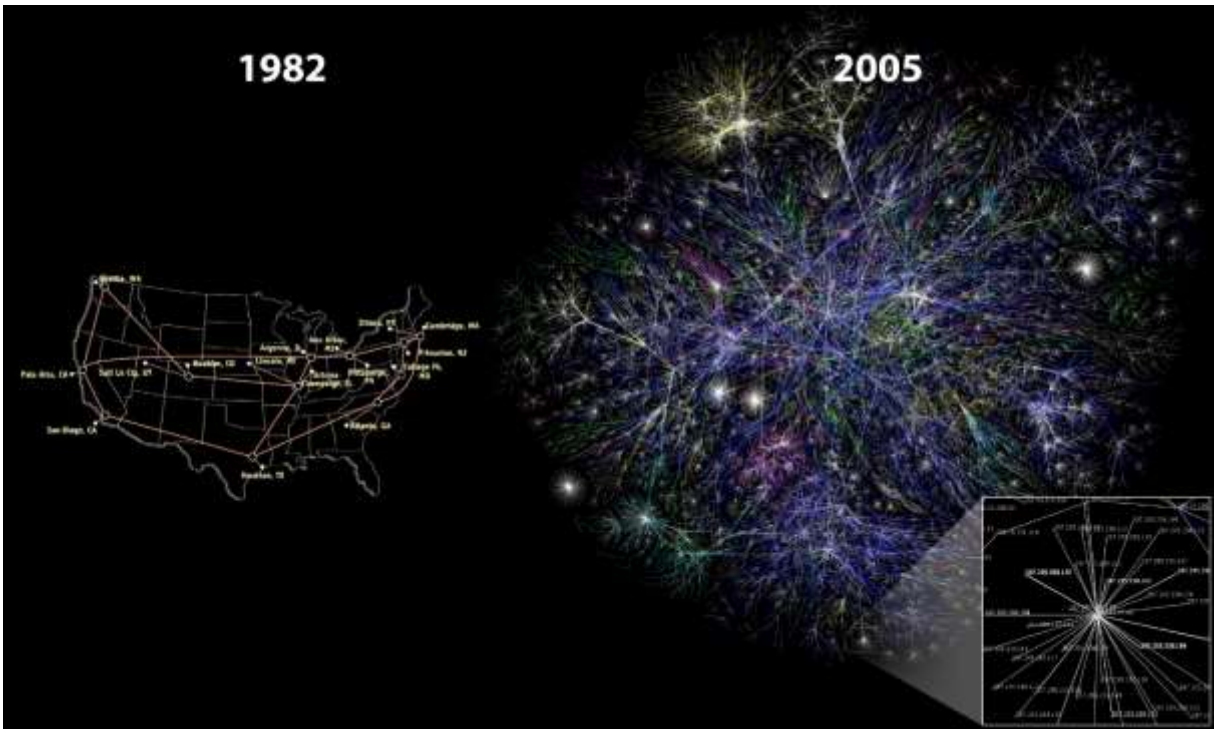
1994-ben az internet is kusza és bonyolult volt. Ha az ember megnéz egy-egy régi show-műsort, amelyben erről beszélgetnek, láthatjuk, hogy ami ma magától értetődőnek és természetesnek tűnik számunkra, egyáltalán nem számított mindig annak. A Bitcoin a többség számára ugyanilyen kusza és bonyolult most, de ahogyan a digitális bennszülöttek, az ezredforduló után születettek számára az internet egy második élettérré vált mára, úgy a jövő bitcoin-bennszülöttei számára is ugyanilyen természetes lesz, hogy satoshikat gyűjtenek, költenek, kezelnek.

„A jövő már itt van, csak nem egyenlően van elosztva.”

William Gibson

1995-ben nagyjából az amerikai felnőttek 15%-a használta az internetet. A Pew Research Center adataiból látszik, hogy azóta az internet hogyan szőtte be az emberek életének minden részét. A Kaspersky Lab fogyasztói felméréséből kiderül, hogy 2018-ban már az ügyfeleik 13%-a használta a bitcoin vagy valamelyik másolatát vásárlásra. A fizetőeszközként való használat nem a bitcoin kizárólagos felhasználási módja, de ha párhuzamot akarunk vonni, akkor most ott tartunk, ahol az internet járt a ’90-es évek közepe előtt.

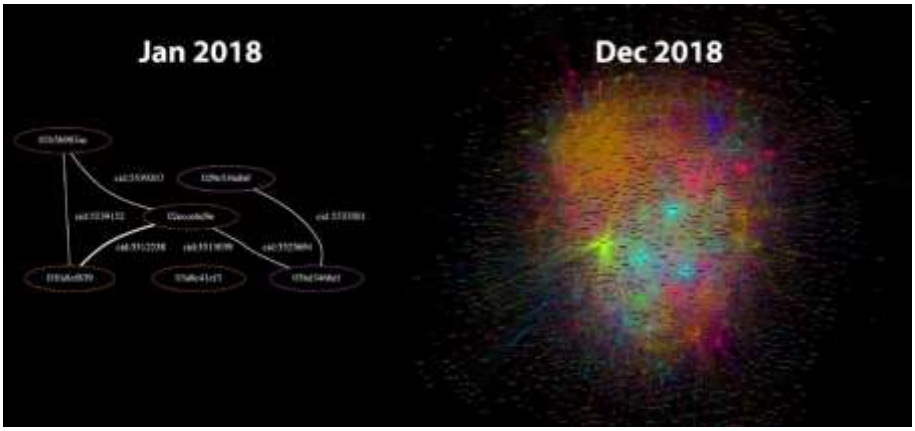
1997-ben Jeff Bezos úgy kezdte az egyik, a részvényeseinek írt levelét, hogy „ez az internet Első Napja”, felismerve a technológiában rejlő hatalmas, addig kiaknázatlan potenciált, és így a cége előtt álló lehetőségeket. Nem tudjuk, hogy a Bitcoin számára most melyik nap is van, de a hasonlóan gigantikus nagyságrendű potenciál mindenki számára egyértelmű.



Az internet két évtizede; Merit Network, Inc.; Barrett Lyon, Opte Project

Az első Bitcoin-csomópont 2009-ben indult el, mikor Satoshi kibányászta a genezis blokkot, és nyilvánossá tett a szoftvert. Nem sokáig volt egyedül. Hal Finney az elsők között csatlakozott hozzá azok közül, akik megértették az ötlet jelentőségét. Egy évtized múltán nagyjából 75 ezer csomópont működik a hálózaton, futtatva a Bitcoint.

Ráadásul nem a főlánc az egyetlen, amely ilyen mértékben erősödik. A Lightning Network, egy második rétegű protokoll még ennél is gyorsabb ütemben növekszi.
2018 januárjában a Lightning Network 40 csomóponttal és 60 csatornával rendelkezett. 2019 áprilisára ez 4000 csomópont és 40 ezer csatornára nőtt. A Lightning egy fejlesztés alatt álló, még nem teljesen kiforrott technológia, így néha veszteségek keletkeznek a használata során. A trend mégis egyértelmű, emberek ezrei vállalják a kockázatokat, és örömmel használják a rendszert.



A Lightning Network növekedése; Jameson Lopp

Én végigkísértem az internet rakétaszerű emelkedését, így számomra egyértelmű a párhuzam a web és a Bitcoin között. Mindkettő hálózat, mindkettő exponenciális technológia, mindkettő lehetővé teszi új dolgok megszületését, új iparágakét, új életmódokét. Ahogyan az elektromosság szolgáltatta a legjobb metaforát az internet jövőjének a megértéséhez az első időkben, az internet mutatja meg a legjobban, hogy mi vár a Bitcoinra. Ahogyan Andreas Antonopoulos is a könyve címének választotta, a Bitcoin „A pénz internete". Ezek a metaforák emlékeztethetnek minket, hogy bár a történelem nem ismétli magát, de gyakran összecseng a múlttal.

Az exponenciális technológiákat nehéz elsőre felfogni, és emiatt gyakran alábecsüljük azokat. Számomra kifejezetten érdekes ez a terület, és közelről követem az alakulását, de még engem is sokszor lenyűgöz az innováció, a fejlődés üteme. Nézni a Bitcoin növekedését olyan, mint amilyen az internet növekedése volt, csak felgyorsítva. Izgalmas.

Hogy megérthessem a Bitcoint, több különböző úton is el kellett indulnom, hogy megismerjem a történelmet. Része volt az utazásnak az, hogy megismerkedjek néhány ősi társadalommal, régóta nem használt pénzekkel, vagy éppen utánanézzek a kommunikációs hálózatok fejlődésének. A kőbaltától az okostelefonig jutva láthatjuk, hogy a technológiai fejlődés már számtalanszor átalakította a világunkat. A hálózati technológiák pedig még nagyobb hatásúak. Az írás, utak, elektromosság, internet. Mindegyik hatalmas változást hozott. Az én világomat a Bitcoin is megváltoztatta, és meg fogja azoknak a szívét-lelkét is, akik elég bátrak, hogy használni kezdjék.

A Bitcoin megtanította, hogy a múlt ismerete elengedhetetlen a jövő megértéséhez. A jövőhöz, amelyik pont most kezdődött el.

***

A tükörben:

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

Összegzés

Kezdd az elején, – mondta a király, komoly hangon, – *aztán folytasd, amíg a végére nem érsz. Akkor abbahagyhatod.*

Ahogyan rögtön a könyv elején említettem, a „Mit tanultál a Bitcointól?” kérdésre adott válaszok sosem lesznek teljesek és véglegesek. A szimbiózis, amelyet a Bitcoin, a technológiai infrastruktúra és a világgazdaság élő rendszerei között láthatunk, egyszerűen túlságosan is sokrétű. Az egész témakör szerteágazó, és sokkal gyorsabban fejlődik, hogy bárki lépést tudna tartani vele, és megérthetné.

A teljes megértés hiánya ellenére, és az összes rövidítésnek, kerülőútnak látszó megoldással együtt is tagadhatatlan, hogy a Bitcoin működik. Átlagosan tíz percenként létrehoz egy új blokkot, ebben pedig van valami gyönyörű. Ráadásul minél tovább működik, annál több embert vonz magához.

Tény, hogy a dolgok működésében gyönyörűség van. A művészet is egy funkció.

Giannina Braschi

A Bitcoin az interneten született. Exponenciálisan növekszik, elmosva a tudományterületek közötti határokat. Az sem egészen tiszta, mikor ér véget egy tisztán technológiai elem valósága, és vált át egy másik realitásba. Igaz, hogy a Bitcoinnak számítógépekre van szüksége, hogy működjön, de a számítástechnika ismerete nem elég, hogy megérthessük. A Bitcoin nem csak a működését tekintve nem ismer határokat, de az akadémiai tudományok határait is áthágja.

Közgazdaság, politika, játékelmélet, gazdaságtörténet, hálózatok, pénzügy, kriptográfia, információtechnológia, cenzúra, jog és törvény, polgári szerveződések, pszichológia, és egyéb területek mind érintettek, mind tanulmányozásra várnak, hogy a segítségükkel megérthessük, mi a Bitcoin, és hogyan működik.

Nem egyetlen önálló innováció miatt következett be a siker. Számos, korábban egymáshoz nem kapcsolódó darab állt össze, hogy a játékelmélet által biztosított anyagi ösztönzés hatására elindítsa azt a forradalmat, amelyet most Bitcoinként ismerünk. Ez a zökkenőmentes összefonódás az, amely miatt Satoshi valódi zseninek számít.

Mint minden komplex rendszer, a Bitcoin is áldozatokat hozott a hatékonyság, a költségek, a biztonság területén, néhány más tulajdonság mellett. Ahogyan nincs tökéletes módszer, amellyel négyzetet lehet faragni egy körből, a Bitcoin problémamegoldásai sem lesznek sosem tökéletesek.

„Nem hiszem, hogy valaha lesz még jó pénzünk, hacsak nem tudjuk kivenni a kormányzat kezéből az irányítását. Márpedig erőszakkal nem tudjuk kivenni, csak annyit tehetünk, hogy egy kerülőúton indulunk el, amelyet nem tudnak lezárni előttünk.”

Friedrich Hayek

A Bitcoin az a kerülőút, amely visszaadja a világnak a jó pénzt. Úgy teszi ezt meg, hogy minden egyes csomópont mögé egy valódi embert rak, ugyanúgy, ahogyan Da Vinci is egy embert rajzolt a kör közepébe, hogy szögletessé tudja tenni. A csomópontok feleslegessé teszik a központi irányítást, így egy elképesztően ellenálló rendszert hoznak létre, amelyet gyakorlatilag lehetetlen leállítani. A Bitcoin él, és valószínűleg túl is fog élni mindannyiunkat.

Remélem élvezted ezt a huszonegy leckét! Talán az a legfontosabb tanulság, hogy a Bitcoint a lehető legtöbb nézőpontból érdemes vizsgálni, főleg, ha tényleg az összképre, vagy legalábbis valami hasonlóra vagyunk kíváncsiak. A komplex rendszerek összeomlanak, ha kiveszünk belőlük egy darabot, a Bitcoin tanulmányozása sem ajánlott egyetlen irányból, nem lehetséges úgy megérteni. Ha csak egyetlen ember kezdi el blokklánc helyett „a blokkok láncolatának” nevezni, nekem már megérte ez az egész.

Az én utam mindenesetre nem ért még véget. Tervezem, hogy mélyebbre merülök ebben a nyúlüregben, ha van kedved, tarts velem!

Köszönetnyilvánítás

Köszönöm! – mondta Alice.

Meg akarom köszönni a számtalan szerzőnek, tartalomkészítőnek a munkáját, akik alakították a Bitcoin és a kapcsolódó témák esetében a gondolkodásomat. Túl sokan vannak, de igyekszem megtenni, amit tudok, hogy legalább néhányukat megnevezzem!

- Köszönöm Arjun Balajinak, hogy feltette nekem a kérdést, amely a leckék megírásához vezetett.
- Köszönöm Marty Bent végeérhetetlen információ-áradatát. Ha nem vagy feliratkozva a Tales from the Crypt sorozatra, gondold át! Matt és Marty bárkit hajlandó elkalauzolni a nyúl üregében.
- Köszönöm Michael Goldstein és Pierre Rochard munkáját, akik kezelik és fenntartják a Nakamoto Institute hatalmas tudásanyagát. Köszönet a Noded podcastért is, sokat tanultam a Bitcoin filozófiájáról a segítségével.
- Köszönet Peter McCormack őszinte tweetjeiért, és a What Bitcoin Did podcastért, amely mindig hasznos gondolatokkal gazdagít ezekről a szerteágazó területekről.
- Köszönöm Andreas Antonopoulos sok éves munkáját, amelyet az oktatóanyagok összeállítására fordított.
- Köszönöm Saifedean Ammous őszinte és nyers tweetjeit, és persze a Bitcoin Standard című könyvet.
- Köszönöm Francis Poulot bíztató szavait, amikor rátalált a timechain témájára.
- Köszönöm Jannik, Brandon, Matt, Camilo, Daniel, Michael és Raphael segítségét, a véleményezésüket, visszajelzéseiket a leckék vázlatairól. Janninknak külön köszönet, hogy több leckét is több alkalommal átnézett a kedvemért.
- Köszönöm, hogy Dhruv Bansal és Matt Odell időt szakítottak az ötleteimről való beszélgetésre.
- Köszönöm Guy Swann hangoskönyvét, amelyet a leckékből készített.

Köszönöm minden bitcoin maximalistának, shitcoin minimalistának, mindenkinek, hogy benépestik a Bitcoin Twitter gyönyőrű kertjét. Köszönöm neked is, kedves Olvasó, remélem, élvezted annyira az olvasást, mint én az írást!

Ha tetszett a könyv, vegyél belőle egyet, írj róla értékelést, vagy egyszerűen csak osszad meg a barátaiddal! Ha bármilyen ötleted, javaslatod van, a Twitteren megtalálsz, küldhetsz üzenetet!