(2024.01.05 változat)

Bitcoin: "magyarul", magyaroknak (1. rész)

(c) minden jog fenntartva!

Tartalom

Jogi “elő-előszó”.....3

Előszó.....4

Első fejezet: A csereeszközök történelme.....8

A “primitív” csereeszközök.....8

A fémpénzek feltalálása.....12

A papírpénzek feltalálása.....14

Az Aranystandard története.....18

Az ezüst demonetizálása.....23

A jólét és virágzás kora.....26

Az Aranystandard eltörlése.....28

A FIAT pénz térnyerése.....30

Második fejezet: A FIAT utáni alternatív lehetőségek.....36

Visszatérés az Aranystandardra.....36

“Becsszó”, nem fogunk nyomtatni.....37

Harmadik fejezet: A Bitcoin felépítése.....40

A szabályok felszabadítanak.....42

A szereplők.....46

A Blokklánc.....49

A nehézségi szint állítás.....53

Az 51%-os támadás.....56

A Bitcoin decentralizáltsága.....59

A tárcák és kulcsok szerepe....64
A Bitcoin gazdasági ösztönzői....67
Az abszolút hiány....69
A Bitcoin volatilitása....72
A Bitcoin bukásának útja....74
A Bitcoin energiaéhsége....78
A Bitcoin “rétegei”, jövőbeli skálázhatósága....84
A Bitcoin csalói....91
A Bitcoin jövője....92

Negyedik fejezet: A Bitcoin használata....95
Az “5%-os szabályom”....95
A Bitcoin tárcák....96
A speciális szavak (“seed”) védelme....102

Utolsó fejezet: Gondolatok....106
Beszéljünk a “hogyan továbbról”....106
Michael Saylor-“féle” megtakarítási modell....109
A BlackRock-“féle” befektetési modell....110
Arany vs. Bitcoin....111
Fúj, kapitalizmus!....117
A Bitcoin és a CBDC-k....124
Nincs “új/jobb” Bitcoin!....126
A Bitcoin Nyert!....128

Utószó....136
Who the “F…” is Alice, azaz ki vagyok Én? :)....136

Források....138

Jogi “elő-előszó”

Mielőtt bárki azt gondolja, hogy ez a könyv bármiféle befektetésre próbálna rávenni, mindenképpen szeretném kiemelni, hogy ez nagyon nem így van! Én ezt a könyvet pusztán tájékoztatás céljából írtam, hogy a Bitcoinról kialakult saját gondolkodásmódomat, gondolataimat bemutassam.

Nem szeretnék senkit semmi olyan cselekedetre biztatni, amihez esetlegesen pénzügyi tanácsadói- vagy egyéb engedélyre lenne szükség, amivel nem rendelkezem.

Most hogy ezt tisztáztuk, jöjjön az “igazi” előszó. :)

Előszó

Azt terveztem, hogy először magamról írok, hogy az olvasó megismerje a témában szerzett kompetenciámat, de szerintem ez teljesen sokadlagos. Akit ez érdekel az lapozzon az utolsó fejezethez, aki pedig a tudás megszerzéséért jött, az egyből belevághat a tanulásba.

Először is beszéljünk a miértekről. Miért gondoltam, hogy ezt a könyvet fontos megírnom?

A Bitcoin pénzügyi rendszer megértéséhez nagyon sok idegen nyelvű szakirodalom van, magyarul viszont sajnos csak nagyon kevés.
Úgy gondolom, hogy az itt leírt “alapigazságok” segíthetnek az embereknek megérteni, hogy miért van a Bitcoin létezésére szükség (1); a lakosság miért van olyan-amilyen helyzetben (2); a mindenkori vezetés és kiszolgáló személyzete (pl. a mainstream média), miért nem fog (szerintem) soha igazán segíteni (3).

Szeretném nyomatékosan kiemelni, hogy ez nem egy általánosságban minden részletre kiterjedő könyv! Arra már létezik az egyik kedvenc írom Saifedean Ammous: The Bitcoin Standard című könyve, ami rendkívüli részletességgel mutatja be a Bitcoin (BTC), valamint a történelmi- és napjaink pénzügyi rendszerének működését.

Már a kezdetekkor elhatároztam, hogy olyan könyvet szeretnék írni, amit a lehető legtöbben hajlandóak elolvasni, ezért elsődlegesen relatív rövid és kizárólag azt a mennyiségű információt tartalmazza, amit úgy gondolom, hogy a Bitcoinról (plusz a hozzá kapcsolódó

pénzek történetéről és a közgazdaságtanról) egy laikusnak tudnia érdemes. Ebből kifolyólag a Bitcoin technikai mélységeibe csak alap szinten fogok belemenni. Miért? Mert úgy gondolom, hogy a túl sok információ között elveszik a lényeg. Lesznek bizonyos technikai részletek, amiket tényszerűen írok majd le és nem fejtem ki a miértjeit, csak azt részletezem, ami a Bitcoin működésének megértéséhez elengedhetetlen.

Ahhoz, hogy ez a könyv könnyen érthető legyen, igyekeztem egyszerű nyelvezettel írni (pl. villamosenergia helyett “áram” kifejezést használok) és úgy egyedivé tenni, hogy a Bitcoin működését (minden előnyével és hátrányával) nem csak a saját szemszögemből írom le, hanem próbálom olyan megvilágításból is prezentálni, hogy azok is megértsék és magukévá tegyék, akiknek igazán szükségük lenne rá.

Kik azok, akiknek úgy gondolom nagyon szükségük van a Bitcoin működésének megértésére?

Azok, akik egyik hónapról a másikra élnek, akiknek nincs jövőképük, akiknek álom csupán egy saját lakás, akik a mindenkori kormánynak totálisan ki vannak szolgáltatva, tehát mondhatni a lakosság nagy részéről beszélek. Célom továbbra is az egyszerű fogalmazás, hogy az itt leírtak megértéséhez előzetes ismeretekre ne legyen szükség.

Az igazán fontos kérdés, hogy Te, mint olvasó egyáltalán a Bitcoinnal miért foglalkozz?

Véleményem szerint, egy olyan lehetséges jövőt tud rövid, illetve hosszú távon biztosítani, amivel anyagi és egyben gondolkodásbeli szabadságot is el tudsz érni.

Az utóbbi nem megy az előbbi nélkül. Itt, mire gondolok? Ameddig egy áruházba bemész és azzal foglalkozol hogy, mennyibe kerül a legolcsóbb kenyér, kifli, sör, bor, tej, párizsi és csak fizetéskor engedheted meg magadnak, hogy némi “különlegességet” vásárolj, mint fagyasztott pizza, némi karaj, de álmodni sem mersz a sajtos pultról, a steakről, a drága borokról, a drága sörökről és ezek ízéről, mert nem is emlékszel mikor ettél, ittál ilyet, na addig (!) esélytelen, hogy a sokkal komplexebb dolgokról tudj dönteni, mint pl. kire szavazzál? Egyáltalán mi értelme a szavazásnak? Melyik orvost válaszd? Milyen gyógyszert merjél bevenni? Ki az, akinek hihetsz? Ki mivel akar hosszú távon tönkretenni? Konkrétan neked mi a jó választás?
Ilyen és ezekhez hasonló holisztikus gondolkodást igénylő kérdésekkel, a mesterségesen “elnyomott” ember, képtelen foglalkozni. A választásod arra fog esni, amit többet hallasz, látsz. Ezt ne vedd sértésnek, de sajnos a történelem a média által több ízben bizonyította, hogy ez az állítás 100%-ig igaz. Most már gondolom érted miért van annyi plakát, internet-, tv- és rádió reklám. Igen, azért, hogy minden információ a tudatalattidba beépüljön, ezáltal droidként döntsél.

Nincs csoda, ha elolvasod ezt a könyvet, nem lesz az életed “csettintésre” jobb. Sőt a “meló” csak ezután jön, mert az a gondolkodás és értékrend, ami generációkon keresztül lett beléd programozva, nem fog egykönnyen megváltozni.

Ebben a könyvben nagyon sok dogmát fogok megkérdőjelezni, amit valakinek könnyű lesz elfogadni és ami valakinek nagyon, de nagyon nehezen fog menni. Az egyetlen kérdés, amit mindig tegyél fel magadnak:”Elgondolkodom-e azon amit itt olvasok, vagy visszatérek abba a megszokott világba és gondolkodásmódba, amiben eddig éltem?”

A döntést neked kell meghozni, de egy dolgot garantálok: Ezt a könyvet nem a haszonszerzés céljából csináltam és igyekeztem a legjobb tudásom szerint megírni. Nem vagyok tévedhetetlen, és mivel nincs mögöttem egy team, aki minden állítást mai divatos szóval “fact checking-el”, így a tévedés jogát fenntartom. Mit jelent ez? Azt hogy ugyan1-1 adatot elgépelhetek, téves forrást használhatok (bár igyekszem ezt ellenőrizni), addig ez az egész a Bitcoinnal kapcsolatos összképen SEMMIT sem fog változtatni. Tehát a fejezetek irányvonala és végső konklúziója bizonyosan állíthatom, hogy a valóságot fogja tükrözni!

A végső döntésed, hogy végül Bitcoin-t vásárolsz vagy sem, az én szempontból teljesen mindegy, mert bizonyosan állítom az árfolyamot nem fogod befolyásolni.
A Bitcoin jelenleg durván 500 milliárd USA dollárt ér, ami a mi nyelvünkre lefordítva kb. 175.000 milliárd forint. Bármennyit is veszel nem fogod az árfolyamot számomra pozitív irányba befolyásolni még akkor sem, ha te vagy a mi gázszerelőnk (*ha te vagy akkor remélem az itt leírt információkért dobsz egy kis “alamizsnát”) :)*.
Ezt tartsd szem előtt, ha esetleg arra gondolnál, hogy az a titkos tervem, hogy tömegeket próbáljak a Bitcoin vásárlására rávenni.

Írhatnám, hogy jó szórakozást kívánok, de valószínűleg ha az itt leírtakkal először fogsz találkozni, akkor nem fogsz szórakozni, így inkább kitartást kívánok!

Első fejezet:
A csereeszközök történelme

A “primitív” csereeszközök

Na nem kell megijedni, nem kezdek bele Ádám és Évától évszámokkal bombázni téged, igazából az itt leírtak csak arról fognak egy képet adni, hogy az emberek a különböző történelmi korszakokban a pénzről, mint csereeszközről hogyan gondolkodtak.

Két lényeges korszakot fogok kiemelni és részleteiben bemutatni: Az emberiség történelmében voltak olyan időszakok (*ebből volt több*), amikor az emberek ugyanolyan gondokkal küszködtek, mint te és volt olyan időszak is, amikor az emberiség minden szempontból (társadalmi és gazdasági) a virágkorát élte.

A barter, mint fogalomról mindenki hallott. A történelem ezt nevezi a legkorábbi kereskedési módszernek, amikor is az áruk egymás között bizonyos váltószám fejében cseréltek gazdát. Ez egy kis közösségben ideális lehet, hisz én mondjuk búzát termelek, te pedig teheneket tartasz, így az általad adott 1 kg húsért mondjuk 12 kg búzát adok. A probléma ott van, ha ezt értékesebb és több termékekre akarjuk kiterjeszteni.
Nem sok embert tudok, aki mondjuk egy házért elfogadna búzát és márpedig ha én csak búzát termesztek, akkor bajosan fogok tudni belőle házat venni. (Arról ne is beszéljünk, hogy romlandó árut elképesztő nehéz a kívánt mennyiségben felhalmozni.)

Mivel az emberek mindig is leleményesek voltak igyekeztek a barter hátrányos oldala miatt egy jobb alternatívát találni.

Itt mindenképpen megemlíteném, hogy azt hogy mi a “jó” csereeszköz, azt soha senkinek nem kellett megmondania, hanem az emberek saját és mások tapasztalatai alapján erre mindig maguktól rájöttek. Persze, persze voltak államilag rájuk erőszakolt csereeszközök (*pénzek*), de azok idővel mindig elbuktak, viszont a “jó csereeszközök” mindig organikusan fejlődtek ki.

Nézzünk a történelemből egy-két példát. Itt van egyből az egyik leghíresebb ősi csereeszköz, a só.

Miért pont a só? Miért volt a só optimálisabb választás, mint mondjuk az általános barter?

Először is szükséges volt egy olyan köztes médiumot találni, ami azok számára jelent megoldást, akik mondjuk romlandó árut termeltek. Szükséges volt, hogy ne csak könnyen lehessen tárolni, de könnyen kis részekre is fel lehessen osztani. Fontos volt, hogy széles körben elfogadják, de a legfontosabb az értékállósága volt, mert ha elkezdem felhalmozni, esetlegesen évekig gyűjteni, jó lenne ha az értéke nem ingadozna.
Akkoriban a só mindezekre megoldásként szolgált, mert nem romlott meg, apró szemcséinek köszönhetően könnyen tárolható (zsák) és könnyen osztható volt. A viszonylag kevés bányászata miatt, jó értéke volt és mivel az élet alapvető működéséhez elengedhetetlen, magas kereslettel bírt.

Érdekesség, hogy a római katonák a sót sokszor az állami fizetőeszköznél is értékesebbnek tartották, és ezért a havi zsoldjukat sóban kérték. Innen van a "salarium" (fizetség) latin kifejezés, ami a "sal"-ból (latinul só) ered. Több nyelv is átvette: pl. Francia "salaire" vagy az angol "salary".

Ahogy az emberiség jobb alternatívát talált, úgy váltott egyik csereeszközről a másikra. Mégis mik ezek a tudat alatt dolgozó feltételek, amiknek a pénzeknek meg kellett felelniük?

Fentebb már elárultam, de összeszedem őket, mert a jövőben ez alapján tudunk majd egyik vagy másik csereeszköz között különbséget tenni.

1. Eladhatóság: Nagyon fontos, hogy az a csereeszköz, amit birtoklunk kellő mértékben kelendő legyen, tehát az emberek "vágyjanak rá". A só példájánál maradva ez megvolt, mert az alapvető életműködéshez elengedhetetlen és emellett az ételek ízét, eltarthatóságát is drámaian javítja.
2. Oszthatóság: Az adott csereeszközzel képesek kell legyünk pl. egy házat kifizetni, de akár egy kávét is. Ehhez az kell, hogy csoportosítani és kellően kis mennyiségre is fel lehessen bontani, ami a sónál triviális.
3. Szállíthatóság: Az adott csereeszköz viszonylag könnyen szállítható legyen és nem szabad, hogy a szállítás folyamán az egyéb tulajdonságai sérüljenek. A só tömb és por formájában is viszonylag könnyen szállítható.
4. Értékállóság: A legfontosabb tulajdonsága egy csereeszköznek, hogy a benne tárolt érték a lehető legkevesebbet csökkenjen és ha lehetséges, akkor inkább növekedjen. A só, ameddig nem

fedeztek fel újabb bányákat és előállítási módokat (pl. lepárlás), addig az értékét viszonylag jól megtartotta.

Összefoglalva a lényeget Carl Menger (az Osztrák közgazdaságtani iskola atyja) fogalmazta meg: “Egy pénz elterjedése, csak az eladhatóságán múlik!”

A fenti kritériumokat egy átlagos ember sose gondolta így végig, hanem a folyamat - ahogy említettem - tudat alatt történt. Bármely kritérium “elbukása” vagy esetlegesen egy másik csereeszköz általi felülmúlása azt jelentette, hogy az adott tárgy feladatát, mint csereeszköz képtelen tovább ellátni és lassan vagy gyorsan a “süllyesztőben” eltűnik, azaz csúnya szóval demonetizálódik.

A só példájánál maradva, mi volt az, ami miatt a bukása borítékolható volt?

Azzal, hogy új sóbányákat és új előállítási módokat fedeztek fel, a só elvesztette magas értékét elveszítve ezzel értékállóságát is. Ezek után nagyon sokan, akik sóban hatalmas értékeket halmoztak fel, a só árának jelentős csökkenésével a vagyonuk nagy részének elvesztésével szembesültek, és a továbbiakban a világ lakossága a sót csak, mint fűszert és tartósítószert használta és használja.
A jó hír viszont, hogy ennek a demonetizálódásnak következményeként a só használatát a hétköznapokban egyre többen, egyre nagyobb mennyiségben engedhették meg. Ezáltal a tömegek nem csak az ételek ízvilágát tudták drámaian javítani, de a szervezetük sóháztartását, azaz az egészségüket is.

Milyen egyéb “primitív” csereeszközök voltak? A són kívül még volt: a jószág, üveggyöngyök, bőr, speciális kövek stb. Mindegyik idővel

elbukott, ahogy valamelyiknél jobbat találtak vagy (és ez volt a legvalószínűbb) a túltermelése miatt elvesztette értékét, és ezért rövid úton leváltották.

Önállóan mindegyik - a fémpénzekhez képest - viszonylag rövid életű volt.

A fémpénzek feltalálása

Nem kell nagyon okosnak lenni ahhoz, hogy rájöjjünk: a primitív csereeszközökkel egy tartósan mindig jelenlévő probléma miatt muszáj volt valami merőben új alternatívát keresni. Ez a probléma nem más, mint a primitív csereeszözök “értéksűrűsége”, azaz nem voltak elég kicsik/könnyűek, ami viszont elég kicsi/könnyű volt, az nem volt elég értékes.

A só, mint mondtam ugyan kicsi, de csereeszköz értékét az új előállítási/bányászási lehetőségekkel gyorsan elvesztette (nem érdemes olyasmiben tartani a vagyont, ami idővel kevesebbet ér). A jószág értékes, de relatíve nagy és könnyen nem szállítható/skálázható. Ugyanígy járt az összes többi primitív eszköz, ezért a kínaiak kb. időszámításunk előtt 500 évvel új csereeszköznek elkezdtek fémpénzeket verni.

Az első ilyen kínai fémpénzek valójában ezüstlapok voltak, de a világ különböző pontjain relatíve gyorsan kerek alakú (szokványos) fém érmék terjedtek el. Ezek nem csak ezüstből, hanem vasból, bronzból és aranyból készültek. A vas és bronz érméket leginkább a kis értékű kereskedelemben használták, az ezüst-, illetve az arany érméket pedig a nagy értékű ügyletekben.

Itt álljunk is meg egy pillanatra. Mi adja az érméknek az értékét? Az hogy “mekkora szám” lett ráírva? Nem. Az értéküket a különböző fémek ritkasága és tartóssága adta.
Az előbbi megértéséhez egy közgazdaságtani fogalmat kell elmagyaráznom, amit a későbbiekben nagyon sokszor fogok emlegetni. Ez a fogalom pedig a *készlet-folyósítási arány* (angolul: stock-to-flow ratio).

Készlet-folyósítási arány: *A készlet-folyósítási arány egy olyan arányszám, melyet egy jelenleg forgalomban lévő erőforrás/áru mennyiségét, az adott erőforrás/áru évente előállított mennyiségével osztva kapunk.*

Magyarul:
Példa 1. A kőolaj. Általában a Földből az emberiség egy évben annyi kőolajat termel ki, amennyit abban az adott évben fel is használ (kicsivel többet). Tehát a készlet-folyósítási arány kb. 1 (kicsivel több).
Példa 2. Az ezüst. A Földön az olajnál már jóval több ezüst marad “készleten” (pl. ékszeripar) és ehhez képest arányaiban jóval kevesebbet is termelünk ki, így az ezüst készlet-folyósítási aránya kb. 22.
Példa 3. Az arany. Az emberiség történelme során kitermelt összes arany megtalálható, mivel viszonylag jó a korrózióállósága és a Földben relatíve ritka, így az arany készlet-folyósítási aránya kb. 70.

A készlet-folyósítási arány mértékének növekvő sorrendje adta a fémpénzek valódi értékét.

Mivel ezek közül a legkissebb arány számmal a vas rendelkezett, azaz a legkönnyebben bányászható és előállítható fémpénz volt, így ezzel oldották meg a kis értékű ügyleteket.
A legmagasabb arány számmal az arany rendelkezett, ezért a nagy értékű ügyletekhez ezt használták.
Ez az arányszám ezekbe a pénzekbe soha nem volt “belekódolva”, az értéküket pusztán az előállításuk költségéből és körülményességéből fakadó ritkaságuk adta.
Az aranypénzre bármennyire is sokan vágytak az egész birodalomban véges számú aranypénzt tudtak veretni, és ezért a kereslet mindig jóval nagyobb volt, mint a mindenkori készlet.

Ez a fémpénz rendszer évszázadokig tökéletesen tudott működni, mert mindegyik pénznek a piacon lévő mennyiségét (készlet), az érme fém tartalmának földben található mennyisége és kibányászásának költségei szabályozta, ezzel stabilizálva a piaci értékét.

A papírpénzek feltalálása

A papírpénz fogalmát időszámításunk után kb. 800 évvel a kínaiak találták fel és kb. 500 éven keresztül használták is. A működése egyszerű volt, mert eredetileg a kinyomtatott pénzeknek a fedezetét a kincstárban lévő arany mennyisége adta. Ezt kezdetben természetesen oda-vissza lehetett ezüstre és aranyra váltani.

Vizsgáljuk meg a papírpénz előnyeit és hátrányait.

Előnyei:

- bármilyen mennyiségben skálázható (kis és nagy címletek),

- sokkal könnyebben szállítható.

Hátrányai:
- a fémek hiányában sokkal könnyebben előállítható,
- nincs természetes korlát (nem kell hozzá fémet kibányászni).

Itt jön a legfontosabb dilemma, amit én úgy nevezek a “Kecskére káposztát?” kérdéskör.
A mindenkori uralkodók számára csábító volt a papírpénzek könnyű központi előállítása, hogy a mögöttük lévő fedezetet meghaladva, jóval több mennyiséget nyomtassanak. Ennek az alternatívája a megnövelt adóztatás, ami ellen az emberek fellázadnak.
Az amerikai erre azt mondaná: “it’s a no-brainer”, azaz nem kérdés, hogy előbb utóbb melyiket fogják választani.

Ezen a ponton újabb fogalommal kell megismerkednünk: *infláció*.

Infláció: Az infláció avagy pénzromlás (hibás kifejezéssel) - a közgazdaságtanban hívták még pénzpuffasztásnak vagy pénzpuffadásnak is -, amely az árszínvonal tartós emelkedése, a pénz vásárlóerejének romlása mellett.

Magyarul: Amikor a mindenkori uralkodó több papírpénzt hoz forgalomba (később igaz ez a digitális változatokra is), mint ami mögött fedezet van, akkor ez inflációt fog okozni.

Ahhoz hogy megértsük hogyan okoz inflációt, egy új fogalmat kell megismernünk, a *Cantillon-effektus*-ét.

Cantillon-effektus: A Cantillon-effektus a monetáris politikák gazdaságra gyakorolt egyenetlen hatását írja le. Vagyis, ha egy központi bank több pénzt juttat a gazdaságba, az ebből eredő áremelkedés nem egységesen következik be.
Azok, akik az újonnan létrehozott pénzt elsők között kapják, változatlan vásárlóerőre tesznek szert és fogyasztási cikkeket vagy beruházási javakat viszonylag alacsonyabb áron vásárolhatnak. Minden további személy, azaz az átlagos fogyasztók később-, csak részlegesen- vagy egyáltalán nem részesülnek ezekből az előnyökből (inkább a hátrányokból, azaz az áremelkedésből). Ennek eredményeként a vagyon- és jövedelemszakadék mélyülhet, és az infláció hatásai az egész társadalomban nem egyenletesen oszlanak meg. Ezért a pénzkínálat bővülése soha nem semleges.

Magyarul:
Példa 1. Én mint bank, a semmiből létrehozok 1 millió forintot és azt hitel formájában Józsinak odaadom. Józsi ezzel az 1 millió forinttal elmegy vásárolni és még úgy tud vásárolni mondjuk 100 kiflit, hogy megkapja darabját az aznapi 100 Ft-os áron. Tegyük fel hogy ezt minden nap meg akarja tenni. Az eladó azt látja, hogy addig naponta 100 darab kiflit adott el, de most hirtelen 200 darabot ad el. Azt gondolja, hogy az áron most 20%-ot emel és még ha az eladásainak száma valamennyit esik is, még mindig a kevesebb eladott (egyben legyártott) kiflivel bőven jól fog járni. Másnap Mari néni, aki pedig a nyugdíjából él, bemegy a boltba és csak azt látja hogy a minden nap megvett kifli már nem 100 Ft, hanem 120 Ft-ba kerül.

Példa 2. Van egy X mennyiséget előállító téglagyár. Tételezzük fel, hogy a gyár a gyártási kapacitásának maximumán dolgozik, hisz minden évben közel azonos mennyiségű téglát ad el. Megjelenik az

imént említett Józsi, aki a frissen kapott pénzéből építkezni is kezd és elkezd téglákat is vásárolni. Neki sikerül az aktuális 1000 Ft /tégla áron vásárolnia. Kiderül viszont, hogy nem csak Józsi kapott 1 millió forint hitelt, hanem még 100 ember és mind építkezni kezdene, amihez mindenki a téglát, az imént említett gyárból szerezné be. A téglagyár vezetője az év első negyedévének végén észreveszi, hogy valami nem okés, mert már a szokásos mennyiség kétszeresét is eladta és folyamatosan érkeznek új vevők. Rájön, hogy 1-2 hónap alatt az egész évi kapacitását eladja. Ekkor ő is úgy gondolkodik, mint a pék az előző példából és inkább emel 30-40%-ot az áron kockáztatva ezzel, hogy kevesebbet fog eladni, de az áremelés kompenzálni fogja a különbséget. Ezután jön Pisti és Gizi, akik egy házra évek óta spórolnak és odáig eljuttottak, hogy nagy nehezen a telket már megvették, de a hitelből már nem tudják a házhoz szükséges téglát megvenni, mert ők már a 30-40%-os áremeléssel találkoznak.

Az előző két példa nagyon sarkított és végleteket vázol, de azt szerettem volna szemléltetni, hogy mindig az, aki először kap a frissen előállított pénzből tudja a vásárlóerejét maximálisan kihasználni és aki utána következik, az a várható áremelkedés miatt már kevesebbet tud vásárolni. Ezek az áremelkedések sose kiszámíthatóan és lineárisan következnek be, mert mindegyik hat a másikra (pl. a pék több pénzt keres, ezért ő is építkezni kezd…). Az abszolút vesztes mindig az, aki (nem valós inflációkövető) bérből él, illetve nyugdíjas.

Kínában a cantillon-effektus által okozott egyenetlen infláció, engedetlenséghez vezetett, aminek hatására a 15. században a

papírpénz évszázadokra eltűnt és a helyét ismét a fémpénzek vették át.

Európában a 17. század közepén, a gazdag bankárok a papírpénz fogalmát, újragondolták. Olyan papírpénzt bocsátottak ki, ami mögött (kezdetben) bizonyíthatóan aranyfedezet volt. Itt nagy neves bankárokról beszélünk (pl. Medici) és így az emberek megbíztak bennük, tehát az aranyaikat ilyen bankokban papírpénzre váltották. Ezek nem a klasszikus ma ismert bankjegyek voltak, hanem egyfajta elismervények, amikben abban az időben annyira bíztak, mintha a kezükben magát az aranyat tartották volna. (A 19. század elején ezekre a bankjegyekre angolul azt mondták:”as good as gold”, vagyis“olyan jó, mint az arany”.)

Az Aranystandard története

Anglia volt az első, amely 1717-ben Isaac Newton fizikus (a királyi pénzverde őrzője) irányítása alatt a modern aranystandardot (aranyalap) elfogadta. Ez azt jelentette, hogy minden bankjegy bizonyos súlyú tiszta aranyat képviselt.
A napóleoni háborúk kivételével (1797-1821) Anglia egészen 1914-ig bankjegyeit az aranystandard alapján bocsátotta ki. Anglia a közel kétszáz év alatt hatalmas birodalmat épített és az egész világ kereskedelmének előmozdítója volt. Példáját később több más európai ország is követte.

Ahhoz, hogy megértsük az aranystandard szerepét Angliában és később több más ország történelmében - miért volt olyan nagy sikere - pár alapvető összefüggést kell megértenünk.

Ameddig Anglia az aranyat kvázi bankjegyre váltotta, addig más országok többféle fémpénzt használtak, vagy ami még rosszabb, csak a kormány által “garantált” bankjegyeket bocsátottak ki. Az utóbbi problémái egyértelműek, hisz már a 15. században a kínaiak megtapasztalták milyen az, ha egy pénz értékét valós, relatív ritka fedezet nélkül csak a kormány szava szavatolja.

Nézzük csak milyen gondokat okoz, ha mint elszámolási egység többféle érmét használunk:

- Minél több elszámolási egységet használunk (vas-, bronz-, réz-, ezüst-, aranypénz), annyi különböző árat kell minden terméknél feltüntetni, ezzel extrém nehézzé téve a gazdasági számítások végzését.
- A nem értékálló pénzek masszív veszteségeket okoznak.
- A váltások általában költségekkel járnak.

Ezzel szemben Anglia azáltal, hogy a bankjegyei az aranystandard alapján voltak kibocsátva milyen előnyökhöz jutott:

- Hatalmas piaci kereslet volt iránta, mert a bankjegye a világkereskedelemben elfogadott fizetőeszköz volt, és mivel megbízhatóan arany fedezet volt mögötte nem kellett a súlyos aranyat és egyéb fémeket cipelni, elég volt csak ezen bankjegyeket.
- Azzal hogy kizárólag egy elszámolási egységet használtak lehetséges volt komplex gazdasági számításokat végezni, ezáltal alkalmas volt a *tőke* felhalmozására is. (Itt megállunk egy pillanatra, beszéljük csak át, mi is a *tőke*?)

Mi a különbség a pénz és a tőke között? A pénz nem egyenlő a tőkével, mert a tőke hozamot termel, a pénz pedig nem. A tőke kockázatos, a pénzben minimális a kockázat. A tőkének a mozgatása költséges, a pénznek a mozgatása minimális költségekkel jár.

- Az arany által biztosított fedezet arra adott lehetőséget, hogy az árak ne nagyon “ugráljanak”, tehát különböző termékek ritkaságát egymáshoz képest is pontos árakkal lehetett mérni.

A fentiek miatt, ahogy Anglia gazdasága növekedett, úgy a kereskedésre és a specializálódásra annál nagyobb lehetőségek nyíltak. A kiszámítható bevételek és kiadások miatt a gyártás hosszabb és szofisztikáltabb struktúrákat vehetett fel.
Lehetőség nyílt kizárólag olyan végfelhasználóknak szánt termékek előállítására, amik nagyobb időintervallumban készülnek, ezzel is magasabb gyártási minőséget állítva elő!

Magyarul:
Példa: Halászat. Az értékálló pénzzel a lakosoknak lehetőségük volt arra, hogy a kézzel való horgászatot az egyre jobb minőségű hajókra való “spórolással” leváltsák, ezzel egyre nagyobb termelékenységi átlagot létrehozva.

Ahhoz, hogy a “spórolást” és az ilyen jövőbeli tervezést, mint üzleti “ösztön” kialakulását megértsük, értenünk kell az emberi döntéshozatalt, az emberi *időpreferencia* működését.

Az egyén időpreferenciája: Alapja egy értékálló eszköz (pl. aranystandard alapú pénz), mert ettől függ, hogy az egyén a jelent, a jövővel szemben hogyan értékeli. Ez lesz az ő időérzéke.

Amennyiben az alapja egy nem értékálló eszköz (pl. fedezet nélküli bankjegy, vaspénz, só, stb.), akkor az egyén időpreferenciája magas lesz. Ez azt jelenti, hogy a jelent a jövővel szemben fontosabbnak értékeli, mert a pénzromlás hatásait tudat alatt érzi és így szeretné a pénzét, minél hamarabb elkölteni.
Amennyiben az alapja egy értékálló eszköz (pl. aranypénz), úgy az egyén időpreferenciája alacsony lesz, tehát egy jövőben vélt magasabb haszon érdekében, hajlandó a jelen vágyainak kielégüléseit elnapolni.

Magyarul: Az ember időpreferenciája mindig pozitív, mert sajnos nem élünk örökké, ezért a jelen fogyasztását mindig többre értékeljük, mint a jövőbelit. Pl. ha (most) nem eszünk, akkor a jövő soha nem érkezik el, mert meghalunk. Ahhoz hogy az egyén bárminemű fogyasztást a jelenben hajlandó legyen elnapolni, mindenképpen valami pozitív jutalomban kell érte részesüljön.

Ez az időpreferencia változás pozitív vagy negatív irányba tudat alatt történik. Ahhoz, hogy tudatosan “spórolni” kezdj az kell, hogy tudat alatt tudd, hogy az amibe a kicsi vagyonodat teszed, az az adott eszköz értékálló, magyarul idővel a vásárlóértékéből vagy nem veszít vagy inkább növekedik. Ekkor a tudatalattid akár saját vagy mások példájából kiindulva alacsony időpreferenciát kezd el kiépíteni, ami alapvető feltétel ahhoz, hogy sikeresen tudjál hosszú távon spórolni és a mai extrém erős pénzköltési vágynak ellenállni.

A napóleoni háborúk vége egyben európa szerte az aranyalapra való átállásnak a kezdetét is jelentette.
Minél több nemzet az aranystandardra állt át, az arany annál piacképesebbé vált és ez annál nagyobb ösztönzést váltott ki más nemzetek csatlakozására.

Ahogy már említettem, az emberi leleményesség lehetővé tette, hogy a betétkönyvek, számlák és csekkek segítségével bármilyen méretű kifizetést végezni lehessen.
Néhány megkötés volt, mint például a betétkönyvek birtokosai a kifizetéseket csak saját maguknak végezhették és a számlákat a bankok csak elszámolásra használhatták, a csekkeket pedig csak a kibocsátó banknál lehetett beváltani.
Ez megoldotta az arany méretarányos eladhatóságát és egyben ezzel a legjobb monetáris médiummá is vált mindaddig, amíg az emberek aranyát felhalmozó bankok az általuk kibocsátott papírok mennyiségét fedezet nélkül nem növelték (lásd fentebb a 15. századi Kína sorsát).

Mégis, mi volt az elkerülhetetlen következménye annak, hogy az aranystandard eladhatósága szerte a világon a bankjegyek, betétkönyvek, számlák és csekkek segítségével új szintre emelkedett?

Az örök “másodhegedűs”, az ezüst pénzügyi szerepe feleslegessé vált. Elkerülhetetlen lett a demonetizálása, azaz a pénzügyi szerepének megszűnése.

Az ezüst demonetizálása

Mindaddig amíg az arany és az ezüst közvetlen fizetőeszköz volt, monetáris szerepe mindkettőnek volt. Ez viszonylag hosszú időn keresztül lehetővé tette, hogy 12 és 15 uncia (1 uncia 28,35 g) közötti ezüst per arany áron stabilizálódjon.

Miért pont ez volt az árfolyam? Ehhez vissza kell kanyarodnunk a *készlet-folyósítási arányhoz*, ami egyúttal mindkettőnek megmutatja a földkéregben lévő relatív ritkaságukat, valamint a kibányászásuk viszonylagos nehézségét és költségét. Mivel sokkal könnyebb volt ezüstöt bányászni, ezért kellett 12 és 15 uncia közötti ezüstöt egy uncia aranyért adni. Ez a viszonylagos stabilitás egészen a 19. század végéig kitartott.

Az első szöget az ezüst koporsójában a francia-porosz háború vége ütötte, amikor Németország Franciaországtól 200 millió font összegű kártalanítást nyert és azt az aranyalapra váltáshoz használta fel, ezzel Nagy-Britanniához, Franciaországhoz, Hollandiához, Svájchoz, Belgiumhoz és másokhoz csatlakozva.

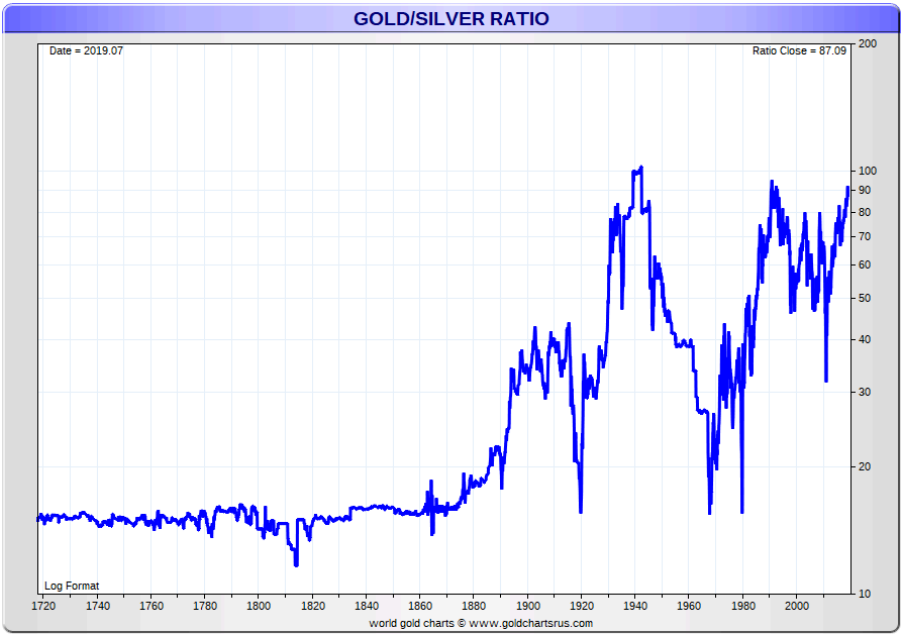
Világszerte az olyan egyéneknek és nemzeteknek, akik ezüstöt használtak azzal kellett szembesülniük, hogy a vásárlóerejük fokozatos csökkenése egyre inkább az aranyra való átállásukat ösztönözte.

Miért csökkent az ezüst vásárlóereje?

Az arany mellett az ezüst a kis összegű ügyletekben (amire kvázi kitalálták) “másodhegedűssé”, azaz teljesen feleslegessé vált, mert az arannyal fedezet banki tranzakciókon keresztül bármilyen kis összeget

ki lehetett fizetni. Ez az ezüst árának jelentős összeomlásához vezetett, amelyből már nem tudott kilábalni.

A kettő átlag aránya a huszadik században 47:1, 2023-ban 85:1 volt.



(Arany/ezüst aránya grafikonon ábrázolva)

Noha az aranynak továbbra is van monetáris szerepe, amint azt a központi bankok felhalmozása is jól mutatja, az ezüst monetáris szerepét vitathatatlanul, elvesztette.

Saifedean Ammous közgazdász ezüstről kialakult véleménye:
”Kína és India története, valamint a XX. század folyamán a Nyugatra való felzárkóztatásuk, a gazdagság és a tőke súlyos megsemmisítésével, amelyet az ezen országok által használt

monetáris fém (ezüst) demonetizálása okozott, elválaszthatatlanul összekapcsolódik.”

Magyarul: Az ezüst demonetizálása gyakorlatilag a kínaiakat és az indiaiakat hasonló helyzetbe hozta, mint a történelem során az összes olyan országot, akinek a pénzneme, azaz cseereszköze könnyen gyártható/bányászható volt:

- a belföldi értékálló pénz (ezüst), a külföldiek számára értéktelen volt, mert idegen értékálló (arany) pénz támogatta őket, ami a külföldiek számára lehetővé tette, hogy ezen időszak alatt Kína és India tőkéjének és forrásainak egyre növekvő mennyiségét, irányítsák és birtokolják.

Az ezüstöt a történelem során, többször próbálták remonetizálni.

- Az amerikai kincstár a 19. század végén úgy döntött, hogy az ezüstöt újra elkezdte pénzként kezelni. Ezután piaci alapon bankok jöttek létre, amelyek kincstárjegyeket és ezüstöt aranyért árultak.
- A kincstár hibás döntésének a következménye a megnövekedett pénzmennyiség (az ezüst készleteket könnyen, relatíve olcsón lehetett elinflálni) az aranykészletek csökkenéséhez vezetett (mindenki a “könnyű” ezüstöt a “nehéz” aranyra cserélte), ami később az 1893-as recesszióba torkollott.

A jólét és virágzás kora

Ahogy már fentebb említettem a francia-porosz háború 1871-ben való befejezésével az összes nagyobb európai hatalom ugyanarra a monetáris sztenderdre, nevezetesen az aranyra váltott.
Ez még mai szemmel is elképesztő jólét és a virágzás időszakához (Európában: La Belle Époque) vezetett.
Közelibb történelmi példa a 19. század második fele is, amely az emberi virágzás, a valaha látott legtöbb innováció- és legnagyobb elért eredmények korszaka volt. Mindegyikben az arany monetáris szerepe döntő jelentőséggel bírt. Miért?

A bolygó nagy része ugyanazt az aranypénzügyi szabványt alkalmazta és ez a viszonylag egyszerű, ám annál fontosabb részlet, a távközlés és a szállítás fejlesztéseit tette lehetővé, mely soha nem látott módon a globális tőkefelhalmozást és kereskedelmet is elősegítette.

Nézzük meg, hogy bizonyos valuták hogyan voltak az aranyhoz kötve.
A brit font 7.3 gramm aranynak, a francia frank 0.29 gramm aranynak és a német márka 0.36 gramm aranynak felelt meg.
Az egymás közötti átváltási árfolyamot szükségszerűen rögzítették 26.28 francia frank és 24.02 német márka per fontban.
Néhány szerencsés országnak az aranyérme meglehetősen jól értékesíthető volt, mert az egész érme színaranyból állt.

Az alábbi táblázatban jól látható, hogy az aranystandardot mely országok meddig használták:

Valuta	Aranystandard periódus	Évek
Francia Frank	1814-1914	100
Holland Forint	1816-1914	98
Angol Font	1821-1914	93
Svájci Frank	1850-1936	86
Belga Frank	1832-1914	82
Svéd Korona	1873-1931	58
Német Márka	1875-1914	39
Olasz Líra	1883-1914	31

Ennyi év távlatából - ha csak a józan észre és arra hallgatunk, amit ezekről az országokról hallottunk/tudunk - láthatjuk, hogy az adott ország mai pozitív vagy negatív gazdasági helyzetét, az aranystandardon eltöltött idő erősen befolyásolta. Miért?

Az egész világban a pénz stabilitása a szabad kereskedelemben tükröződik. Talán még ennél is fontosabb, hogy az aranyalappal rendelkező legfejlettebb társadalmak megtakarítási arányának nem csak számbeli növekedése, hanem időbeli hossza is lehetővé tette, hogy a lakosságban egy alacsony időpreferencia kifejlődjön.
Ez magával hozta a tőkefelhalmozást, amely tőke az iparosodás, az urbanizáció és a technológiai fejlesztések finanszírozására fordítódott. Mindezek a mai modern életüket is formálták.

Ez az időszak az emberiség történelmében teljesen egyedi volt. Se előtte, se utána nem volt olyan időszak, amikor a világ nagy része egy azonos szilárd monetáris egységet alkotott volna. Világszerte ennek hatására soha addigi méretű tőkefelhalmozás, globális kereskedelem, kormányzati korlátozás és életszínvonal fejlődés nem volt tapasztalható. Nem csak gazdaságilag, de társadalmilag is sokkal

szabadabbak voltak, mert a kormányzati bürokrácia nagyon fejletlen volt, ezzel minimalizálva a polgári életbe való beleszólást.

Nézzünk néhány konkrétumot, amely erre a virágzó időszakra jellemző volt:

- Az emberiség legfontosabb technológiai, orvosi, gazdasági és művészeti eredményeit az aranyszabvány korszakában fedezték fel.
- Nagy-Britannia a birodalmát a Pax Britannica csúcséveiben - katonai konfliktusok nélkül - az egész világra kiterjesztette.
- A Bank of England (Nagy-Britannia) bankjegyei ebben az időszakban olyannyira globálisan elfogadottak voltak, hogy pl. 1899-ben Nellie Bly (amerikai író) a rekordnak számító (72 nap) világkörüli körútjára csak brit aranyat és a Bank of England bankjegyeit vitte magával.

Mégis miért lett ennek a jólétnek vége? Miért tűnt el mára az aranystandard?

Az Aranystandard eltörlése

Az 1914-es katasztrofális évben az általános jólét virágkora összeomlott. Nemcsak az I. világháború kitörése miatt, hanem ebben az évben a világ legnagyobb gazdaságai az aranyszabványt elhagyták és azt “fedezetlen”, úgynevezett *FIAT* kormányzati pénzekkel helyettesítették.

FIAT pénz: A fiat valuta, egyszerűen fogalmazva egy olyan törvényes fizetőeszköz, amelynek értéke a kibocsátó kormánytól függ, nem pedig egy fizikai árutól vagy árucikktől. Az ilyen típusú pénzeknél a fiat valuta értékét meghatározó kormány erőssége kulcsfontosságú. A világ legtöbb országa az áruk és szolgáltatások vételére, illetve befektetésre és megtakarításra a fiat valutarendszert használja.

Érdekességképpen megemlíteném, hogy az aranystandardot az első világháború alatt (az 1930-as évek után is) csak a semleges Svájc és Svédország tartotta meg. (*Széljegyzetként költői kérdés: Esetlegesen ezen országok emiatt is lettek mára olyan gazdagok? Vagy csak véletlen egybeesés lenne? Megsúgom nem, de erről később.)*

Az aranystandard, mint elképzelés működhetett volna, de mivel mi emberek vagyunk, ezért “muszáj volt” egy alapjaiban tökéletesen működő rendszert (lásd a fémpénzek korát) tönkretenni. Hogyan?

A “hogyan” megértéséhez, két fontos elemet emelnék ki:

1. A kormányok és bankok mindig a tartalékban lévő aranymennyiségen túlmutató csereeszközöket (pl. bankjegyeket) hoztak létre.
2. Sok ország tartalékaiban nemcsak aranyat használt fel, hanem más országok pénznemeit is.

Mit okoztak a fentiek? A központi bankok “túlnyomtattak”, mert amíg az aranyérme nagyon értékálló (nehezen előállítható) pénz volt, a központi bankok közötti fizetések kiegyenlítésére használt instrumentumok (bár azok névlegesen visszaválthatók) a gyakorlatban az aranynál könnyebben előállíthatóak voltak. Ezáltal a rendszer összeomlása “borítékolható” volt.

A FIAT pénz térnyerése

Rájöttek a központi bankok vezetői, hogy az emberek akkor is hajlandóak a FIAT pénzt használni, ha a mögött már semmilyen konkrét árucikk (pl. arany), mint fedezet nincs.
Az országok vezetői a hatalmukat arra használják, hogy a lakosságot minden áron a saját kormányuk által kibocsátott FIAT pénz használatára kényszerítsék.

Viszont egy dolgot tisztázzunk: a vezetők szava, a lehetséges új területek vagy új ország vagyon/teljesítmény, a forgalomban lévő FIAT pénzzel semmilyen valódi kapcsolatban nincs.
Az adott pénz értékére kizárólag a “marketing” (mennyire tartják a belföldi és külföldi befektetők értékesnek) van hatással és az, hogy mennyi van belőle forgalomban.
A túl sok pénz nyomtatása, ahogy a történelem már többször bizonyította inflációt fog okozni.

Nincs kivétel, mert ha “kecskére bízzuk a káposztát”, akkor a káposztát a kecske meg fogja enni. Bármilyen jó lehet marketingben egy ország a pénznyomtatás és az ezzel járó infláció minden országot sújt, csak nem egyforma mértékben.

Hivatalosan a kormány a FIAT pénz értékét három politikai eszközén: a monetáris, fiskális és kereskedelempolitika összegén keresztül határozza meg, de ami a leginkább kiszámíthatatlan, az az egyének a politikai eszközökre való reakciói.

Sajnos világszinten az oktatás minőségének szisztematikus leépítésével a különböző generációk teljesen elfogadottnak veszik,

hogy a pénz “romlik” és ez ellen pedig nincs mit tenni legfeljebb annyit, hogy minél hamarabb elköltjük. Ez a mai modern (keynesiánus) közgazdaságtant végzett emberek “meséjének” hatása.

Ezzel szemben az osztrák iskola (valódi) közgazdaságtant vallók azt hirdetik, hogy:

- a vagyon, amely által az egyén mindenki élete felett a pénz irányításán keresztül hatalmat szerez a pénz mennyiségének manipulálásával nem állítható elő (lásd fentebb a *Cantillion-effektus*-t),
- a civilizált társadalom mindig a pénz integritásától függött, ami a kereskedéshez és a tőkefelhalmozáshoz biztos alappal szolgált.

Magyarul: A pénz független kell legyen bármilyen külső behatástól. Ezért volt az arany évezredekig tökéletes, mert az éves inflációja (kitermelése) alacsony és ez ellen “nyomtatással”, azaz semmiből való előállítására, egyik uralkodó/vezető sem volt képes.
Az emberek ebből kifolyólag az arany értékében bíztak és ez a bizalom hozta létre, hogy a társadalom fejlődjön, a gazdaság és a kereskedelem komplexebb struktúrákat hozzon létre.
Ezzel szemben jól látható, hogy a keynesiánus gondolkodáson alapuló vezetés, “nyomtatással”, adóemelésekkel, korlátozásokkal próbálja ugyanazt létrehozni (sikertelenül), amit az arany és a szabad piac minden probléma nélkül, organikus úton létrehozott.

Az aranynak lényegében az átlag lakosságon kívül csak ellenségei voltak. Ezt Ludwig von Mises, osztrák közgazdász tökéletesen összefoglalta:

“A nacionalisták az aranystandard ellen küzdenek, mert el akarják húzni országaikat a világpiacról, és amennyire csak lehetséges, nemzeti gazdasági önellátást létesíteni. Az intervenciós kormányok és nyomásgyakorló csoportok az aranyszabvánnyal harcolnak, mert úgy ítélik meg, hogy ez az árak és bérek manipulálására tett törekvéseik legsúlyosabb akadálya. Az arany elleni legfanatikusabb támadásokat azonban a hitelkiterjesztés szándéka képezi. Ezekkel együtt a hitelbővítés az összes gazdasági betegség orvosa. Az aranystandard a készpénz által kiváltott vásárlóerő változásainak meghatározását a politikai színtérről eltávolítja. Általános elfogadása megköveteli az igazság elismerését, miszerint a pénznyomással nem lehet minden embert gazdagabbá tenni. Az aranystandard elleni felháborodást az a babona ihlette, miszerint a kis papírdarabokból a mindenható kormányok gazdagságot teremtenek […] A kormányok lelkesen el akarják pusztítani, mert a téveszmék mellett elkötelezték magukat, hogy a hitelbővítés megfelelő eszköz a kamatlábak csökkentésére és a kereskedelem egyensúlyának „javítására” […] Az emberek harcolnak az aranyszabvánnyal, mert a nemzeti kereskedelmet, a szabad kereskedelemet, a békeharcra, a szabadság totalitárius kormányának mindenhatóságára akarják felváltani. “

A fentiektől függetlenül, mindig azt kell nézni, hogy mi a valódi emberi (itt vezetői) cselekedet. Szándékosan fogalmaztam így, mert Mises: Human Action (Emberi cselekvés) című könyve, a közgazdaságtant nem, (a mai) “közgazdaságtani modellek” ráerőszakolásán keresztül próbálja megmagyarázni, hanem az egyszerű ember belső indíttatása által irányított cselekedetein keresztül. (*Mivel én is az osztrák iskola tanait tanultam, így ez a könyv is ennek az irányzatnak a mentén íródott*).

A 20. század második felében, amikor már masszívan a FIAT pénz volt az elfogadott és az USA dollár mint “globális standard”-ként kezdett elterjedni, a központi bankok az arany felhalmozását mégis folytatták. Miért? Amikor az aranynak már abszolút semmilyen monetáris szerepe nem volt, miért halmozták fel? A válasz egyszerű: tudták hogy a relatív ritkasága és általános ismertsége/elfogadottsága magas értéket képvisel.

A központi bankok arany vásárlása a napjainkra is igaz, sőt egyes országok (pl. Kína) extrém módon évtizedek óta nettó arany felvásárló ország (a saját területeken is kibányászott arany náluk marad).

A saját és sokan mások véleménye is az, hogy ez a központi bankok általi aranybirtoklási “láz” pusztán azért van, mert tudják, hogy a saját és mások FIAT valutája valójában teljesen értéktelen és egy potenciális globális pénzügyi összeomlás esetén a raktárban lévő arany jó csereeszköz lehet.

Mielőtt összegezzük ezt a részt először kiemelném, hogy gyakran figyelmen kívül hagyott tény az, hogy ellentétben azzal, amit a név állíthat, egyetlen FIAT pénz sem került forgalomba kizárólag a kormány “FIAT útján”!
Mindegyik eredetileg aranyra vagy ezüstre volt beváltható, vagy olyan pénznemekre, amelyek aranyra vagy ezüstre voltak átválthatók. Csak és kizárólag ezután következtek a különböző korlátozó intézkedések, amik folyamán az emberek már csak a kormányzati pénzt használhatták, mindenféle arany, ezüst vagy bármilyen kézzelfogható árucikk fedezete nélkül.

Ha tehát tudjuk, hogy a nyomtatás inflációt szül, akkor miért “nyomtatnak”? A válasz viszonylag egyszerű. Ha egy kormány adót

emel azt a lakosság azonnal vagy relatíve hamar érezni fogja, és ennek a választásokon negatív hozamánya lehet (másra szavaznak), rosszabb esetben a vezetők ellen fellázadhatnak. Viszont, ha a kormány a forgalomban lévő pénzt “hígítja” (inflálja), akkor annak hatása (általában) csak évek múlva lesz igazán érezhető.
Minél nagyobb egy pénz piaca, annál később lesz a pénz “nyomtatásnak”, negatív értelemben hatása.
Egyes elemzők azt mondják, hogy az USA ma “kinyomtatott” dollárjának az inflációs hatását kb. 18 hónap múlva fogja kifejteni. Ez bőven elég idő arra, hogy bármilyen mondvacsinált indokkal (pl. járvány) a kormányról (nemzeti bankról) a figyelmet elterelják, és ezzel úgymond a dolgot “megússzák”.
Persze ha nagyon elszalad velük a ló, akkor *hiperinflációs* helyzet is fennállhat és akkor már teljesen mindegy mi a kifogás, mert a népharagot csak statáriummal és/vagy egyéb kényszerítő eszközökkel tudják leverni.

Hiperinfléáció: A hiperinfláció egy szélsőségesen nagy infláció. Általában a havi 50%-nál nagyobb árszínvonal-emelkedést, hiperinflációnak nevezzük. A pénz értéktelenné válik, a továbbiakban a vagyontartási-, értékmérő- és csereeszköz szerepét nem látja el.

Sajnos ma nagyon sok ország hiperinflációs környezet közelében van. Pl. Argentína, Venezuela, Törökország, stb. Ezen országok lakosságának létfontosságú, hogy a mindennapi keresetüket egy értéktartó eszközbe tegyék, mert a pénzük napi szinten látványosan kevesebbet ér. Sajnálatosan nekik a legnehezebb, mert ezen kormányok a pénz bárminemű egyéb értékálló eszközre való váltását erősen korlátozzák.

Az infláció tehát egy olyan rejtett adó, amit mindenki, aki az adott pénznem használtára rá van kényszerítve megfizet.

A FIAT pénz egy kormány számára milyen egyéb előnyökkel jár?

Korábban, egy olyan monetáris rendszerben, ahol az arany mint pénz az emberek kezében volt, a kormánynak a háború finanszírozására szolgáló adózás vagy kötvénykibocsátások mellett csak a saját kincstára volt. Ez az országok közötti konfliktusokat meglehetősen jól korlátozta és a huszadik század előtti, világszerte tapasztalható viszonylag hosszú békeidőszak középpontjában állt. Mindez a “fék” mára többé egyik országban sem létezik, így jól látható, hogy a háborúk visszatartásának lehetősége minimálisra csökkent.

Itt tartunk most, de mielőtt a Bitcoin világába belevágunk, előbb egy kis kitekintő.

Második fejezet: A FIAT utáni alternatív lehetőségek

Lényegében bármely nap a világ nemzeti bankjainak vezetői az alábbi két lehetőség közül tudnak választani:

Visszatérés az Aranystandardra

Fel kell tegyük a kérdést: Ha az arany annyira értékállónak bizonyult és mint pénz, kvázi évezredekig nagyon jól funkcionált, akkor mi tart minket vissza attól, hogy az aranystandardra újra visszatérjünk?

Először is röviden, a mindenkori kormány. De tényleg.
A kormány a visszatéréssel a felettünk lévő hatalmát totálisan elveszítené, mert mindenhez “jóváhagyást” kellene kérnie, azaz támogatásért “kuncsorognia”. Miért? Mert, ha az adóbevételek a rossz költségvetés miatt elfogynak és/vagy esetlegesen egy új háborút akarnának indítani, de nincs hozzá elég pénzük, akkor a lakosságtól kellene további adóbevételeket szerezniük.

Ezen túlmenően még a forgalomban lévő pénzkészletet is (a meglévő aranykészlethez képest) újra kellene értékeltetni. Mivel az aranykészletek a forgalomban lévő pénzmennyiséghez képest köszönő viszonyban sincsenek, emiatt a valuta nagyon durva leértékelése hatalmas felháborodást szülne.
Ezentúl az emberek a kormányzati pénzben soha többé nem bíznának meg (főleg, ha lenne egy alternatíva), és csak és kizárólag az aranyhoz ragaszkodnának, ezzel kvázi a kormányzati pénzt feleslegessé téve.

A bankok a helyzetet rövid távon is megsínylenék, mert az emberek nem mernék az aranyukat a bankokban tartani (ekkor a pénzt aranyra már rég visszaváltották), és ez a gazdaság és a kereskedelem zsugorodását okozná. Miért?
Azért, mert az aranyrög nagyon nehezen és drágán tud “utazni”, tehát mondjuk egy kínai rendelés aranyban való kifizetése rendkívül nehézkes és költséges lenne. Minden export és import extrémen megdrágulna, és ezzel üzletek, cégek mennének tönkre.

Idővel természetesen az emberek és a bankok között a jelenlegihez hasonló bizalom újra felépülne, ami előbb-utóbb ezt az angolul “boom and bust” (fellendülés és válság) ciklust is újraindítaná. Miért? Mert valamikor valaki a pénz feletti irányítást ismét a “kezébe” akarja majd venni, ami kvázi az aranystandard ismételt “felfüggesztésével” és a “nyomdagépek beindulásával” járna .

“Becsszó”, nem fogunk nyomtatni

Előfordulhat olyan eset is, hogy egyik másik kormány magába száll és azt mondja: “Mától fogva a központi banknak megtiltja, hogy a meglévő pénzkészleten túl további pénzmennyiséget állítson elő.”
Ekkor egy érdekes helyzet áll majd elő, mert az aktuális évi költségvetéssel egészen addig lehet majd mínuszba menni, ameddig az ország központi bankjában tárolt tartalékai kitartanak. Utána vagy - leegyszerűsítve - “nyomtatnak”, vagy új adót vetnek ki, vagy csődbe megy az ország.

Mégha a kormányt a legjobb szándék is vezérli, két komoly irányból is bukás lehet a vége. Külföldi tehetős kormányok mind kintről, mind

bentről (pl. maffia, ellenzék) mindent megtesznek majd azért, hogy a kormány a lehető legtöbbet hibázzon, ezzel is növelve az államháztartási hiányt, hogy végül elbukva más nemzetek számára ne legyen pozitív követendő példa. Miért tennének ilyet?
Azért, mert előbb utóbb a pozitív példa a saját országukat is "megtalálja" és majd egy párt vagy mozgalom segítségével a lakosság is ezt az "önmegtartóztatást" fogja követelni. Miért követelnék?
Az általam említett "önmegtartóztatás" kvázi az inflációt megszüntetné és ha kellően hosszú távon kitartanak, akkor akár deflációt is okozhatna. Tudom ettől a fogalomtól a legtöbb közgazdászt kirázza a hideg, de gondolkozzunk csak el, tényleg akkora "mumus" a defláció? Mi is történik ekkor?
Ilyenkor az árak nem felfelé, hanem lefelé mennek. Nem a piac fog zsugorodni, mert a pénz értéke egyfajta versenyt fog beindítani. A silány termékek kiesnek, mert azért senki sem akar majd fizetni (hisz tudják "holnap értékesebb lesz a pénzem"), viszont egyre több, az emberek számára értékes termékek/szolgáltatások fognak megjelenni, amiért a lakosság majd hajlandó lesz fizetni. Tehát nem csak az árak fognak csökkenni, hanem a silány helyett minőségi termékek/szolgáltatások fognak megjelenni.

Ezt az utat választva a másik lehetséges bukás pedig egyszerűen csak a rossz gazdaságpolitika miatt következhetne be. Az ország tartalékai elfogynának, ez csőd közeli állapotot hozna, ami miatt a "nyomtatást" újra be kellene vezetni. Ez hirtelen nagyon durva inflációt okozna (a lakosság és a befektetők a forgalomban lévő pénzből menekülnének), és ez végül más nemzetek számára újabb ékes példaként szolgálna, hogy a pénzkészletet miért nem szabad "maximalizálni".

Arra ne is gondoljunk, hogy egy természeti “baleset”, személyekkel kapcsolatos “véletlenek” (pl. merénylet), új vezetés ezt a tervet megbuktathatja.
Ne felejtsük el, hogy itt a kormányzatból mindenkinek nagyon hazafinak kell lennie, hogy még véletlenül se tegyenek el maguknak (“zsebre”) egy fillér plusz pénzt se. Meddig tarthat ez? 4 évig? 40 évig? Egyszer mindenki nyugdíjba megy, az utána lévő generáció se fogja majd a könnyebbik utat választani? Mi a garancia? Semmi.

Ami biztos, hogy az adott ország pénze egy időzített “bomba” lenne, mert bármelyik pillanatban (mondjuk egy vasárnap késő este) úgy dönthet a kormány, hogy a könnyebbik inflációs utat választja. A pénzt a hétfői piacnyitáskor a pánik miatt a világ különböző piacai katasztrofális szinten leértékelnék.

A kérdés tehát adott: egy ilyen helyzetben, Te kedves Olvasó, szeretnél-e egy ilyen “ketyegő bombán” ülni?

Harmadik fejezet: A Bitcoin felépítése

Elérkeztünk a várva várt részhez, amiért valójában mindenki ezt a könyvet a kezébe vette. Muszáj volt az eddigi 36 oldalt figyelmesen átolvasni, mert tudván, hogy a történelem szereti önmagát megismételni, így a Bitcoinnal kapcsolatban is sokszor fogok az előzőekben leírtakra utalni.

Mielőtt a Bitcoin felépítésére, működésére kitérnék, szeretnék pár szót arra is szánni, hogy egyáltalán ki-mit gondol vagy vár tőle:
Először is vannak azok, akik pénzügyi érdekek miatt utálják, ellenzik, mert vélt vagy valós félelmükből kifolyólag a saját egzisztenciájukat féltik. Ezek mivel általában a mainstream média szereplői, igyekeznek a lakosság nagy részét a szokásos (már leírt) módon manipulálni, ezáltal is a Bitcointól a lehető legjobban eltántorítani.
Vannak pedig a támogatók, akik igen sokrétűek. Ezek lehetnek, akik a gyors meggazdagodást látják benne, a szabadságjogok kivívásához fontos eszközeként tekintenek rá, vannak akik *értékálló pénz*ként tekintenek rá, és persze vannak a spekulánsok, akik csak a piaci mozgásokon akarnak FIAT valutában meggazdagodni.
Jól látható, hogy a Bitcoin bárhogyan is, de nagyon sokféle emberre sokféle tekintetben, de mindenképpen hatással van.

> *Értékálló pénz: a piac által szabadon választott pénz. Azaz az a pénz, amelyet teljes egészében annak a személynek, aki a szabad piacon jogszerűen szerezte és nem más (harmadik fél) ellenőrzése alatt áll.*

Mi a különbség a FIAT pénz és a Bitcoin között?

Valójában azt a minimális készpénzt leszámítva, ami forgalomban van, a FIAT pénz nagyrészt csak digitális valójában létezik (USD esetében az összes pénzmennyiségnek kb. 6-7% van készpénzben). Ha a FIAT is lényegében digitális és a Bitcoin is, akkor a Bitcoin miben jobb, mint a FIAT pénz? Röviden: szinte mindenben és olyasmiben is, amire nem is gondolnál.

A Bitcoin olyan tulajdonságokkal is rendelkezik, amivel a FIAT (digitális) pénz soha. Mégpedig a készpénz pozitív tulajdonságaival, amik a közvetítő nélküli kereskedelmet és a tranzakciók véglegességét biztosítják.

Magyarul: A Bitcoin utalás mindig 2 entitás között történik anélkül, hogy bárki engedélyére, jóváhagyására lenne szükség. Csak úgy, mint a készpénz esetében, ha én odaadok neked 1000 Ft-ot abba senki sem tud beleszólni. Ugyanígy igaz a tranzakciók véglegességére is. Amikor én készpénzben az 1000 Ft-ot odaadtam neked, akkor annak a tranzakciónak ott vége is lett. Ez viszont a digitális FIAT pénz (pl. banki tranzakciók) esetében nagyon nincs így. Főleg, amikor mondjuk a bankkártyádat használod. Azonnal megterhelik a kártyát (zárolják az összeget), de a pénz effektív könyvelése (a te és a másik fél számláján) több nap után történik meg.

A Bitcoin esetében, amint bekerült egy blokkba (erről bővebben később) az ügylet teljesen véglegesnek tekinthető. Ezzel lényegében a Bitcoin a digitális készpénz fogalmát valósította meg.

A szabályok felszabadítanak

Először is tisztázzuk, hogy mi az a minimum, amit a Bitcoin-tól várunk, hogy a történelem során már többször bemutatott “monetáris bukás” ne következzen be:

- A mennyiségét NE lehessen elinflálni, mert ha az adott pénzből bármilyen lehetőség is van többet csinálni, akkor bizonyosan valaki valamikor meg fogja próbálni.

A világon a Bitcoin az első olyan eszköz, amiből bizonyítottan 21 millió darabnál több nem lesz. Ez egy olyan szabály, amit a legtöbb ember, aki egy kicsit is hallott róla talán tud. Hogyan lehet az, hogy senki sem tud belőle többet csinálni?
Ahhoz, hogy ezt megértsük a hálózat felépítéséről minimálisan is, de beszélnünk kell.

A Bitcoin-ról akkor beszélünk, ha mindenki a Bitcoin szoftvereit ugyanolyan szabályok alapján futtatja!

Ez nagyon fontos, mert a rendszer úgy van kitalálva, hogy ha én bármilyen szinten az induláskor rögzített szabályokba belenyúlok, akkor az összes többi hálózatban résztvevő szoftver egyszerűen csalás miatt engem kizár. Lényegében magányosan fogok egy “alternatív” hálózatban létezni, ahol rajtam kívül senki más nincs.

Ahhoz tehát, hogy a maximum 21 milliónyi Bitcoin szabályt bárki megváltoztassa, a rendszerben résztvevők 51%-nak a “beleegyezése” kell!
Magyarul, ha én azt mondom, hogy holnaptól 100 millió Bitcoin legyen forgalomban, akkor a Bitcoinnal kapcsolatos (szoftvert futtató)

entitások legalább 51%-át rá kell vegyem, hogy a maximális mennyiséget kereken (!) 100 millió Bitcoinra változtassák meg. Miért fontos, hogy “kereken”?
Azért, mert az informatika világában ezek a szabályok úgy működnek, hogy bárminemű kis eltérés azt jelenti, hogy nem ugyanarról beszélünk, így tehát azt pontosan 100 millióra kellene állítani. Annak az esélye, hogy egymagam erre a többséget rá tudjam venni rendkívül kicsi, mondhatni elhanyagolható. Miért?

A Bitcoin rendszere teljesen egyedülálló, mert úgy van felépítve, hogy központi irányítás nélkül tökéletesen tud működni. A rendszer alapja a totális bizalmatlanság, így mindenki mindenkit ellenőriz. A legtöbb Bitcoin szoftvernél nincs “automatikus frissítés”.

Nagyon sokféle Bitcoin csomóponti szoftver (ezekről a következő részben beszélek) létezik és mind (szándékosan) úgy van megírva, hogy manuálisan kelljen frissíteni (minimum 1 gombot meg kell nyomni). Ebből kifolyólag, amint valamelyik változatába az egyik fejlesztő olyan programkódot csempészne bele, ami a szabályokkal vissza élne, az azonnal kitudódna és azt a fejlesztőt/programot a felhasználók “dobnák”. Lényegében elég lenne, ha a módosítást nem telepítik, de inkább valószínű, hogy azt a csomóponti szoftvert lecserélnék.

Régebben még elképzelhető lett volna egy olyan frissítés (többen próbálkoztak ilyennel), hogy egy úgynevezett “Hard fork”-al mindenkit (!) egy új módosításra való átállásra kötelezzen. Ez viszont visszafelé már nem lett volna kompatibilis, így akik ezt nem telepítették volna, azokat a rendszer a használatból kizárta volna. Mivel ez elképesztő koordinációt igényel (lásd fentebb a 21 millió Bitcoin szabály módosítását), ezek a próbálkozások már a kezdetekben elhaltak.

Néhányan persze nem bírtak magukkal és inkább egy “másolatként” (egy új elnevezéssel és a kívánt módosítással) egy “alternatív” Bitcoint indítottak. A régi Bitcoin felhasználók többsége ezekkel az új irányvonalakkal nem értett egyet, így a piac ezeket kivétel nélkül bukásra ítélte, és így az értékük napjainkban (2023) a nullához konvergál.
Ma már (nagy valószínűséggel) a felhasználói bázis mérete és széttagoltsága miatt csak olyan frissítést lehet a hálózaton “végigvinni”, ami nem kötelező érvényű, tehát nem kell mindenki egyetértsen vele (azaz telepítenie).
Ez azt jelenti, hogy aki bármely okból kifolyólag nem akarja ezt a módosítást/frissítést a hálózatot továbbra is ugyanúgy tudja használni mint előtte, csak az új fejlesztések számára nem lesznek elérhetőek.

Emellé a hab a tortán, hogy a rendszerben mindenki saját érdekéből úgy vesz részt, hogy annak összes szabályát betartja. Mit jelent ez? Lényegében azt, hogy az előző példánál maradva senki sem fogja a 21 millióról 100 millióra való maximális mennyiség növelést “megszavazni”, mert az azt jelentené, hogy a saját Bitcoin mennyiségének az értéke azonnal mindenkinek durván ötödét érné.

Általános hibás vélekedés: “A 21 millió Bitcoin semmire sem elég, sokkal több kellenne belőle! A Földön több, mint 8 milliárd ember van. Ez tuti nem elég mindenkinek!”

Aki osztrák közgazdaságtant tanult (sajnos csak kevesen) az tudja, hogy bármekkora pénzmennyiség bármekkora gazdaságnak elegendő. Ezt megismétlem: tehát bármekkora pénzmennyiség, bármekkora gazdaságnak elegendő. Miért?
Nem a pénz mennyisége a fontos, hanem a vásárlóereje!

Mindaddig, amíg megfelelően osztható és csoportosítható (!), hogy a tulajdonosok tranzakciós igényeit kielégítse, az adott pénzzel nem lesz gond.
Márpedig minden Bitcoin 100 millió “sat” (Satoshi)-ra osztható. Nana, de mi lesz, ha 1 sat ára túl sok lesz? A “második rétegen” (erről később) már most is van “msat” (“mili” Satoshi), azaz 1 sat 1000 msat-ot ér. Piaci igény esetén ez bármikor tovább osztható.
Tehát ez nem úgy van, mint a FIAT pénzügyi rendszer esetében, ahol azért, hogy mindenkinek jusson (hazugság), a pénzt további “nyomtatással” állítják elő. A Bitcoin esetében a már meglévő készletet osztják kisebb mennyiségre. Ez azt jelenti, hogy ha neked 12 millió satoshi-d van, amely egyben 1.2 milliárd msat-nak is megfelel, bármelyiket is nézed, attól a vagyonod értéke és mennyisége nem változik. Így abban az esetben, amikor a Bitcoin értéke tovább emelkedik és egy kenyér ára nem 1 satoshi lesz, hanem csak 123 msat-ba (0.123 sat) kerül, könnyen ki tudod majd fizetni.

Most akkor a szabályok hogyan is szabadítanak fel? A “fejemben” a szabályok mindig korlátoznak valamiben.

Téves elképzelés, mert John Stuart Mill filozófus A Szabadságról című művében a következőket írja:
"Minden olyan cselekedetet el szabad nyomni, amely igazolható ok nélkül kárt okoz másnak… Az egyén szabadságának tehát korlátozottnak kell lennie: nem lehet más emberek kárára."
A könyv a szabadság filozófiájával foglalkozik, és Mill azt a tézist fogalmazza meg, hogy a szabadság nem feltétlenül azt jelenti, hogy mindent szabad csinálni. Szerinte a szabadság azt jelenti, hogy az egyén szabadon dönthet, hogy mit akar csinálni, anélkül, hogy mások akadályoznák. A szabályok biztosítják, hogy mindenki

szabadon élhesse az életét anélkül, hogy mások szabadságát korlátozná.

Amennyiben Bitcoint birtokolsz és a szabályrendszerének önként “aláveted magad”, akkor ez olyan mértékű gazdasági szabadságot ad, amely a Bitcoin feltalálása előtt nem volt lehetséges. Lehetőséget ad, hogy nagy mennyiségű értéket küldj anélkül, hogy bárkitől bármilyen engedélyt kellene kérned!
A Bitcoin értéke, a világ bármely pontján semmiféle fizikai tényezőtől nem függ, ezért a politikai vagy a bűnöző világ bármely fizikai ereje teljesen soha nem akadályozhatja meg, semmisítheti meg, nem kobozhatja el!
Ezzel a modern világ történelmében először az egyén a saját kormánya ellen olyan pénzügyi szabadságot tudott kivívni, amely előtte soha nem létezett!

Oké, oké, beszéltem itt “Bitcoin szoftverekről”, “csomóponti szoftverről”, “résztvevőkről”, “mindenki mindenkit ellenőriz”, de ezek most mik is valójában és ki, hogyan, kit ellenőriz?

A szereplők

A Bitcoin rendszer három fő résztvevőből áll:

- Bitcoin csomópontok: Ezek azok a szoftverek, amelyeknek feladata ellenőrizni, hogy mindenki minden szabályt betart.

Ezek azok, amelyek a Bitcoin blokklánc (erről később) működését és a “bányászokat” is felügyelik.

- Bitcoin “bányászok”: A köznyelvben így terjedt el és ezért a könyvben is végig a “bányászok” kifejezést fogom használni, de valójában ezek olyan otthoni vagy ipari létesítményekben lévő gépek, amik a Bitcoin utalásokat ellenőrzik és ezeket úgynevezett blokkokba rendezik (erről később). Semmilyen klasszikus értelemben vett bányászatot nem folytatnak, hanem számításokat végeznek, adatokat dolgoznak fel. Konkrétan, ha pl. Józsi Pistinek 1 Bitcoint utal, a gépek az egész “láncolaton” azt ellenőrzik, hogy az az 1 Bitcoin tényleg létezik-e, illetve korábban jogosan került-e Józsihoz, amit Pistinek át akar utalni. Ha minden rendben van, akkor az utalást jóváhagyják és az majd egy “blokkba” bekerül (erről később).

- Bitcoin tárcák: Remélhetőleg a legtöbb ember, aki bárminemű Bitcoint birtokol, egy ilyen szoftveres (ingyenes) vagy hardveres (fizikai) tárcában “tárolja” (valójában nem, de erről később) és nem valakinek a szerverén (pl. tőzsde).
  Ezek mindegyike a tranzakciók elvégzésének idejére vagy egy saját, vagy valakinek a Bitcoin csomópontjára vannak direkt vagy indirekt módon (erről bővebben a 4. fejezetben) kötve. A tranzakciók nem tudnak csak úgy a levegőben lógni, ezen csomópontok memóriájában “pihennek” mindaddig, ameddig azokat egy bányász nem ellenőrzi és blokkokba nem rendezi.

Mint állítottam, senki nem bízik senkiben, így mindenki mindenkit ellenőriz.

A Bitcoin csomópontok feladata, hogy a szabályosságot mindenkin (!) megkövetelje!
Ez úgy történik, hogy amennyiben egy bányász csal, vagy a blokkok létrehozásának szabályait megszegi, vagy esetleg a tranzakciókat bármi egyéb módon manipulálja, úgy az összes csomópont azt a konkrét bányászt és a hozzá tartozó manipulált adatot kizárja. Ezzel a bányász minden befektetett energiát elveszített. Szerencsére a rendszer költségek szempontjából teljesen asszimetrikus felépítésű.
Mit jelent ez?
Egy Bitcoin csomópontot bárk relatív olcsón létrehozhat (kb. 50-70 000 Ft) és üzemeltethet, így a világban jelenleg nagyon sok (30 000+) ilyen csomópont van szétszórva. Ezáltal a bányászok munkáját nagyon olcsó ellenőrizni, viszont ezzel ellentétben extrémen drága bányászni.

A csomópontok futtatásának viszonylagos olcsósága és a blokkok létrehozásának magas költsége (energia) miatt a bányászok arra kényszerülnek (a gazdasági ösztönzők miatt), hogy minden szabályt betartsanak.

A tárcák esetében is bármely csomópont - amely nem lett manipulálva - úgy működik, hogy minden tranzakciót előzetesen ellenőriz mielőtt az a bányászokhoz kerülne. Ez azt jelenti, hogy egy szabályosan működő csomópont minden alapvető ellenőrzést elvégez és a bányászoknak ezt kvázi csak jóvá kell hagyniuk. De, mint említettem senki sem bízik a másikban, vagyis a bányászok ettől függetlenül a fent leírt módon mindent az elejétől kezdve újra ellenőriznek.

Üzletileg a Bitcoin csomópont futtatása azoknak éri meg, akik nem akarnak senkiben sem megbízni, hanem szeretnék, hogy a Bitcoin blokkláncának egyik másolata náluk legyen (1) és biztosak akarnak lenni, hogy mindenki minden szabályt betart (2). Másodsorban, ha ők

Bitcoint utalnak vagy kapnak, akkor a saját csomópontjukon ellenőrizve bizonyosak lesznek abban, hogy az adott utalás ténylegesen megtörtént (3), ezzel minden átverést kizárva. *(Itt megjegyezném, a titkosításoknak köszönhetően a tranzakciók megmásítása teljességgel kizárt, itt maximum csak az emberekhez köthető különböző félrevezetésekről beszélhetünk, melyekről egy későbbi részben írok.)*

Itt ismét új fogalmakkal találkoztunk, mint a “blokklánc” vagy a “blokk”, melyekről a most következő fejezetben beszélek.

A Blokklánc

Mivel a Bitcoin hálózat úgy működik, hogy nincs egyetlen egy központi szereplő sem, ezért valamit ki kellett arra találni, hogy hogyan legyen minden lényeges információ mindenki által ismert és egységesen az összes résztvevő között megosztva.
Erre sok gyorsabb és egyszerűbb központosított megoldás létezett, de decentralizált rendszerben való használatra egyik sem volt alkalmas. Miért? Lényeges volt, hogy az adatbázisban a bővítéseket minden résztvevővel csalás kizárásával lehessen “leegyeztetni”.

A rendszer kitalálója (Satoshi Nakamoto, anonim kitalált név) úgy gondolta, hogy a fenti problémára a blokklánc elrendezés a legalkalmasabb megoldás. Ezt valójában úgy kell elképzelni, mint egy gyöngyfüzért, aminél az egyes gyöngyök precízen sorszámozottak; mindegyik egymáshoz kapcsolt és a sorrendjük technikailag egyedi, megmásíthatatlan.

A gyöngyöket a Bitcoin hálózatában “blokkoknak” nevezzük. Ezekbe a blokkokba a bányászok, a csomópontoktól kapott utalásokat rendezik. Az egyes blokkok mérete maximalizálva van, és mivel bármennyi utalás nem tud beleférni az utalások között egyfajta verseny van, hogy a blokkba melyik utalás, mikor kerülhet. Hogy kell ezt a versenyt elképzelni?

Amikor mi egy Bitcoin utalást elküldünk nem csak azt adjuk meg, hogy melyik számlánkról, kinek, mennyit szeretnénk utalni hanem azt is megadjuk, hogy erre az utalásra mennyi utalási díjat szeretnénk áldozni. Ez teljesen egyedi, mert lehet 1 sat/byte -tól bármennyi, attól függően, hogy az utalás nekünk mennyire sürgős.
A “byte” itt arra vonatkozik, hogy minden tranzakciónak van egy mérete és ezt jelen esetben “byte”-ban fejezik ki. Tehát, ha mondjuk egy tranzakció mérete 200 byte, akkor a bányászoknak 1 sat/byte tranzakciós díj megadásával 200 sat díjat vagyunk hajlandók fizetni.

Jó jó, de miért fizetnék többet? Miért nem lehetne fixen mindenkinek a (minimum) 1 sat/byte az utalási díj?

Ahogy már említettem a blokkok mérete maximalizált, tehát egy blokkba kb. 2 000 - 3 000 tranzakció fér. A bányászok egy blokkot átlagosan 10 percenként hoznak létre, azaz naponta 24x6 = 144 blokkba kb. 288 000 - 432 000 tranzakció fér bele.
Jól látható, hogy ez globális szinten nagyon kevés, így valamilyen sorrendet kell felállítani kinek mennyire fontos, hogy az utalása a közvetlen következőbe vagy csak a sokadik blokkba kerüljön bele.
Erre lett a dinamikus utalási díjrendszer kitalálva, azaz mindenki az utalási díj megadásával dönti el, hogy neki az utalás mennyire sürgős.
A tárcák általában úgy működnek, hogy javaslatot tesznek arra, hogy a Bitcoin hálózat mindenkori telítettsége alapján milyen utalási díjat érdemes használni.

Mi a helyzet a Bitcoinok “nyomtatásával”, hogyan kerül új Bitcoin forgalomba?

Jelenleg kicsivel több, mint 19 millió Bitcoin van forgalomban. Tehát durván még 1.5 - 2 millió Bitcoin kerül forgalomba ameddig a bűvös 21 millió Bitcoin-t elérjük. Ez még kb. 113 év, azaz kb. 2136 körül érünk el arra a pontra, amikor új Bitcoin többé nem kerül a forgalomba. Hogyan lehetséges ezt ennyire pontosan megmondani? Ennek a magyarázata a bányászokhoz köthető.
A bányászok, amint sikeresen egy blokknyi utalást feldolgoznak és azt (csalás nélkül) a blokklánchoz “hozzáfűzik”, akkor az elvégzett munkáért (blokk) jutalomban részesülnek, mellé persze a blokkban szereplő összes tranzakció utalási díját is megkapják.

Blokk jutalom, na az most micsoda és ki adja? Ugye, hogy akkor van valamilyen vezető, aki ezt osztogatja?

Satoshi Nakamoto úgy találta ki a Bitcoin hálózatát, hogy az indulást követően, amikor lényegében semmit vagy alig ért valamit, akkor is a bányászokat valahogyan ösztönöznie kellett, hogy pénzt és energiát nem spórolva a tranzakciók ellenőrzésével foglalkozzanak. Erre egy speciális jutalmazási rendszert talált ki, amely a következőkből állt:

Esemény megnevezése	Blokkszám	Blokk jutalom	Dátum
Genezis block	1	50	2009. január 09.
Első felezés	210 000	25	2012. november 28.
Második felezés	420 000	12,5	2016. július 09.
Harmadik felezés	630 000	6,25	2020. május 11.
Negyedik felezés	840 000	3,125	2024. március - május (becsült)
Ötödik felezés	1 050 000	15,625	2028
Hatodik felezés	1 260 000	78,125	2032
.....	....	....	....
32. felezés	6 720 000	1	2136

Ahhoz, hogy a fenti táblázatot megértsük jó pár dologról kell beszélnünk. Az egyik ilyen a “Felezés”.
A “Felezés” (angolul: Halving), mint esemény minden 210.000 blokkonként történik. Az első felezés a táblázat szerint 2012. november 28-án történt, és a blokkonként járó 50 Bitcoin helyett a bányászoknak már csak 25 Bitcoin járt.
Mivel - ahogy említettem - a blokkláncra a blokkok 10 percenként kerülnek “felfűzésre”, így könnyen kiszámíthatjuk, hogy 210 000 x 10 = 2 100 000 perc = a “Felezés” kb. 4 évente van. Ezzel az egyszerű becsléssel azt is meg tudjuk mondani, hogy kb. mikor lesz a következő, illetve azt is, hogy kb. mikor lesz az utolsó.

Jó jó, de a táblázatban a dátumok nem 4 évente vannak, akkor most hogy is van ez?

A Bitcoin hálózat az emberi időt nem ismeri, azaz azt amit te dátumként gondolsz, illetve azt amikor az órádra nézel. :)
A Bitcoin hálózat “blokk időt” használ. Ahogy említettem a blokkláncban a sorrend egyedi és megmásíthatatlan, minden megoldott blokknak sorszáma van és ezek egymás után vannak “felfűzve”. Ezt a sorbarendezést a bányászok úgy végzik, hogy valójában nincs “időérzékük”, hanem a tranzakciók ellenőrzése mellett még egy igazán nehéz (számításigényes) feladatot is meg kell oldaniuk. Ez a feladat úgy van kitalálva, hogy a megoldása kb. 10 percig tartson.

Na és ki adja a feladatot, vagy hogyan találja ki milyen nehéz legyen, hogy a megoldása 10 percig tartson?

A nehézségi szint állítás

Élve az írói szabadsággal :) ennek külön részt szántam, mert véleményem szerint ez a funkció a Bitcoin hálózat legzseniálisabb találmánya. Miért tartom annak?
Ehhez azt kell elképzelnünk, hogy 2008-ban vagyunk a világgazdasági válság közepén, amikor Satoshi Nakamoto kitalálta, hogy a Bitcoint létrehozza.

Elsőre kvázi mindent tökéletesen vagy majdnem annak kellett megírjon, mert hiszen nincs központi rendszer, amit egy módosítással

javítani lehet, hanem az elkészített frissítést mindenkinek manuálisan egyénileg kellett az összes csomóponton végrehajtania, ami ráadásul mindmáig teljesen önkéntes alapon történik. Ehhez azért a csomópont üzemeltetői sok segítséget kaptak(nak).

Ami szerintem az indulás előtt a legeslegnehezebb feladat volt az az, hogy a rendszert “jövőbiztosra” tervezzék. Mit értek ez alatt?

A fejlesztő 2008-ban nem tudta előre megmondani, hogy 2018-ban, 2048-ban, 2140-ben stb. milyen bányagépek fognak létezni, illetve egyáltalán hányan fognak Bitcoint bányászni?
Márpedig a számítási feladatot “osztó” rendszert úgy kellett megtervezni, hogy a bányászok lehetőleg mindig minden nehéz feladatot 10 percenként oldjanak meg. Miért? Mert ez a számítási feladat csak azért van, hogy a blokkok fix időnként jöjjenek létre és ne véletlenszerűen másodpercenként vagy óránként történjenek. Magyarul egyfajta programozott rend legyen. Ezt központi irányítás és maga az idő fogalma nélkül a Bitcoin előtt nagyon nehéz volt elképzelni.

Ehhez kellett egy olyan algoritmust írni, ami annyit csinál, hogy 2016 blokkonként (kb. 2 hét) megnézi, hogy a blokkok között mennyi átlag idő telt el és a következő 2016 blokkra a nehézségi szintet ez alapján állítja.

Mitől függ, hogy a blokkok között több vagy kevesebb idő telik el?

Mivel engedély nélkül bárki Bitcoint bányászhat (az erre alkalmas gépekkel), így a hálózatról bármelyik pillanatban a bányász gépek egy része megjelenhet és akár el is tűnhet.

Például: Tegyük fel, hogy az elmúlt 2 hét (2016 blokk) a nehézségi szint 100 egységnyi gépnek a teljesítménye alapján van állítva és ezért ez a 100 egységnyi gép a feladatokat pontosan 10 percenként oldja meg, ezzel a blokkokat 10 percenként létrehozva és utalásokkal megtöltve.
Most tételezzük fel, hogy a világ másik végén, ahol 20 egységnyi gép üzemelt, tornádó söpör végig és az összes ottani gépet tönkreteszi. Ekkor a hálózaton 80 gép maradt és minden blokknál olyan feladatot kell megoldaniuk, ami 100 gépre volt tervezve. Mivel 20%-al kisebb a globális teljesítmény, ezért a 2016 blokkot átlagosan 12 perces "blokkidővel" oldják meg. Ekkor az algoritmus 20%-ot csökkent a nehézségi szinten, hogy a blokkokat a 80 gép a következő 2016 blokkra ismét 10 perces időközzel hozza létre.
Most képzeljük el, hogy valaki feltalálja a soha nem látott csúcs bányagépet. Olyan gépet, amiből 1 darab 100 (régi) egységnyi géppel ér fel. A teszt példányt azonnal hadrendbe állítja, és így a hálózaton hirtelen 180 (régi) egységnyi gép kezd el dolgozni.
Ekkor 2016 blokkot vizsgálva a blokk közötti idő 4 perc 27 másodpercre csökken, tehát az algoritmus a nehézségi szintet 2,25x-es mennyiségben növeli, hogy a blokkokat újra 10 percenként hozzák létre. Zseniális, ugye? :)

Ezáltal az egész hálózat működése (lásd pl. felezések) kiszámíthatóvá vált. Egy monetáris rendszer pedig akkor válik a leghatékonyabbá, ha segítségével minél könnyebben, minél pontosabb számításokat lehet végezni.

Az eddigiek és azt ezt követő szabályok vagy funkciók semmit sem érnének, ha ezt a nehézségi szint állítás, mint automata funkció, nem került volna bele. Miért?

A rendszer az indulását követően e nélkül és az újfajta bányagépek megjelenésével a blokkokat egyre gyorsabban generálta volna. Ezáltal a felezések nem kb. 4 évente történtek volna meg, hanem akár naponta. Így mondjuk 1 hónap alatt az összes 21 millió Bitcoint forgalomba állítva. Mi ezzel a gond?

A gond csupán annyi, hogy a Bitcoin bányászok mind a mai napig pusztán csak az utalási díjakból a 10 percre eső villanyszámlát nem tudják kifizetni (nem beszélve az egyéb költségekről). Így abban az esetben, ha a blokkjutalmak már nem lennének, akkor a bányászok a bányászatot hamar abbahagyták volna és csak nagyon kevés bányász maradt volna (akiknek még a kevés utalási díjért is megérne bányászni).

Kit érdekel, miért fontos az, hogy sok bányász legyen, amik ráadásul sok áramot is fogyasztanak?

Az 51%-os támadás

A Bitcoint érő lehetséges legveszélyesebb támadási forma, az úgynevezett “51%-os támadás”. Mit jelent ez?

A Bitcoin hálózatában, ahogy azt többször is említettem, nincs központi irányítás, így a működésében bárminemű változtatást a csomópontok programkódjának módosításával lehet csak elvégezni.

A tervező ezt úgy oldotta meg, hogy azt vette alap igazságnak, hogy “mindig a többségnek van igaza”. Tehát leegyszerűsítve, mindig az az “igazi” Bitcoin hálózat, amit a legtöbb, a bányászoknak min. 51%-a képvisel.

Ahhoz, hogy a szabályokat könnyen ne lehessen módosítani, a feltaláló zseniális módon ezt a lehetőséget a bányászok kezébe adta. Miért fontos ez?
A Bitcoin hálózatot vizsgálva ők azok, akik az indulástól kezdve a Bitcoint tartó személyeknél jóval nagyobb mértékben kockáztatnak. A teljes bányászati infrastruktúrát nekik kell kiépíteni: bánya- és egyéb gépeket vásárolni, üzemeltetni (pl. hosszútávú olcsó energiaforrást biztosítani) mindezt úgy, hogy a blokk jutalomért minden 10 percben versenyezniük kell (csak a leggyorsabb helyesen válaszoló kapja meg).
Ők azok, akik ha a Bitcoin bukik, akkor nem csak a már tulajdonukban lévő Bitcoin értékét veszítik el, hanem a bányászathoz vásárolt (jelentős befektetési hányadot képviselő), úgynevezett bányászó "célgépek" (angolul: ASIC miner) értékét is.
A gazdasági érdekeikből fakadóan a szabályok módosításába (ezáltal a Bitcoin működésének megváltoztatásába) csak akkor mennek bele, ha az elengedhetetlenül szükséges, és egyben a gazdasági érdekeik sem sérülnek.

Akkor most ki támad kit és hogyan? Mi is konkrétan az "51%-os támadás"?

Abban az esetben lehetne a Bitcoin hálózatot rövid vagy hosszú távra tönkretenni, ha ebben a támadásban az összes hálózaton lévő bányászati teljesítmény legalább 51%-a részt venne. Ha ez megtörténne, akkor a többség mondja meg "mi az igaz", és így lehetőségük lenne a hatalmukkal visszaélni.
A Bitcoin alapvető értékét adó struktúrája sérülhetne, és ezzel az értéke nagyon gyorsan a nullához közelítene. Mindenki, aki vagy

közvetlenül vagy közvetett módon a Bitcoin sikerességében érdekelt, az a befektetésének értékét elveszítené. Mennyire kell ettől félni?

2014-ben a Bitcoin hálózat számítási kapacitásában egy támadó több, mint 50%-os részesedést szerzett, amivel blokkokat blokkolt, és tranzakciókat vont vissza. A támadás mintegy 100 000 dollár kárt okozott.

Azóta elvi síkon kb. 2021 nyaráig ez valós veszély volt, mert a legsikeresebb Bitcoin bányagép gyártó cég kínai volt és egyben a bányászati teljesítmény több, mint 51%-a is Kínában volt. Miért csak 2021 nyaráig, mi történt ekkor?
A kínai kormány Kínában a Bitcoin bányászatot egy huszárvágással betiltotta. Ennek az lett a következménye, hogy ma már (2023) a kínai bányászati hányad (a tiltás ellenére) a teljes hálózat csak kb. 21%-a.

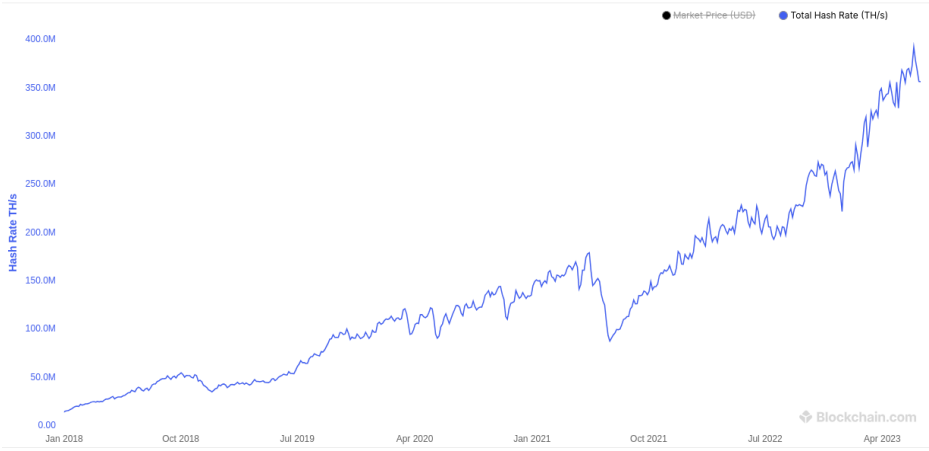
A kínai kormány ezzel a lépéssel egyértelműen a Bitcoinnak akart ártani, de valójában a Bitcoint ennél jobban nem is segíthette volna. Miért?
Egyszerűen azért, mert ameddig a gazdasági ösztönzők (rendkívül olcsó áram) miatt a Bitcoin bányászat nagy része ott összpontosult, addig ők kvázi egy kormánydöntéssel az irányítást ezen gépek felett átvehették volna és ezzel a Bitcoin működésébe belenyúlhattak volna.

Ezt a lehetőséget csúnyán elszalasztották, cserébe viszont velünk nagyon jót tettek, mert így a hálózatot igazán decentralizálttá tették.

A következő részben vizuálisan is megmutatom mennyire és milyen irányba változott a Bitcoin bányászata.

A Bitcoin decentralizáltsága

Először is, ha a Bitcoin decentralizáltságáról beszélünk, az összképet mindenképp meg kell néznünk. Hogyan növekszik a Bitcoin bányagépek teljesítménye, azaz hogyan növekszik a hálózat összteljesítménye?

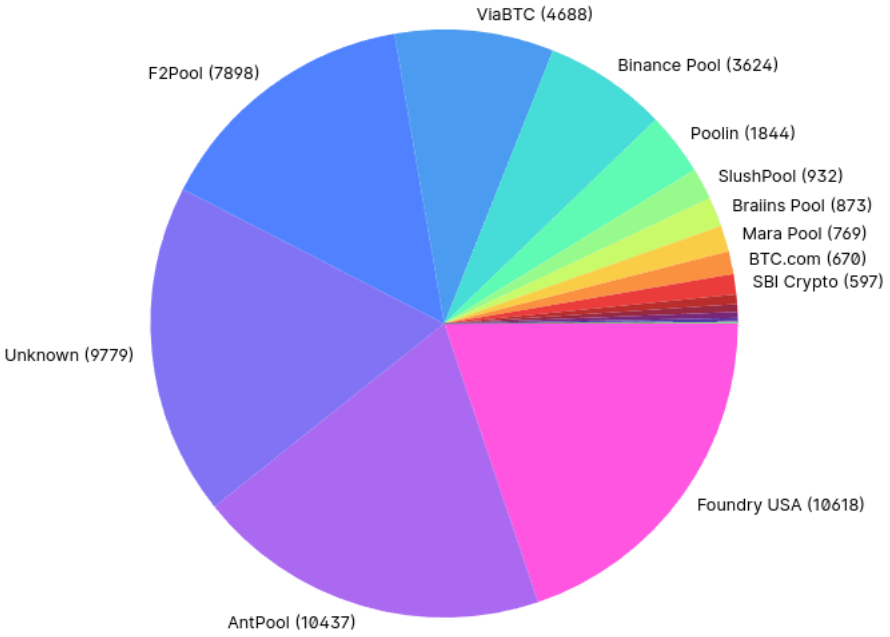


A fenti grafikonon jól látható, hogy az évek alatt hogyan emelkedik az össz Bitcoin bányászat teljesítménye és az is jól kivehető, hogy 2021 nyarán volt egy szabad szemmel is látható hirtelen esés, amit durván fél év alatt ki is “hevert”. Igen, ez volt az az időszak, amikor a kínai kormány (szerencsére) a Bitcoin bányászatot betiltotta.

A fenti grafikon a laikus számára semmit nem mond, ezért segítek elképzelni, hogy igazából mennyi gép is lehet a hálózaton?

A grafikon számait értelmezve azt látjuk, hogy a grafikon “TH/s” mértékegységet használ, ami “TerraHash” per másodpercnek felel meg.
Jelenleg kb. olyan 350 millió TH/s a teljesítmény van, ami elképesztően nagy szám elnézve, hogy 4 évvel ezelőtt kb. a hetede (!), olyan 50 TH/s körül volt. Hogy pontosan ez a szám milyen gépekből jön össze, azt nem lehetséges megmondani, csak különböző becslések vannak.

Amikor még bányásztam nekem 13,5 TH/s gépeim voltak, ami azt jelenti, hogy a fenti összteljesítményhez abból majdnem 26 millió darab kellene. Ha hozzávesszük, hogy egy ilyen gépnek kb. 1300W fogyasztása volt, akkor ez gigantikus, 33,7 GW energia (17,7 db paksi atomerőmű) fogyasztást jelentene.
Ugyankkor az emberiség minden téren fejlődik, ezért a ma (2023) kapható egyik legmodernebb gép teljesítménye 257 TH/s, így ebből már “csak” kb. 1,36 millió darab kellene. Ezeknek a fogyasztása kb. 5350 W ami azt jelenti, hogy ha a hálózatban minden gép ilyen lenne, akkor ez már csak 7,28 GW energia (3,8 db paksi atomerőmű) fogyasztást jelentene.
Az igazság valahol a kettő között van, mert mint mondtam a hálózatból azt, hogy az egyes bányászok milyen gépparkkal rendelkeznek nem lehet megtudni.

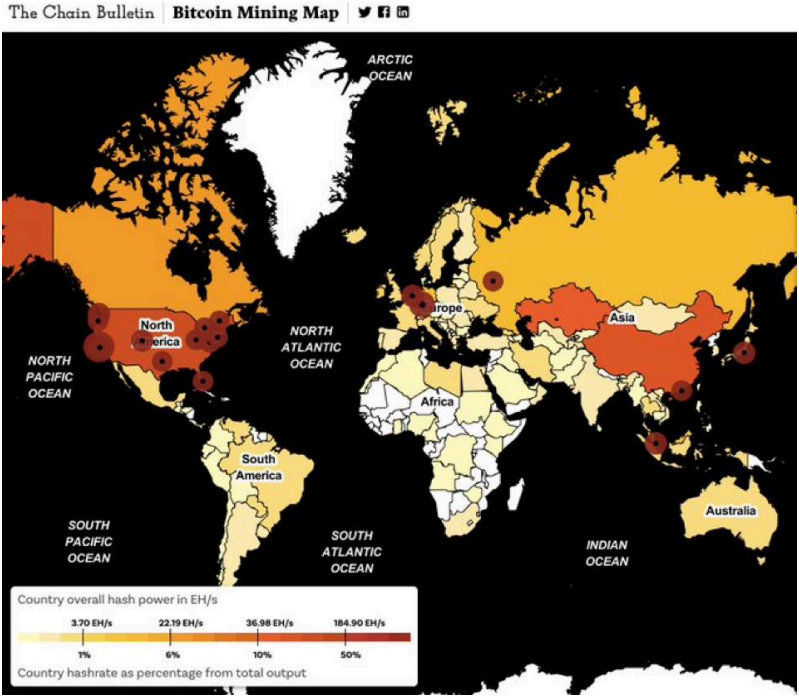


A fenti grafikon az elmúlt egy év (2022 nyara - 2023 nyara) alatt a bányászok által létrehozott blokkok eloszlását mutatja.
A Bitcoin bányászatra egész iparágak épültek, így mindenki a gépparkját az energiaforrás lehetőségeihez mérten alakította ki. Nagy részük publikus csoportosulások (tehát van egy konkrét cég/oldal, amin keresztül elérhetőek), de még mindig a hálózatnak kb. az ötöde teljesen anonim módon bányászik, akikről semmit sem lehet tudni.

Itt fontos megjegyeznem, hogy a fenti grafikon arányai lehetnek valósak és lehetnek teljesen mások is. Hogy lehet ez? Úgy, hogy amikor egy bányász egy blokkot befejez, akkor a “fejlécébe” beírja,

hogy ő az, aki létrehozta. A fenti grafikon ezekből a fejlécek adataiból készült.
Ha én nem akarom a gépparkom teljesítményét elárulni, akkor ezt a fejlécet üresen hagyom, és akkor az ismeretlenek közé leszek besorolva. Politikai okokból vagy “elbújás” céljával “behazudhatom” azt is, hogy én XY vagyok és a fejlécbe annak a nevét írom. A hálózat decentralizáltsága miatt ezt senki sem ellenőrizheti, illetve oda bármelyik bányász, bármit beírhat.

A blokklánc elemzésével foglalkozók azért általában azt mondják, hogy fent a valós grafikont látjuk, mert egyenlőre nincs ismert indok, amiért ide vagy oda érdemes lenne azt manipulálni.



A fenti publikus bányász csoportosulásokat - mivel ahogy említettem egy weboldallal (szerver IP címe alapján) vagy publikusan nyilatkozott helyszín (cég adatok) alapján- a globális térképen is el lehet helyezni. Mára jól látható, hogy a Bitcoin bányászat teljesen globálissá vált, ami viszont jó hír azoknak, akik politikai támadástól félnek. A globálisan szemben álló felek nem csak más fontos dolgokban, de a Bitcoin betiltásában sem fognak nagy valószínűséggel egyetérteni. Ebből kifolyólag a Bitcoin globális térnyerése (ezáltal további decentralizálódása) megállíthatatlan, mert a döntéshozókat a gazdasági ösztönzők abba az irányba tolják, hogy ahol sok olcsó (nem használt) áram van, ott azt a Bitcoin segítségével “pénzzé tegyék”.

Kiegészítés: A bányászat gazdasági és technikai részleteibe nem megyek bele, mert ez a könyvnek nem része, de annyit elárulok, hogy aki azon gondolkozik, hogy üzletileg Bitcoin bányászattal foglalkozzon azt a következőkkel kell elkeserítenem.
Amint a grafikonokon is látszik, a Bitcoin bányászat (iparosodott jellege miatt) nagyon összetetté és nehézzé vált, ami magával hozta, hogy hosszútávon csak olyan területeken éri meg bányászni, ahol nagyon sok felesleges energia van. Ökölszabályként elmondhatom, hogy Bitcoin bányászatról 0,04 USD (!) (kb. 14 Ft végponti) KWh áram fölött gondolkodni sem érdemes, mert nagyon nagy valószínűséggel a befektetés sohasem térül meg.

A tárcák és kulcsok szerepe

Banki analógiát fogok használni, mert azt sokkal több ember ismeri, mint mondjuk a PGP titkosítást. Ugye? :)

A Bitcoin tárca, legyen az egy alkalmazás a telefonon, számítógépen vagy egy erre a célra készített fizikai eszköz, olyan mint egy bankszámla, amit pinkódok és kétlépcsős azonosítók védenek.

Először is tisztázzuk, ezek a tárcák mit védenek? A tárcában lévő Bitcoint? Vagy mit?

A Bitcoin NINCS a tárcában, mert a Bitcoint nem úgy kell elképzelni, mint mondjuk egy digitális fényképet, ami a telefonodon van és azt egy gombnyomással tovább tudod küldeni. Ha így lenne, akkor semmi sem állítana meg, hogy ugyanazt ne csak 1 embernek küldd el, hanem még több embernek.
A Bitcoinok a blokkláncot valójában soha nem hagyják el, hanem a tárca egy utalásnál mindig csak annyit csinál, hogy a tulajdonjogot egy másik tulajdonosra írja át. Ezt, ha a bányászok jóváhagyják, akkor onnantól kezdve annak az adott Bitcoinnak új tulajdonosa lesz.

Ok, tegyük fel szerzek magamnak egy ilyen tárcát, hogyan működik?

A tárca első használatánál biztosítékként egy algoritmus 2048 darab angol szólistából 12 vagy 24 (szoftver függő mennyi) darab szót (angolul: “seed”-et) választ ki. Ezekkel a szavakkal tudsz bármikor a Bitcoinodhoz jutni. A tárca létrehozásánál ezek a szavak mindig véletlenszerűen vannak kiválasztva és az, hogy valaki másnak is ugyanazokat ugyanabban a sorrendben válassza ki szinte lehetetlen

(matematikailag elképesztően kicsi az esélye). Mik is ezek a szavak, de először is mennyire biztonságos ez az egész?

Egy kis matematikai kitekintő, hogy bebizonyítsam mennyire kicsi is annak az esélye, hogy egy tárca valaki másnak is ugyanazt a 12 vagy 24 darab helyreállító “seed” szavakat generálja ki:

Ahogy említettem egy algoritmus 2048 db angol szóból választ ki 12 vagy 24 db szót.
12 db szó esetében: $2048^{12} = 5.444517871 \times 10^{39}$ a lehetséges variáció.
24 db szó esetében: $2048^{24} = 2.964277484 \times 10^{79}$ a lehetséges variáció (némileg kevesebb, mert a 12. és a 24. szót a rendszer az előző 11 és 23 szó alapján választja ki).

Ahhoz, hogy “csak” a 12 db szót a helyes sorrendben “eltaláld” 1 milliárd db számítógép kell (!), melyek mind másodpercenként 1 billiót (1000 milliárdot) tippelnek (!), és így is 10 milliárd évre van szükségük.

Ezek olyan óriási számok, hogy összehasonlításképpen: ahhoz hogy egy pénzt 100 szor egymás után feldobva mindig “fej” legyen, annak 1 a 1.2676506×10^{31} az esélye. Mondhatni elég kicsi, hogy egymás után 100x “fej” legyen, de még mindig ennél 268 milliószor (!) nehezebb egy a tárcád által kiválasztott 12 db szót valaki másnak is a helyes sorrendben eltalálni/kitalálni.

Egy utolsó összehasonlítás: a Világegyetemben egyes becslések szerint 10^{78} - 10^{82} atom létezik. A 24 darab szó eltalálásának az esélye olyan, mint bárhol a Világegyetemben egy darab atomot megtalálni.

A szavakra tehát úgy kell tekinteni, mint egy “mesterkulcsra”, aminek segítségével, ha a tárcádat elveszted a Bitcoinjaidhoz bármikor, bármilyen másik tárcán keresztül hozzáférsz. Hogyan lehet ez?

Mint említettem, a Bitcoinjaid az adott eszközödön soha nem léteztek, hanem csak kvázi az “aláírásod”, az úgynevezett “privát kulcsod”. Mi is ez a privát kulcs?
A 12 vagy 24 darab szó egy algoritmus segítségével kigenerál egy hosszú betű és számsort. Ez lesz az úgynevezett privát kulcsod, és e mellé egy publikus kulcsot is kigenerál. Ez utóbbit pedig úgy kell elképzelni, mint a bankszámlaszám, amire az utalásokat tudod fogadni (nem konkrétan az, de hasonló).

Tehát, egyszerre bármennyi eszközt és szoftvert lehet a te 12 vagy 24 darab szavaddal “betanítani”, és onnantól kezdve a Bitcoinjaidhoz mindegyiken hozzáférsz. Ezért rendkívül fontos (!), hogy ezekhez a szavakhoz rajtad kívül senki se férjen hozzá, mert akkor a Bitcoinjaidat könnyen el tudják lopni.

A tárcádat - miután be lett “tanítva” - általában egy pinkóddal és még egy jelszóval is lehet védeni, hogy illetéktelenek a te privát kulcsodhoz ne férhessenek hozzá, azaz az utaláshoz (valójában tulajdonjog átruházáshoz) szükséges “aláírásodhoz”.

Lényegében pár perc alatt arra a pontra eljutsz, hogy van egy 12 vagy 24 szavas listád (ennek védelméről a negyedik fejezetben írok), egy privát kulcsod (elrejtve az alkalmazásban vagy fizikai tárcában) és egy publikus kulcsod.

Amikor utalást szeretnél kapni, akkor az adott tárca mindig a publikus kulcsod alapján megjelenít neked egy címet, amit bárkinek

megadhatsz és amire a Bitcoin utalásokat várhatod. Ezekből a címekből nagyjából végtelen generálható, ezért javaslom minden utaláshoz egy új címet használj (a legtöbb tárca mindig egy új üres címet ad), hogy a blokklánc esetleges elemzésével, ne lehessen hozzád egy vagy több utalást kötni.

Most ez miért is fontos? Miért használjak külön címet? Miért nem jó, ha csak 1 címet használok mindenre?

- Ha csak 1 címet használsz mindenre, akkor amikor te utalsz, a Bitcoin működésének sajátossága miatt (minden nyilvános a blokkláncon) elég csak egy címzettet beazonosítani, hogy hozzád is el lehessen jutni és ezzel az összes Bitcoin-od mennyisége is nyilvánosságra kerüljön.
- Bárki, akinek azt az 1 újrahasznált címet megadod az összes múltbéli és jövőbeli tranzakciódat láthatja majd és emellett - ami nagyobb gond -azt is, hogy összesen mennyi Bitcoinod van. Ebből kifolyólag NAGYON (!) fontos, hogy egy címet csak egy utalás erejéig használj és ha azt akarod, hogy valaki neked utaljon, minden egyes alkalommal új címet adj. Így elkerülve, hogy mások könnyen az összes Bitcoin-od mennyiségét megtudják.

A tárcákról bővebben a negyedik fejezetben írok.

A Bitcoin gazdasági ösztönzői

A szereplők résznél arról már beszéltem, hogy a Bitcoin gazdasági ösztönzői olyanok, hogy a játékszabályokat mindenki betartsa, ugyanakkor a rendszerben viszont, mindenki pótolható. Mit jelent ez?

Minden olyan fél, amely a Bitcoin működését elősegíti az valójában - egyénileg nézve- a Bitcoin működéséhez nélkülözhető, mert a Bitcoin számára senki sem pótolhatatlan. A Bitcoin a működését tökéletesen képes úgy folytatni, hogy mostantól bárki is a programkódjához hozzányúlna.

A Bitcoin egy olyan technológia, amely ugyanazon okból marad fenn, amiért a kerék, kés, telefon vagy bármilyen technológia, azaz a használatával a felhasználók számára előnyöket kínál.

A felhasználók, a bányászok és a csomópont-üzemeltetők a Bitcoin-nal való interakcióból mind gazdaságilag jutalomban részesülnek, a hálózatot ez harmónia tartja életben.

A Bitcoin-felhasználók tranzakciós díjakat fizetnek és a bányászoktól Bitcoint vásárolnak. Mindezt azért teszik, mert szeretnék ezt a digitális készpénzt birtokolni és használni (1), az értéknövekedését idővel élvezni (2), illetve majd utalások formájában a bányászok beruházásait finanszírozni (3).

Mint már említettem, a bányászok: a bányászati infrastruktúrába (pl. épületek, vezetékrendszer, szellőztetés, stb.), villamos energiába és bányagépekbe fektetnek be. Cserébe őket a jutalom (blokkjutalom és tranzakciós díjak) motiválja.

Na de félre ne érts, itt senki sem jószándékból vesz részt, hanem csakis önös érdekből! Ez fontos, mert a Bitcoin az egyedüli olyan gazdasági rendszer, ahol pusztán önös érdekből hozott döntések az egész rendszer minden résztvevőjét elősegítik. Hogyan lehet ez? Példának okáért, az arany esetében a bányászok önös érdeke, hogy

minél több aranyat bányásszanak. Ez teljesen logikus és érthető is, viszont ennek egyenes következménye, hogy a már kibányászott készletet elinflálják, ami elkerülhetetlenül az arany értékének csökkenésével jár (ezzel ártva az arany birtokosainak).
Ez viszont a Bitcoin esetében nincs így, mert a programozott kibocsátás a bányászok mohó érdekeinek abszolút gátat szab. Tehát a Bitcoin bányászok és a Bitcoin birtokosai között nincs ez az "ellenségeskedés", hanem mindenkit ugyanaz a cél vezérel, hogy a Bitcoin értéke a lehető legmagasabb legyen, mert akkor az a kicsi részesedés, amit a bányászok kapnak a későbbiekben sokat fog érni (FIAT valutában), illetve a birtokosok is természetesen ugyanezen okokból örülni fognak.

Ez egy olyan gazdasági rendszer, amely minden résztvevő számára eredményes és jövedelmező, ami viszont azt eredményezi, hogy a hálózat továbbra is elképesztő ütemben növekszik.

Az abszolút hiány

Satoshi Nakamoto volt az első és egyetlen, aki a Földön képes volt az abszolút hiányt feltalálni. A Bitcoin előtt sem digitális, sem fizikai valóban abszolút hiány nem létezett, magyarul olyan valós vagy virtuális "valami", amiből bizonyosan egy rögzített mennyiségnél nem lehet többet bányászni, készíteni.

A Bitcoin feltalálásáig a szűkösség mindig relatív volt, soha nem volt abszolút. Általános téves elképzelés, hogy bármilyen fizikai áru véges vagy teljesen ritka. Ezen áruk mennyiségének a korlátja, amely alapján bármely árut előállíthatunk, soha nem annak bolygón lévő előfordulása,

hanem az előállítására fordított erőfeszítés és idő volt a határa. (Erről bővebben az utolsó fejezetben olvashatsz.)

Pusztán csak a Bitcoin abszolút hiányossága miatt időről időre nagymértékben eladhatóvá válik. Miért? Gondoljunk csak a véges számú (eddig többet nem gyártott) járművekre, festményekre, régiségekre, amiknek az ára időről időre felfelé megy, főleg azok amikből csak pár darab van (pl. Ferrari 250 GTO - $70 000 000).

Az abszolút hiány és a nehézségi szint állításának segítségével a Bitcoin inflációs ütemét számíthatjuk ki:

Év	2009	2010	2011	2012	2013
Össz. Bitcoin	1,6M	5M	8M	10M	12M
Éves növekedés (%)		209,13	59,42	32,66	14,94
Év	2014	2015	2016	2017	**2023**
Össz. Bitcoin	13M	15M	16M	16,7M	**19,4M**
Éves növekedés (%)	12,06	9,93	6,8	4,35	**1,75**

A táblázat eléggé beszédes, mert jól látható, hogy 2023 nyarára már 19,4 millió érmét bányásztak ki, ami az összes létező érme 92,4% -át tette ki. A kínálat éves növekedése lényegében 6 év alatt, 4,35% -ról több mint felére (-60%), már csak 1,75%-ra esett vissza.

2024-ben a Felezést követőe, az össz készlet várhatóan, csak kismértékben növekszik (kb. 19,9M körül lesz), viszont ezzel szemben az idei évhez képest a kínálat éves növekedése 1,26%-ra csökken.

Hogy mindezeket perspektívába helyezzük, a következő kb. 25 évben a Bitcoin kínálat növekedése összesen olyan 7,5%-al növekszik, viszont hozzá képest az aranykészlet 52% -kal, a többi FIAT valutára pedig lehetetlen ilyen hosszú időtávban becsléseket mondani, mert a 2020-as pandémia két évében szinte elmebeteg módon “nyomtatták” a pénzt.
Matthew Mežinskis közgazdász, elemző az 1970 - 2022 időszakra a világ összes pénznemét vizsgálva átlagosan 13%-os éves monetáris bázis (pénzkészlet) bővülést (inflációt) számolt. (2001 kivételével, ahol 0% volt és 2019 ahol kb. 1% defláció volt.)
Ez úgy jött ki neki, hogy az összes nemzet bankjainak nyilvános adatait megszerezte és összegezte.
Érdekességképpen, a világon 1970-ben még összesen $150 milliárd USD összértékű pénz volt forgalomban, 2023. áprilisában ez a szám $28,18 billió USD (28 180 milliárd) volt.

Magyarul, a világon az elmúlt durván 50 év alapján átlagosan kevesebb, mint 6 évente (kamatos kamat számítás miatt) a forgalomban lévő pénzkészlet megduplázódik (!).

Összehasonlításképpen, a 2017-ben megjelent The Bitcoin Standard könyv a FIAT valutáknál, az alábbi becsléssel számolt:

- Az elkövetkezendő 25 évben (2017-hez képest) a japán jen 64% -kal, a svájci frank 169% -kal, az amerikai dollár 272% -kal, az euró 286% -kal, a brit font pedig 429% -kal növekszik.

Tehát összefoglalva, míg a FIAT valutáknak a forgalomban lévő pénzmennyiségük folyamatosan növekszik és ezáltal a vásárlóerejük csökken, addig a bitcoin a valós vásárlóerő jelentős mértékű növekedését tapasztalta. Mindezt nagyrészt annak köszönhette, hogy kínálatának bővülése folyamatosan csökkenő trendben van (lásd táblázat) és abszolút korlátos is (max. 21M Bitcoin).

Bónusz: A tranzakciókat hitelesítő bányászokat bitcoinokkal jutalmazzák, ezért ezeknek a bányászokna, a hálózat integritásának fenntartásához komoly érdeke fűződik, ami viszont ugyancsak a Bitcoin értékét növeli.

A Bitcoin volatilitása

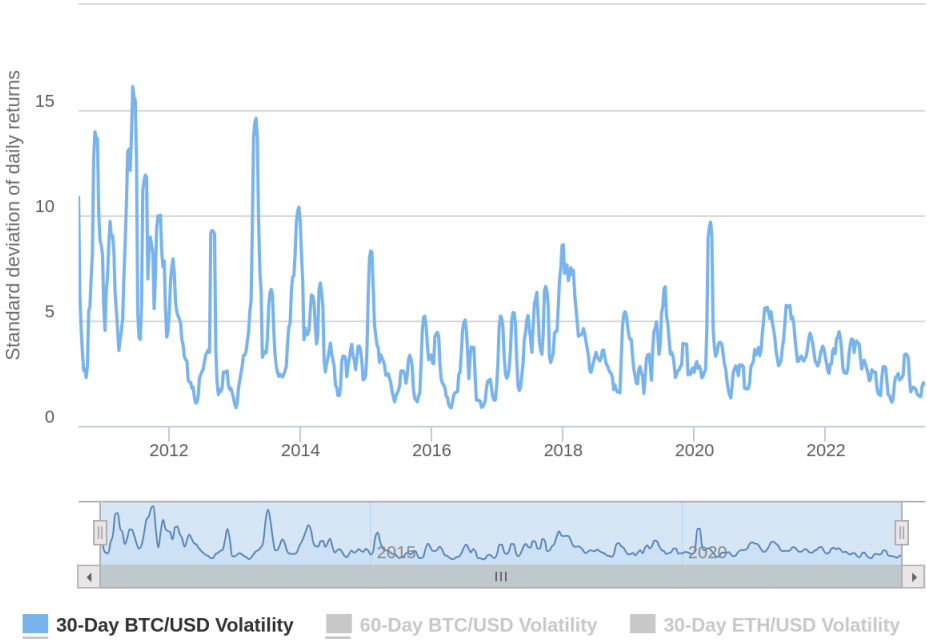
Az abszolút korlátosság, a gazdasági ösztönzők, mind az árfolyam kiugró változására (volatilitásra) komoly hatással vannak. A külső tényezőkről (pl. Kínában betiltották) nem is beszélve.
Ezekre a Bitcoin árfolyama nagyon rugalmatlanul válaszol. Magyarul, mivel a készlete véges és kiszámítható ütemben növekszik, ebből fakadóan a volatilitása jelentős lehet, ha esetleg valamilyen váratlan negatív/pozitív hír jelenik meg róla.

Miben különb, mint egy másik árucikk, részvény, FIAT pénz stb. esetében?

Bármely szokásos árucikk esetében az áruk gyártóinak termelési döntéseit a kereslet változása befolyásolja.

Magyarul, a kereslet növekedése növeli a termelésüket ezzel az áremelkedést mérsékelve, cserébe viszont lehetővé téve a jövedelmezőség növelését.
Abban az esetben, ha a kereslet csökken az a kínálat csökkenéséhez vezet, ez pedig lehetővé teszi a veszteségek minimalizálását.
A FIAT valutáknál a különböző központi bankok hasonlóan manipulálnak, ahol a monetáris politikájuk változtatásával próbálják a piaci ingadozásokat ellensúlyozni.

A Bitcoin volatilitása hogyan alakul?



A előző ábra a Bitcoin-kereskedelem 2011 - 2023 között a BTC/USD árfolyam 30 napos szórását mutatja.

Jól látható, hogy a kezdeti extrém volatilitások kezdenek megszűnni és ahogy a Bitcoin egyre nagyobb “tömeget”, azaz értéket vesz fel a volatilitása úgy lesz egyre kisebb. Ez még nagyon csekély időszak, hogy ebből messzemenőkig terjedő következtetéseket vonjunk le, de a későbbiekben pár Felezés után már tisztább trendet fogunk tudni felállítani.

A Bitcoin bukásának útja

“Hatásvadász” cím, amit választottam, mert ezt biztosan mindenki el fogja olvasni. :)

A Bitcoinnak az elsődleges támadói a központi bankok és azok szolgálói. Nekik évszázadokig nem voltak versenytársaik és a pénzzel azt csinálhattak, amit csak nem szégyelltek.

A Bitcoin megjelenését követően, bárki számára olyan szolgáltatásokat nyújtott, amellyel a Föld bármely pontján végleges elszámolást tett lehetővé mindezt alacsony költségekkel és harmadik fél jóváhagyása nélkül.
A kiszolgáltatott embereknek mentőcsónakként funkcioná, a kormányok folyamatos sarca (adók) és a pénz elértéktelenedését okozó inflációval szemben is. Nekik és mindenki másnak is a Bitcoin hosszútávú értéktárolóként és egy szuverén pénzformaként szolgál.

A bukása akkor következhetne be, ha az emberek vagy találnának egy jobb funkciókkal ellátott pénzeszközt, vagy a fenti előnyök nem lennének elég “kecsegtetőek” és lassan a használatát elhagynák.

Ezzel lassú (vagy gyors) kereslet csökkenéssel az ára hosszútávon esne és így nem érné meg bányászni, amivel pedig elveszítené a csalás és visszaélések elleni stabil védelmét. Végül a FIAT pénzrendszer eltörlésének egy újabb sikertelen próbálkozásává halványulna.

Mi van, ha valakinek (mondjuk a kormánynak) kvázi végtelen pénze van? Pénzzel el lehet pusztítani?

Ahhoz, hogy a Bitcoint elpusztítsa vagy csalásokon keresztül megbuktassa nagyon nagy összegeket kellene megmozgatnia anélkül, hogy az egyáltalán megtérülne!
Tegyük fel, hogy a pénz nem számít és a bányászaton keresztül a Bitcoin hálózatot célba veszi. Tegyük fel, hogy valami csoda hatására sikerül is neki, ekkor csak arra van szükség, hogy a “kisebbség” (a becsületes bányászok) visszatérjenek a támadás előtti blokklánc állapotához, hogy a Bitcoin csalás nélküli működése biztosítva legyen.

De hát ez hogy lehet? Nem azt mondtad az 51%-os támadásnál, hogy a többségi teljesítmény mondja meg mi az igazi hálózat?
Igen, de a hálózat használói nagyon rövid úton értesülnének arról, hogy valaki a hálózaton az irányítást csalárd módon átvette. Ekkor a gyors technikai módosítások következtében (pl. a csaló bányászok hálózatának kizárásával) az úgynevezett elcsalt blokkokat ki lehetne “dobni”. Hogyan? Úgy, hogy a nagy többség, akiknek az érdekei a csalóéval ellentétesek, a csomópontok szoftverét egyöntetűen módosítanák (hisz a közös érdekeik ezt kívánják). A csaló természetesen újra próbálkozhat, de a támadás kitartása irgalmatlan költségekkel jár.

Ma mennyire drága lenne a Bitcoin hálózatát elméletben tönkretenni?

Egyes számítások szerint (2023. jún-i adatok alapján) az 51%-os támadáshoz majdnem 1 millió darab bányagép kellene a legmodernebb, legjobb teljesítményű változatból, ami $7,9 Milliárd USD-ba kerülne + a tárolásukhoz szükséges építmények + kiegészítő egységek + személyzet + hűtés rendszer és nem utolsó sorban az áram.
Az áram igény igazán gigantikus, 1 millió x 5 350 W = 5 350+ MW áramra lenne szükség, ami csak a gépek üzemeltetése és nem tartalmazza a kiegészítő dolgok pl. szellőztető rendszer hatalmas fogyasztását. Ennek a költsége óránként (átlagos amerikai áram díjjal számolva) 0,23 USD/KWh, tehát 5 350 000 x 0,23 = 1,2 millió USD / óra. Nem tűnik egetverően soknak, pl. USA kormány szinten és nagy valószínűséggel a támadás költségét maguknak hónapokra megengedhetik.

Akkor mégis a kormányokat mi tartja vissza?

Az hogy, a valóság nem egyenlő egy kockás füzetnek megfelelő számolással, mert ezeknek a gépeknek a legyártása évekbe kerülne (ami alatt a becsületes bányászok száma tovább nőne, ezzel is a támadás költségeit és időpontját kitolva).
Az építmények felépítése és a hozzá kisajátított erőmű átszervezése is jelentős időbe és költségekbe kerülne.
Ahogy fentebb állítottam, a szoftver egyöntetű módosításával ezt a támadást (csaló blokkokat) relatíve könnyen kizárhatóvá lehetne tenni (akár egymás után többször).

Ezzel szemben a kormány, ha úgy döntene, hogy csalás helyett inkább “beszáll” és Bitcoint termel, akkor a blokkok legalább felének feldolgozását megszereznék, ami azt jelenti (2023. júniusban), hogy

144/2+1 = 73 blokk / nap = 73 x 6,25 x $30 000 = $13 687 500 napi (!) bevétel (+ ezen blokkokban található összes tranzakciós díjak). Azért ez mindjárt jobban hangzik, mint a csalás esetében “csak” az áramdíjra “ellocsolt” legalább napi (!) 28,8 Millió USD költség. Természetesen a bányászat a jelenlegi árfolyamon még mindig naponta $15 112 500 veszteséget termelne, de mégsem $28,8 milliót. A későbbiekben pedig (a támadással ellentétben) a kibányászott Bitcoin árának további emelkedésével (ha a kormány nem kényszerűl eladásukra) a befektetett összeg akár többszörösen is megtérülhet.

Állami szinten a Bitcoin bányászat nem csak gazdasági érdek, hanem stratégiai is, hisz amennyiben a későbbiekben organikusan fejlődve (lásd történelmi pénzek) a Bitcoin lesz a vezető nemzetek közötti elszámolási egység, akkor jó ha az adott országnak van “néhány” Bitcoinja. Nem említve a potenciális jelentős árfolyam emelkedés esetén bekövetkező számottevő haszonról.

Nem léphetünk tovább a Bitcoin decentralizáltsága résznél írt “keretes” mondandóm újbóli megemlítése nélkül: Ezen példa is jól szemlélteti, hogy míg állami szinten a fent számolt veszteség (a 0,23 USD/KWh áram miatt) és stratégiai okok miatt még elviselhető lehet, addig ez egy gazdasági társaság esetében abszolút csődöt jelent.

A fenti számok az általam javasolt maximum 0,04 USD/KWh áram árral + 51%-os hálózati teljesítménnyel = $5 136 000 napi áram költség, de ami még érdekesebb, hogy a bányászat ez esetben már $8 551 500 napi profitot (!) termelne.

A Bitcoin energiaéhsége

Először is a Bitcoin becsült energiaéhségéről a Bitcoin decentralizáltsága résznél már írtam, amit pusztán a gépek teljesítményéből becsültem meg.
Napjainkban elég tág határok között olyan 7,28 - 33,7 GWh fogyasztásról beszélünk. Nagyon sok pontosabb becslés is van, de az igazság az, hogy a lehetséges részrehajlás miatt egyik sem győzött meg.

A kérdés tehát, hogy a Bitcoin energiafogyasztása jogos-e vagy sem?

Tegyük fel ezt a kérdést egy kicsit átfogalmazva (árnyaltan):
Mi a fontosabb pl. a téli karácsonyfafüzér vagy az otthoni szárítógépek vagy a Bitcoin bányászata? Ezek globálisan kb. ugyanannyit fogyasztanak.
Először is kinek van joga ezt eldönteni? Nekem? Neked? Manci néninek a 7. emeletről? A “jachtos” palinak? A kormánynak?

Segítek a válaszadással: Annak, aki azt a bizonyos villanyszámlát kifizeti. Mindenkinek egyéni joga (kellene legyen) eldönteni, hogy azt az áramot, ami a konnektorból “kijön” mire használja, hisz ennek a számláját ő fizeti be.

Na, de a gépek: “felforralják az óceánt”, globális felmelegedést okoznak, az áramot előlem elhasználják, miattuk lesz drágább az áram stb. kijelentéseket lehet mindenfelé olvasni, de ezek mind sületlenségek (későbbiekben megindoklom). Na, de akkor nézzük csak meg, hogy ha - ahogy fentebb írtam - a Bitcoin gazdasági ösztönzői

olyan jól működnek, akkor ezen a téren, mármint az energia szabályozás terén hogyan működnek?

A bányászok részéről a verseny a Bitcoin blokkokért egyre durvább, ahogy a decentralizáltságnál bemutatott grafikon látványosan bemutatja. Miért releváns ez? Ez azért fontos, mert ebben az esetben a bányász azért, hogy “játékban” legyen, azaz a következő blokk feldolgozásáért és az ebből adódó jutalmakért kellő eséllyel induljon állandóan, akár év közben nagyon komoly optimalizációkat kell végeznie.

Az adott bányásznak vagy extrémen olcsó áramot kell használnia és/vagy extrémen hatékony bányagépeket. A győztes egyértelműen az, aki mindenkettőhöz hozzáfér, mert kellően nagy teljesítménnyel bányászik, kellően nagy hatásfokkal, hogy amikor a Bitcoin piaci ára alacsony,ő ő akkor is a gépeit profittal tudja üzemeltetni. Viszont a Bitcoin bányászat nem ennyire egyszerű (szerencsére?).

Általában az olcsó áram nagyon elhagyatott helyen van (azért olcsó, mert nincs ki megvegye vagy túl kevés vevő van) és a jó hatásfokú bányagépek pedig nagyon drágák. Aki pedig vezetett már céget az tudja, hogy ahhoz nagyon pontos tervezés kell, hogy a várható bevétel (itt blokkjutalom + tranzakciós díjak) tartósan több legyen, mint a kiadások (áram, eszközök, személyzet, stb.).

Tapasztalatból mondom, hogy ameddig úgy tűnik, hogy a “kifizethető” áramot megtaláltad (1), a szükséges infrastruktúrát (épület, vezetékek, szellőztetés, felügyeleti rendszerek stb.) kiépítetted (2), a viszonylag “jó” hatásfokú bányagépeket (+ kifizetted rá szállítást, vámot+áfát) beszerezted (3) és ezeket elkezdted üzemeltetni (4), nagyon rövid idő alatt meglepetésben lehet részed.

Vagy úgy, mint az én esetemben, hogy a kormány majdnem egyik napról a másikra az áram díját duplázza és ezzel a matek teljesen megborul (csőd) vagy egyszerűen a piac rajtad “túlfejlődik”. Mit jelent ez utóbbi?

Ahogy a piac egyre többszereplős lesz és a blokkokért egyre jobb hatásfokkal (olcsóbb áram + jobb gépek) bányászók versenyeznek, úgy a másik végén a legrosszabb hatásfokkal bányászók (drága áram + rossz hatásfokú géppark) “kiesnek”, mert a költségük több lesz, mint a bevételük.

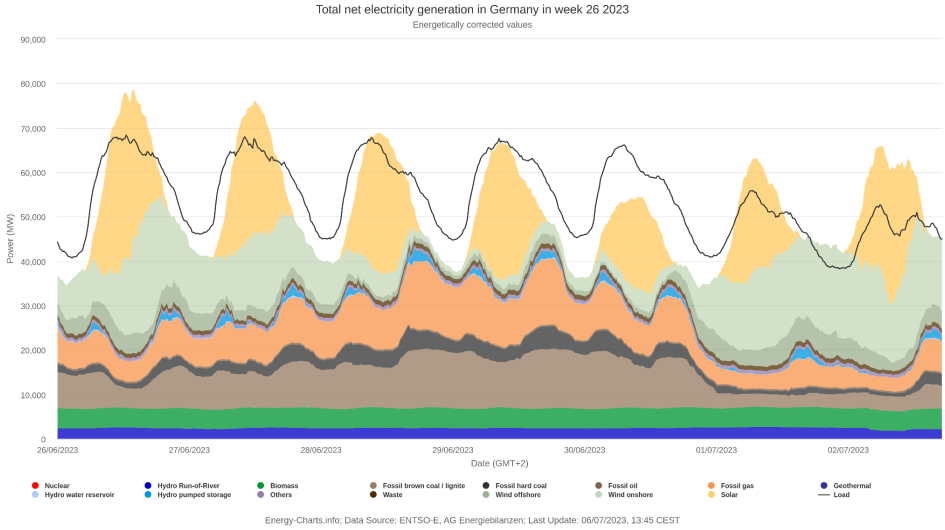
Kik lehetnek azok, akik hónapról hónapra az emelkedő verseny miatt kiesnek?
Nehéz ezt konkrétan megmondani, de ahogy már említettem, ott ahol sok a fogyasztó, ott ahol ha energiahiány van, akkor az áram nagyon drága (lásd pl. városok). Ott viszont, ahol valami oknál fogva csökken vagy megszűnt a fogyasztás (pl. elvándorló népesség, csődbe ment gyár stb.), ott az áram nagyon olcsó. Ma már nincs olyan ipari méretben Bitcoint bányászó cég, aki drága áramot használna (0,04 USD/KWh felett erősen biztos a csőd), tehát te nálad a városban az áram díját biztosan nem fogja felverni, mert ott eleve már rég nem éri meg bányászni.

A Bitcoin gazdasági ösztönzőinek és a beépített verseny miatt a bányászat nem csak a városokat kerüli el, hanem akár egyik napról a másikra országokat is. Ez egy globális pénznem, ami magával hozza, hogy a szabad olcsó áramforrásért az egész világot megversenyezteti. Ebből kifolyólag bizonyosan állítható, hogy az egyén életére, mint árfelhajtó erő nem fog megjelenni. SŐT! Itt jön a meglepő fordulat! A

Bitcoin bányászata, akár nekünk magyaroknak (és más nemzeteknek is) árcsökkentő hatással is lehet. Hogyan?

Amellett, hogy egyes becslések szerint 2023-ban a Bitcoin bányászata már több, mint 52.4%-a megújuló energiából származik, egy nagyon fontos szerepet még el tud látni, amit sok helyen (pl. Texas) már aktívan ki is használnak. Ez pedig nem más, mint a terhelés kiegyenlítése.

A megújuló energia, bővebben a szél és a nap attól függetlenül, hogy messzemenőkig alig termeli meg a bekerülési (gyártás + telepítés) energia igényét, az energia hálózatot még elképesztően destabilizálja is. Erre példa Németország, ahol a megújuló (szél és nap) energiatermelés miatt nagymértékű a kitettség.



A fenti grafikonon szabad szemmel is jól látható, hogy a napi energiatermelés nagyon durván kiegyensúlyozatlan. Van olyan nap,

hogy a nappal és az éjszaka között a különbség több, mint duplája. Ezt a különböző elosztó központokban elképesztően nehéz menedzselni, mert nem csak az a probléma, ha nincs áram, az is gondot okoz, ha valamikor túl sok van. Az időjárás kiszámíthatatlansága miatt ez a helyzet hatványozottan okoz károkat. Olyan, mint egy időzített bomba és ez nem túlzás, mert csak az elmúlt években többször másodpercekre volt Európa (nem csak Németország), hogy teljes áramkimaradás legyen (link a Forrásoknál).

A Bitcoin ezzel szemben a túltermelést és az esetleges alultermelést is ki tudja egyensúlyozni. Hogyan? Pusztán csak a piaci árazással. A Bitcoin géppark sajátossága, hogy perceken belül le és be lehet kapcsolni. Ezt egy energiatermelő erőműnél csak nagy időeltolódással és/vagy magas költségek árán lehet megtenni.
Tehát elmondhatjuk, hogy az energiatermelés rendkívül rugalmatlan, míg a Bitcoin bányászat rendkívül rugalmas tud lenni, így a kettő nagyon jól kiegészíti egymást. Hogyan?
Amennyiben egy valós időben való piaci árazást bevezetünk, úgy amikor nagy az energiaigény és hozzá kevés az áramtermelés (ergo felmenne az áram díja), akkor ezt a Bitcoin bánya rendszer érzékeli és amikor eléri a gazdaságilag “már nem éri meg” bányászni szintet egyszerűen kikapcsol és ezzel a lefoglalt áram mennyiségét felszabadítja, így csökkentve a hálózat terhelését és egyben a hálózat bővítésének lehetőségét is gazdaságilag biztosítva (a még nem használt új energia mennyiséget Bitcoin bányászatra lehetne fordítani, amiből a szolgáltató profitot termelne).

Ez nem utópia, ez már több helyen - köztük a már említett Texas-ban (közelről követtem) - évek óta működik. Olyannyira sikeres, hogy a nyári hőségben és a téli fagyban, amikor a lakosság sok klímát/elektromos fűtést üzemeltet már zsinórban két év úgy telt el,

hogy a fent leírt bányászok által biztosított kiegyensúlyozásnak köszönhetően nem volt áramszünet.

Ezeken kívül az áramot valójában még a lakosság számára is olcsóbbá tudja tenni. Hogyan? Azáltal, hogy egy erőmű építésénél már az indulástól számítva fix stabil fogyasztóval lehet tervezni a megtérülése kvázi biztosítva van és így a későbbiekben becsatlakozó extra fogyasztók számára már egy jelentősen olcsóbb árszintről indulva alkudoznak. Íme erre egy példa:
Játszunk el a gondolattal, hogy egy atomerőmű mondjuk 5 Ft / KWh bekerülési áron tud áramot előállítani. Amennyiben azt mondja a Bitcoin bányász cég, hogy biztos 10 Ft-on átveszi, az építkezés így azonnal megkezdődhet. Hogy lesz ez a lakosságnak olcsóbb? Az atomerőmű építői és üzemeltetői nem hülyék, ha tudnak ugyanazért 10 Ft helyett 20 Ft-ot elkérni, akkor annyit fognak. Márpedig nagyon valószínű, hogy a lakosság a 20 Ft-ot tartósan ki tudja fizetni, de egy Bitcoin bányász cég már nem.
Ekkor a lakosság jól jár, mert az örökké növekvő energia éhsége olcsó energiával lett csillapítva, ami a társadalom fejlődéséhez elengedhetetlen, viszont a Bitcoin bányászok sem feltétlenül jártak rosszul. Nagyon sok olyan időszak van, amikor a lakosság kevesebbet használ, bányászni azokban az időszakokban is be tudnak csatlakozni. Amint pár bekezdéssel ezelőtt írtam, ameddig nincs elég új fogyasztó (ez lehet évek), addig az új erőmű felesleges kapacitását Bitcoin bányászatra is tudják használni. Ez egy amolyan win-win helyzet, mert az erőmű, a bányászok és a majdani lakosság is jól fog járni.
Egy dolgot viszont ne felejtsünk el: az energiatermelést csak lassan és/vagy nagy költségek árán lehet “le-fel tekergetni”. Ezért a bányászok, mint stabil állandó felvevőkör, még további termelési költségcsökkentéssel tud járni, ami a lakosság részére az áram árában további árcsökkenést eredményezhet.

Ez a fejezet (szerintem) abszolút bizonyította, hogy a Bitcoin, mint sok egyéb területen az energiaszektorban is tud pozitív szerepet játszani.

A Bitcoin “rétegei”, jövőbeli skálázhatósága

Adott a Bitcoin maximálisan 2 MB körüli blokkjai és ehhez a kb. maximum 500 000 napi tranzakció. A napnál is világosabb, hogyha a Földön mindenki ezzel akarná csak a reggeli kávéját kifizetni, akkor az bajosan sikerülne vagy csak napok, hetek alatt.

Téves feltételezés tehát, hogy a Bitcoin a VISA, Mastercard, PayPal és társai ellenfele, mert a Bitcoin valójában, ahogy eddig már többször említettem a következő értéktároló eszköz, aminek a napi pénzforgalom lebonyolítása, NEM elsődleges feladata.

Most, hogy ezt tisztáztuk azért ne essünk kétségbe, mert a Bitcoin fejlesztői a megoldást, erre a problémára is megtalálták.
Újabb “rétegeken” dolgoznak, amik viszont többek között az azonnali utalásokra lettek kifejlesztve. Én ebben a könyvben ezek közül csak a legismertebbet, a Lightning Network (LN - Villám Hálózat)-ot fejtem ki.

Ezt a “második rétegen” alapuló hálózatot úgy kell elképzelni, hogy a már bemutatott Bitcoin hálózattal párhuzamosan működik. A kettő egyáltalán nincs összekötve, tehát kvázi nincs közük egymáshoz.

Az LN lényegében csomópontokból áll, amikhez egy vagy több tárca tartozik. A csomópontok egymással interneten keresztül kommunikálnak és az utalások is ezen a kommunikáción keresztül

történnek. Ahhoz, hogy senki se tudjon csalni, na meg ne legyen ilyen “tartozom neked” meg “beccszó megadom” helyzet, a csomópontok egymással “szerződéses viszonyban” állnak, amit a Bitcoin hálózata garantál.

Hogyan is kell ezt a “szerződéses viszonyt” elképzelni?

Tegyük fel, hogy én egy ügyvéd jelenlétében szerződést kötök veled és az ügyvédnél 1 millió forintot letétbe helyezek. A szerződés szerint abban állapodunk meg, hogy ameddig a szerződést életben tartjuk (bármelyikünk bármikor felmondhatja) addig 1 millió forintig azonnal bármikor tudok nálad vásárolni. Nem kell megvárni ameddig az utalás egy Bitcoin blokkba belekerül, hanem te a vásárlás ellenértékét, azonnal visszavonhatatlanul levonod.

A fenti szituációnál maradva tegyük fel, hogy nálad 40 000 Ft-ért vettem egy cipőt. Ekkor te az 1 millió forintból 40 000 Ft-ot levonsz és ezután nálad 960 000 Ft-nyi “keretem” maradt. Viszont ugyanez a szerződés arra is lehetőséget kínál, hogy a nálad lévő pénzből nálam is tudj vásárolni. Tehát 40 000 Ft-ig, ameddig a szerződés életben van, nálam is tudsz ugyanúgy vásárolni.

Az egész itt nem ér véget, hiszen neked is más emberekkel/cégekkel is vannak szerződéseid és tegyük fel egyike a ferihegyi reptéren lévő kávézó. Én épp ebben a kávézóban vagyok és fizetni akarok. Sajnos nekem ezzel a kávézóval nincs szerződésem, de rajtad keresztül viszont tudok fizetni. Én kifizetem neked a kávé árát. Te levonod a maradék 960 000 Ft-ból és a pénzt a kávézónak tovább küldöd. Az egész hálózat valahogy így néz ki:

Persze te ezt nem ingyen teszed, mert az én kávém árával a kávézóval kötött szerződésed keretét miért csökkentenéd ingyen, ha neked ehhez gazdasági érdeked nem fűződne. Itt jön a képbe a jutalék. Minden rajtad átmenő forgalomból a résztvevőkkel megbeszélt módon a “fáradtságodért” egy kis jutalékot “lecsípsz”.

Ez a szerződéses viszony technikai úton történik komoly titkosításokkal, a csalás teljes kizárásával. Az ügyvéd maga a Bitcoin hálózat, ahol egy ilyen szerződés létrejöttéhez valós Bitcoin utalás szükséges. A modern kriptográfia segítségével lehetőségünk van kettőnk között a szerződést bármikor felbontani és az épp aktuális elszámolás állása alapján mindenki a neki járó pénzt megkapja (egy Bitcoin utaláson keresztül). Csalni nem érdemes, mert a rendszer úgy van felépítve, hogy a lebukás szinte 100%-os és ebben az esetben a szerződésben foglalt, teljes rád eső részt a másik fél irányába elveszíted.

Miért érdemes az LN-el foglalkoznod?

Azért, mert ameddig mindenki azt hangoztatja, hogy a Bitcoin ilyen lassú, olyan korlátai vannak, addig mindezekre a “2. rétegen” az LN megoldást kínál. Mit tud ez a rendszer?

Jelenleg (2023. nyara) 5 426 Bitcoin van “ügyvédi letétben”, azaz szerződésekkel a hálózaton lekötve. Ez durván 162 millió USD értéket képvisel. Becslések szerint a hálózaton kb. 20 000 olyan csomópont van, amely 70 000 publikus szerződéssel rendelkezik (lehet privátot is kötni és akkor arról csak a két félnek van tudomása).
Mivel ez a hálózat központi egységgel nem rendelkezik (úgy, mint a Bitcoin az első rétegen), ezért ez a csomópont és szerződés mennyiség csak egy becslés, valójában jóval több van.

Mondhatnád, hogy ne már, most ezt csak 20 000-en használják?
20 000 ember 8+ milliárd lakoshoz képest semmi.

Ez nem így van! A hálózaton 20 000 a becsült LN csomópont mennyisége de, mint az elején írtam egy csomóponthoz egy vagy több tárca is tartozhat.
Egy csomópont, mint pl. a “Wallet of Satoshi” - ami egy bárkinek (akinek van egy email címe) LN tárcát biztosító szolgáltatás - egyedül több százezer felhasználóval rendelkezik és már túl van a 10 millió azonnali tranzakción is.
Nagyon sok hozzá hasonló “nagy” LN csomópont (pl. tőzsde) van, olyanok, akik milliós felhasználó bázissal rendelkeznek. Ezek tehát mind 1-1 csomópont ebből a 20 000-re becsült mennyiségből, szóval az LN “lefedettsége” mondhatni már most is tízmilliós nagyságrendű úgy, hogy még csak egy 5 éves technológiáról beszélünk.

Milyen gyors is ez a rendszer, mennyire “azonnali” az a fizetés?

Lényegében pár másodperc (1-2) ameddig egy ilyen azonnali utalás normális esetben megtörténik, de technikai okok miatt ez lehet valamivel több (mondjuk max fél perc).

Mennyi ilyen utalásra képes a rendszer?

A Bitcoin “első réteg” napi 500 000 utalásához képest, ami olyan 7 utalás/másodperc, ezen a rendszeren keresztül kb. 1 millió tranzakció/másodperc lehetséges. A VISA és a Mastercard együtt csak olyan 30 000 tranzakció/másodpercre képes.
Jelentős ugrás, amivel a Bitcoin globálisan, mint mindennapi pénzként való használata kvázi megoldódott.

Mennyire biztonságos ez a hálózat, mondjuk a Bitcoin “első rétegéhez” hasonlítva?

Az első réteghez képest kevésbé biztonságos, mert a csalást elméletben lehetséges úgy kivitelezni, hogy ha minden “összeáll”, akkor a pénzünkkel a szerződésben lévő másik fél megléphet.
Miért mondom, hogy csak elméletben? Mert ehhez az kell, hogy a mi LN csomópontunk, ami nem csak a közvetlen fizetésekért, de a szerződések betartásáért is felel, több mint egy napra le kell legyen kapcsolva.
Ez idő alatt, ha a másik fél csal és mi ezt “észrevesszük”, magyarul a csomópontunk újra online lesz, akkor büntetésből a másik fél a szerződésben épp aktuális teljes részesedése a miénk lesz. Ez az eshetőség persze előfordulhat, hisz elmegyünk nyaralni, épp áramszünet van vagy tönkremegy a csomópontunk. Mindehhez azt is

feltételeznünk kell, hogy a másik fél csak erre vár, hogy csalni tudjon. DE! Van egy dolog, amivel a másik fél, nem tud számolni: A mi csomópontunknak több csomópont tud ingyenesen, “őrtoronyként” üzemelni. Ez azt jelenti, hogy mindameddig a mi csomópontunk bármi oknál fogva nem elérhető, úgy ezek az őrtornyok a mi velünk szerződött partnereinkre figyelnek. Ennek a funkciónak a használatáról a mi partnereink nem tudnak és mivel egy ingyenes dologról beszélünk elég nagy az esélye, hogy ezt mindenki használja. Ha csalnak, akkor ezek az “őrtornyok” azonnal aktiválják a büntető mechanizmust és a csalás a csalónak azonnal hatalmas veszteséget okoz. Összefoglalásként, abszolút nem éri meg egy ilyen csalást megkockáztatni és ezért is írtam az elején, hogy a csalás csak elméletileg lehetséges.

Mi az LN jövőbeli haszna?

- Azonnali kis összegű tranzakciók (akár 1 msat).
- A bankkártya extrém magas (~3%) tranzakciós díjak helyett átlagosan 0,0029% (1000x kevesebb).
- A banki rendszer “kitaszítottjai” számára (pl. fejlődő országok) pénzügyi szolgáltatások (pl. azonnali tranzakciók, hitelek, befektetések).
- A SPAM teljes megszüntetése (pl. azzal, hogy minden email küldés/fogadás 1 sat-ba kerül).
- Harmadik fél nélkül különböző pénzek közötti azonnali váltások (pl. BTC → USDT*).
- A felhasználók harmadik fél nélkül létrehozhatnak decentralizált pénzügyi alkalmazásokat (DeFi), melyek új lehetőségeket. biztosíthatnak (pl. kölcsönfelvételt, befektetéseket és biztosításokat).

- Kisvállalkozások részére azonnali (akár ingyenes) POS terminál (kereskedői “kártyás” rendszer), hogy az LN rendszeren keresztül bárki bármikor tudjon fizetni.
- Közösségi pénzügyek; az LN-t használhatják a közösségek arra, hogy közös célokra pénzt gyűjtsenek, mindezt harmadik fél beleszólása nélkül.
- Weboldalakon egyszerűbb biztonságosabb azonosítás (felhasználónév és jelszó szükségessége nélkül).
- Value for Value (Érték Értékért): Maga a tartalom fogyasztója közvetlenül a tartalom akár egészéért, akár részéért az előállítójának tud fizetni/támogatni. Pl. podcast hallgatása közben a műsor készítőjét másodperc alapon támogatni.

Az LN-nek bizonyosan lesz még nagyon sok egyéb területen haszna, mivel ez organikusan bárki (hozzáértő) által programozható, ezért az ötletek tárháza szinte végtelen. A könyvemben nem véletlenül ezt a hálózatot emeltem ki, mivel egyelőre ebben látom a legnagyobb potenciált, hogy az emberiség hasznára váljon.

**USDT: Az USDT token egy “stablecoin”, ami azt jelenti, hogy az értéke egy másik eszközhöz, ebben az esetben az amerikai dollárhoz van rögzítve. Egy USDT token mindig 1 dollárt ér.*
Az USDT-t a Tether cég bocsátja ki, és a Tether Limited a FIAT dollárral való fedezetet biztosítja. Ez azt jelenti, hogy a Tether cég egy bankszámlán minden kibocsátott USDT tokenhez 1 dollárt tart fenn.

A Bitcoin csalói

Rengeteg Bitcoinnal kapcsolatos csalás létezik és fontos ezekkel tisztában lenni, hogy képesek legyünk ellenük megvédeni magunkat. Íme néhány a leggyakoribbak közül:

- Adathalászat: A csalók legitim kriptovaluta tőzsdéknek vagy más szolgáltatásoknak álcázhatják magukat, hogy az áldozatok személyes adatait megszerezzék. Ilyenek lehetnek például a bejelentkezési adatok vagy a tárca címek. Ezeket az adatokat ezután felhasználhatják az áldozatok pénzének ellopására vagy a Bitcoin tárcájuk hozzáférésének a megszerzéséhez.
- Ponzi-rendszerek: A Ponzi-rendszerek olyan befektetési csalások, amelyben a korai befektetők hozamait az újabb befektetők pénzéből fizetik ki. A Ponzi-rendszerek végül összeomlanak, amikor nincs elég új befektető, hogy a korai befektetőknek a hozamokat kifizesse. A Bitcoinnal kapcsolatos Ponzi-rendszerek gyakran magas hozamokat ígérnek kis kockázattal.
- “Pump and dump”: A pump and dump csalások során a csalók egy adott kriptovalutáról hamis vagy eltúlzott információkat terjesztenek, hogy annak az árát megnöveljék (pump). Ezután mielőtt az ár esésnek indulna a kriptovalutájukat gyorsan eladják (dump). A “pump and dump” csalások gyakran a közösségi médiában vagy más online platformokon terjednek.
- Felhőbányászat: A felhőbányászat olyan szolgáltatás, amely lehetővé teszi az emberek számára, hogy Bitcoint bányászhassanak anélkül, hogy saját bányászgépet és ehhez szükséges infrastruktúrát kellene birtokolniuk. A felhőbányászati csalások azonban gyakran átverések, és az áldozatok a pénzükért semmit sem kapnak.

- “Scamcoinok”: A scamcoinok olyan kriptovaluták, amelyeket kifejezetten a befektetők megtévesztésére terveztek. A scamcoinok mögött gyakran nincsen valódi üzleti modell és a fejlesztők is sok esetben rejtőzködnek.

A fentiekkel kapcsolatban ökölszabályként felállíthatjuk, hogy:

1. Soha NE add meg személyes adataidat vagy a pénztárca címedet ha nem vagy biztos benne, hogy az adott felület/oldal teljes mértékben megbízható.
2. Soha NE tölts le vagy telepíts olyan alkalmazást, amely nem biztos, hogy megbízható.
3. Soha NE kattints olyan linkre, amelyben I nem vagy biztos, hogy biztonságos.
4. Soha NE nyiss meg olyan e-mail csatolmányt, amelyben I nem vagy biztos, hogy ténylegesen ismert címzett küldte és nem tartalmaz valamiféle kártékony kódot (vírust).

A Bitcoin jövője

A Bitcoint mindig is az általa nyújtott megoldások tették egyre népszerűbbé. Tehát a 0 USD értéktől egészen a jelenlegi (2023) 69.000 USD csúcsig, úgy jutott el, hogy mindenki, aki ebben közreműködött az azért tette, mert a használatában megtalálta a neki passzoló funkcióját és ennek érdekében időt és pénzt áldozott rá.

Elmondhatjuk, hogy a Bitcoin a kezdetektől fogva egy alulról felfelé építkező technológia volt. Ami azt jelenti, hogy a “hírét” a különböző érdekek mentén a vele kapcsolatba jutó személyek terjesztették és valószínűleg ez a jövőben sem lesz másképp. Miért mondtam ezt?

A Bitcoin mára annyira értékes lett, hogy sok (amerikai) politikus a jövő évi (2024-es) választások miatt a Bitcoin “hullámait” próbálja “meglovagolni” és ezáltal további népszerűséget szerezni. Azt azért ne felejtsük el, hogy azok akik a politikai pályán ezeket a politikusokat anyagilag is támogatták, nos ezeknek az érdekeivel abszolút ellentétes az, amit a Bitcoin képvisel.
Azt sem tartottam okos ötletnek, hogy adománygyűjtéssel az amerikai szenátus minden egyes tagjának egy Saifedean: The Bitcoin Standard könyvet küldtek, mert bár a könyv szenzációs az ötlet pazarlás, mivel akik az elejétől fogva (és most is) a Bitcoin térnyerését ellenzik, azok ezután is ezt fogják tenni, ugyanis a pénzügyi támogatóik miatt nem tehetnek mást. A politika egy aljas színtér, ott naivitásnak helye nincs.

Említettem, hogy ez egy alulról felfelé építkező technológia, ezért én inkább azt támogatnám, hogy az iskolákban az ilyen és ehhez hasonló könyveket a gyerekek kapják meg, ezzel is a jövő generációinak gondolkodását formálva.

Szerencsére minden reklám jó reklám, még a rossz is (ha esetleg a fent említett választásokon induló politikusokat rossz, hátsó szándék vezérelné).
Érdekektől függetlenül akár egy pozitív vagy egy negatív példán keresztül a példa hatása a végén mindenképp a Bitcoin előnyére fog válni. Nem lehet megállítani, ezért a korlátozása/betiltása csak a lakosság ellenszenvét fogja kiváltani és előbb utóbb a tiltó hatalmat úgyis megkerülik. Nem működött Kínában sem és még ez a kínai tiltás is hosszú távon a Bitcoin előnyére vált (a bányászat decentralizáltabb lett).

Úgy gondolom, hogy a Bitcoin esetében a gazdasági ösztönzők elképesztően erősek. Gondoljunk csak a fejlesztőire, akik közül a

protokollt nagy részük ingyen, minden támogatás nélkül fejlesztik. Nekik az elsődleges gazdasági céljuk: a már birtokolt Bitcoin értékének növelése. Ahogy egyre több ember (lásd rossz reklám is jó reklám) találkozik vele és megtalálja benne a jövőbeli számításait, úgy pusztán csakis önös érdekből azon fognak dolgozni, hogy az minél értékesebb legyen.

Ez hosszú távon nagyon jó hír, mert az egyénnek a saját hétköznapi munkája mellett nem kell befektetési szakembert “játszanin”, hogy a pénzének értéke ne a “lefolyón keresztül” távozzon, hanem van ideje arra, hogy a szakmájának csúcsát képviselje és mellette normális életét éljen.
Pusztán csak a Bitcoin ösztönzői miatt az élete jelentősen megkönnyebbül csakúgy, mint anno az Aranystandard alatt volt.

Ezt a fejezetet pedig egy Saifedean: Principles of Economics (A közgazdaságtan alapelvei) könyvéből kiragadott résszel szeretném lezárni:

“Ahogy az emberiség egyre nehezebben előállítható monetáris médiát használ, úgy növekszik a jövőnkről való gondoskodási képességünk. Növekszik a jövőbeli énünkkel folytatott tranzakciók hatékonysága, csökken a jövő bizonytalansága. A pénz, mint megtakarítási médium biztonsága számtalan ember számára tette lehetővé, hogy a háború és a katasztrófák pusztításai elől vagyonukkal világszerte könnyen szállíthatóan menekülhessenek. A jövő bizonytalanságának csökkenésével és az átruházható vagyon növekedésével a jövő diszkontálása és az időpreferencia mértéke csökken. Bármely- és mindenkori társadalomban az emberek számára elérhető monetáris technológiák keménysége az idő preferenciájával jó vagy rossz értelemben elválaszthatatlanul összefügg.”

Negyedik fejezet: A Bitcoin használata

Az “5%-os szabályom”

Először is itt is kiemelném, hogy ez nem pénzügyi tanácsadás, nincs ilyen végzettségem, tehát részemről bármi ilyen tanácsadás törvénytelen lenne. Itt csak azt írom le, amit én csináltam és, hogy mi a vele kapcsolatos tapasztalatom.

Az elmúlt években rendszeresen megkaptam (majdnem mindenkitől), hogy “nekem nincs pénzem, amiből Bitcoin-t tudnék venni”. Természetesen ez egyfajta reflex válasz és az esetek elenyésző számában volt csak igaz (nekik szeretnék ebben a részben leírtakkal segíteni). Mivel a legtöbbjük több ingatlant, járművet, egyéb befektetéseket birtokolt, számomra ez a kijelentés valójában azt jelentette, hogy a Bitcoin jövőjében nem hittek és ezért nem akartak vásárolni.
Ez nem az ő hibájuk, hanem az enyém, mert mint oktató náluk elbuktam. Nem tudtam kellően körültekintően fogalmazni úgy, hogy minden részletet, felmerülő aggályt átbeszéljünk. (Ez is motivált arra, hogy a lényeget jól összeszedve ezt a könyvet megírjam.)

Évekkel ezelőtt egyik-hónapra a másikra éltem, szinte nulla megtakarítással. Ekkor gondoltam arra hogyan tudnék úgy Bitcoint vásárolni, hogy évek múlva ne mondjam azt magamnak: ”Te ott volt a lehetőség, mégis elcs*szted.”

A végtelenül egyszerű “5%-os szabályomat” erre találtam ki, ami igazából annyit jelentett, hogy a bruttó (!) keresetemnek az 5%-ból minden hónap elején Bitcoint vásárolok.
Ha valaki belegondol, teljesen mindegy mennyit keres, az 5%-át lazán olyasmire költi, amiről könnyen le tud mondani. Ez az összeg mindenkinél más, ezért konkrét példát nem említek.
Jól látható, hogy ez a szabály nagyon egyszerű és egyben nagyszerű is, mert aki hosszú távon tervez annak teljesen mindegy, hogy per pillanat a Bitcoin árfolyama hol van. Nekem ez a stratégia nagyon bevált, és persze az egyszerűsége miatt bárki saját magára szabhatja, mert a kulcs úgyis a következetességben van.

Na jó, akkor indulásnak ez a stratégia megteszi, de a Bitcoint hol tároljam?

A Bitcoin tárcák

A Bitcoin tárcákat kétféle csoportba tudjuk sorolni. Az egyik az úgynevezett “szoftveres”, a másik pedig a “hardveres” tárcák.
Az előbbi kvázi ingyenes, mert bármilyen eszközön (pl. mobiltelefon, PC, laptop, stb.) futtatható. Az utóbbi az, ami viszont némi költséggel jár (kb. 22 000 Ft-tól a “csillagos égig”).

Régen nagyon fanatikus voltam, mert mindenkinek azt mondtam, hogy az extra védelem miatt (erről később) kizárólag a hardveres tárcákban gondolkodjanak.
Pár éve még ebben a könyvben is csak ezt ajánlottam volna, de azóta sok olyan emberrel találkoztam, aki vagy nem engedheti meg magának és/vagy a tolvajok kifinomult módszereinek egyáltalán nem célpontja (még).

Ezért előbb térjünk ki a “pro-kontra” összehasonlításra és utána igyekszem egy “ökölszabályt” felállítani, hogy kinek melyik változatot ajánlom.

Kategória	Szoftver tárcák	Hardver tárcák
Biztonság	Kevésbé biztonságosak, mivel a privát kulcsok nem védett eszközön tárolódnak.	Biztonságosabbak, mivel a privát kulcsokat speciális céleszközön (a jobbak külön biztonsági chippel) védve tárolják.
Kényelem	Kényelmesebbek, mivel a készítésüknél ez a fő szempont.	Kényelmetlenebbek, mivel külön fizikai eszközt kell használni.
Költség	Általában ingyenesek vagy legalábbis a “tároló” funkciójuk.	Költségesek, kb. 22 000 Ft-nál kezdődnek.
Funkciók	Általában a legszélesebbkörű funkciókat kínálják.	Korlátozottabb funkciókkal rendelkeznek, mivel a biztonságra összpontosítanak.
Visszaállítás	Van, amelyik a visszaállításhoz szavakat nem biztosít (egyre ritkább), a többi könnyen visszaállítható.	Ha a hardvertárca elveszik/megsérül, akkor az első indításnál generált speciális szavakkal egy új hardveres tárca vásárlásával könnyen visszaállítható.

Összességében, a hardver tárcák a szoftver tárcáknál biztonságosabbak, de a szoftver tárcák kényelmesebbek. A számodra legmegfelelőbb tárca típusa az egyéni szükségleteidtől és kockázatvállalási hajlandóságodtól függ. Mit jelent ez?

Egy “ökölszabályt” kell felállítani, amit viszont a Bitcoin értékének növekedésével folyamatosan újra kell értelmezni:
A szoftveres tárcákra úgy kell tekinteni, mint a valódi pénztárcánkra. Kizárólag olyan összeget szabad a szoftveres tárcában tartani, aminek elhagyása/ellopása nem jelent számunkra azonnali anyagi csődöt! Minden ennél nagyobb összeget, ahogy a FIAT pénz esetében is, nem a pénztárcánkban tartunk, hanem a “párnában”, széfben, bankban stb., a Bitcoin esetében erre egy hardveres tárcát kell használnunk.

Tárca és tárca között nagyon nagy különbségek vannak! Itt külön kitérek majd arra, hogy milyen tárca tulajdonságokat preferálok.

Szoftveres tárcák:
A szoftveres tárcák használatára bármilyen indok is vigyen, igyekeznünk kell a “támadási felületetet” csökkenteni. Ilyen tárcának a tárolására NE a napi használatban lévő telefonunkat, számítógépünket vagy tabletünket használjuk (1)!
Ha otthon nincs egy nem használt, mondjuk régi android telefon, akkor egy ilyen telefont a használt piacon már nagyon olcsón lehet venni (2). Ne felejtsük el minden esetben a gyári visszaállítást elvégezni rajta (3), hogy egy esetleges régebben telepített vírus nehogy mindent azonnal ellopjon.
Természetesen lehet használni egy kiszuperált régi laptopot is (ezt is “formázni” kell) vagy akár kicsi miniPC-ket (pl. Raspberry Pi), amik ugyanúgy el tudják látni ezt a feladatot.

Ebben az esetben a régi android telefont jobban preferálom, mert a kevésbé szakavatott emberek egy PC/laptop esetében sokkal több hibát tudnak elkövetni, mint egy gyári visszaállításon átesett android telefonnal, ezért ezt az általános leírást ezzel módszerrel folytatom.

Ettől a ponttól kezdve semmilyen egyéb szoftvert, mint a Bitcoin tárca NEM SZABAD rá telepíteni (4)! Konkrétan általam ajánlott szoftveres tárcák listáját, az alábbi oldalon tudod megtekinteni:

http://bitcoinmagyarul.com/szoftveres-tarcak/

Lezárásként újra visszatérek ahhoz a kijelentésemhez: Kizárólag (!) csak a tárca legyen telepítve (a gyári alkalmazásokon kívül), és csak akkor kapcsold be, amikor utalást vársz vagy akarsz küldeni (5). Ezen kívül legyen jól “eldugott” helyen, de mindenképpen a speciális helyreállító 12 - 24 szótól fizikailag elkülönítve (6)! (Lehetőleg ne egy épületben.)

Érdemes ezt a hat lépést külön egy “post-it”-re is kiírni, hogy még véletlenül se legyen valamelyik lépés kihagyva, mert azzal jelentősen megnöveled a tárolt Bitcoin elvesztésének kockázatát!

Hardveres tárcák:
A hardveres tárcák esetében egy fokkal (na jó, több fokkal) jobb helyzetben vagyunk, mert a privát kulcsunk optimális esetben maximálisan védve van. Mi az optimális eset?

A számítástechnikában nincs ellophatatlan információ, csak kellően nehéz út, amivel teljesen eltántoríthatjuk a többieket a próbálkozástól. Ezt megértve vannak olyan hardver gyártók, akik a védelmet nem bízzák a véletlenre, hanem egy (vagy több) úgynevezett Biztonsági

Chipet (angolul: secure element) is alkalmaznak. (Ezzel a tolvajok dolgát jelentősen megnehezítve.) Mit tud ez a “mágikus” chip?

A tárca első indításánál már működésbe lép és a speciális 12 - 24 db helyreállító szó generálása és tárolása, valamint az utalások aláírásához szükséges privát kulcs tárolása/használata is már ezen a chipen keresztül történik.
Ezt a chipet elsődlegesen a banki rendszerek biztonságának szavatolására fejlesztették, ezért feltörni meglepően nehéz. Ahogy fentebb említettem van olyan gyártó, amely nem egyet, hanem kettő ilyet használ és mindkettőt különböző gyártóktól, így maximalizálva a védelmet.
Persze mindent fokozni is lehet, mert az igazán profik a teljes “offline módot” is támogatják, ami azt jelenti, hogy egyáltalán nem szükséges a számítógéphez/mobiltelefonhoz való csatlakoztatásuk. A kommunikáció csak egy hordozón keresztül (pl. memóriakártya) történik. Ez azért nagyszerű, mert ez esetben egy vírus általi lopás veszélye és a csatlakoztatott telefonon/számítógépen keresztüli feltörés kizárható.
Konkrétan az általam ajánlott hardveres tárcák listáját az alábbi oldalon tudod megtekinteni:

http://bitcoinmagyarul.com/hardveres-tarcak/

Bármelyiket is választja az ember, azaz szoftveres vagy hardveres tárcát, a felelősség az adott tárcát használó egyénen van! Ebből kifolyólag jól nézzen utána, hogy az adott választás mennyire megbízható és mennyire szolgálja (kizárólag) a felhasználó érdekeit. Ezt nem szabad elkapkodni és ténylegesen időt kell rá fordítani! Mivel ez a könyv csak amolyan általános tájékoztatásként szolgál, pontosabb és személyreszóló tanácsokat csak az adott egyén helyzetének megismerése esetén tudok javasolni.

Létfontosságúnak tartom, hogy a Bitcoint az emberek a saját tárcájukban tartsák, mert a Bitcoin külső (harmadik fél) kezében való tartása rendkívül kockázatos! Lehet egy “sima” csőd, esetleg ún. exit scam (bedönti a céget, hogy a Bitcoinnal “megpattanjon”), állami lefoglalás/kényszerített beszolgáltatás stb.

Történelmi példa a kényszerített beszolgáltatásra:

Az Egyesült Államokban a 6102. sz. elnöki rendelet, amelyet 1933. április 5-én Franklin D. Roosevelt amerikai elnök írt alá, betiltotta az Egyesült Államok kontinensén a nem törvényes fizetőeszközök, köztük az arany és az ezüst birtoklását.
A rendelet a nagy gazdasági világválság idején született, amikor az Egyesült Államok gazdasága összeomlott. A kormány attól tartott, hogy az emberek aranyban és ezüstben fogják elrejteni a pénzüket, ami a gazdaság helyreállítását akadályozta volna.
A rendelet értelmében minden amerikai állampolgárnak 1933. május 1-ig be kellett szolgáltatnia az összes arany-, ezüst érmét és rudat az Egyesült Államok Kereskedelmi Minisztériumának. A kormány 20,67 dollárt fizetett ki minden troy uncia (31,1034768 gramm) aranyért és 12,50 dollárt fizetett ki minden troy uncia ezüstért.

Kedves olvasó, mit gondolsz, ha a fentieket az arany esetében el

lehetett követni, akkor egy hasonló gazdasági helyzetben, a Bitcoinnal nem lehetne újra megtenni? Érdemes a Bitcoin elvesztését kockáztatni azáltal, hogy egy 3. fél számára teljesen ki vagy szolgáltatva?

A speciális szavak (“seed”) védelme

A tárcák és kulcsok szerepénél leírtam, hogy mik is ezek a speciális szavak (angolul: “seed”) és miért olyan rettentően fontos, hogy 1.) ne veszítsük el 2.), és csakis a tárca tulajdonosának “kezében” legyenek.

Általában, ha valaki egy hardveres tárcát vásárol, akkor kap hozzá egy kis papírt vagy valamilyen fém lapot, amibe ezeket a szavakat beírhatja (fém esetében gravírozhatja). NAGYON javaslom, hogy ezeket NE használjátok, mert a jövőben ezek közül bármelyik bárki kezébe kerül egyértelműen tudni fogja, hogy a kezében mit tart.

Nem javaslom, hogy a 12 db vagy 24 db szó (ahogy már írtam a mennyiségük tárca függő) egy lapon vagy bármilyen felületen egyben szerepeljen. Érdemes ezeket több részre feldarabolni, hogy bárki bármely részét találja meg a tárca tartalmát ne tudja megszerezni. Erre a “darabolásra” több lehetőség is van. Íme egy példa:

24 szó esetében			*12 szó esetében*		
“1-es felület”	**“2-es felület”**	**“3-as felület”**	**“1-es felület”**	**“2-es felület”**	**“3-as felület”**
1. szó		1. szó	1. szó		1. szó
2. szó		2. szó	2. szó		2. szó
3. szó		3. szó	3. szó		3. szó
4. szó		4. szó	4. szó		4. szó
5. szó		5. szó	5. szó	5. szó	
6. szó		6. szó	6. szó	6. szó	
7. szó		7. szó	7. szó	7. szó	
8. szó		8. szó	8. szó	8. szó	
9. szó	9. szó			9. szó	9. szó
10. szó	10. szó			10. szó	10. szó
11. szó	11. szó			11. szó	11. szó
12. szó	12. szó			12. szó	12. szó
13. szó	13. szó				
14. szó	14. szó				
15. szó	15. szó				
16. szó	16. szó				
	17. szó	17. szó			
	18. szó	18. szó			
	19. szó	19. szó			
	20. szó	20. szó			
	21. szó	21. szó			
	22. szó	22. szó			
	23. szó	23. szó			
	24. szó	24. szó			

A fenti példa jól szemlélteti, hogy a tárca helyreállításához a 3-ból bármely 2 különböző lap elegendő. Viszont bárki, aki megszerzi bármelyik darabot is, a tárcát nem tudja helyreállítani és ezzel a Bitcoint ellopni.

Végezetül pedig a következőket külön kiemelem, mert NAGYON fontos tanácsok következnek, amit nagyon javaslok megfogadni!

A több részre bontott szavakat érdemes egymástól fizikailag külön helyen tárolni (1), és amennyiben lehetséges (úgy, ahogy már írtam) NE egy épületben legyenek (2), hanem 3 különböző épületben, városban, országban stb., hogy egy esetleges lakástűz, földrengés, vihar stb. ne tudjon visszahozhatatlan kárt okozni.

Az internetet “bogarászva” a szavak tárolására millió egy lehetőség van, de amit semmiképp nem javaslok, hogy bármilyen digitális formában tároljátok (3). Ez, amennyiben rosszul van kivitelezve (elég könnyű hibázni) egy vírusnak, hacker-nek könnyű prédává teheti.

Bármelyik megoldást is választva abszolút javaslom, hogy a tárca első beállítását követően mindenképp egy próba visszaállítást végezzetek el (4)! Azaz tegyetek rá egy nagyon kevés összeget és miután meggyőződtetek, hogy biztosan (!) megvan a 12 vagy 24, a helyreállításhoz szükséges szavatok, akkor a tárcát töröljétek vagy állítsátok vissza gyári állapotba (ez a tárca törlésével jár!).
Ezután a szavak használatával a tárca visszaállítását próbáljátok ki és amennyiben sikeresen működött, az előzőleg ráutalt összeg meg kell jelenjen. Csak és kizárólag ezen sikeres teszt után javaslom, hogy egy nagyobb összeget tegyetek rá (5), mert ha a kezdetekben bármit is elrontottatok (pl. a szavakat nem megfelelő sorrendben, írtátok fel), akkor ami rajta volt örökre elveszett!
A szavak (megfelelő sorrendje!) nélkül a tárca tartalmát, SENKI SEM TUDJA VISSZAÁLLÍTANI!
Időnként mindenképpen érdemes ellenőrizni, hogy minden, a szavakról készített biztonsági mentés érintetlenül megvan (6)!

Ahogy a szoftveres tárcáknál is javasoltam, érdemes ezt a hat lépést külön egy “post-it”-re is kiírni, hogy még véletlenül se legyen valamelyik lépés kihagyva, mert azzal jelentősen megnöveled a tárolt Bitcoin elvesztésének kockázatát!

Utolsó fejezet: Gondolatok

Beszéljünk a “hogyan továbbról”

A következőkről általánosságban nem lehet beszélni, mert (remélhetőleg) ezt a könyvet majd többféle korosztály olvassa, és szerintem mindenkinek az itt leírtakat az életébe teljesen máshogy kellene beépítenie.

Fontos megjegyeznem, hogy amikor ezt a könyvet írom (2023) a Bitcoin árfolyama 30e USD körül mozog és ez az ár sokakat arra fog majd késztetni, hogy azt mondják “ez a vonat már elment”. Remélhetőleg a könyv eddigi tartalma, azért ezen személyek számát jelentősen mérsékelte, de akik még mindig így gondolják, azoknak szeretném azt mondani, hogy a Bitcoin egy értéktároló/értékmegőrző rendszer. Nem úgy kell rá tekinteni, mint egy kaszinó, amivel gyorsan meg lehet gazdagodni. Ezt fontos leszögeznem, mert ez a rendszer -úgy, mint évezredekig az arany - már a kezdetektől arra volt tervezve, hogy hosszú távon a vagyon öröklésének és biztonságos értékmegőrzésének módját nyújtsa.

A Bitcoin használatával kapcsolatban megpróbálok a különböző korcsoportokra és különböző anyagi helyzetre bontva tanácsokat adni, hogy én a helyükben a Bitcoin segítségével hogyan állnék az élethez.

Iskolás korosztály: Tudom elég tág, de itt kb. a 14-18 körüli korosztályra gondolok. Nekik a buli, a csajozás, a pasizás mellett elcsépelten, de az elsődleges dolguk a tanulás kellene legyen. Véleményem szerint nekik a legnehezebb, mert a mai felgyorsult

globalizált világban a tanulásnál maximális teljesítményt kellene nyújtaniuk, mert a munkahelyek a munkaerőt, már nem lokálisan, hanem globálisan keresik (bárki bárhonnan jelentkezhet rá). A szerencsének tehát nagy valószínűséggel nem lesz igazán szerepe, mivel a jövőben a globalizáció hatására a munkaadók külföldi, magasan képzett (akár szegény) országból jövő munkaerőből bőven választhatnak majd. Úgy gondolom, hogy a kötelező iskolai tananyagon túl a közelgő MI (Mesterséges Inteligencia) “forradalom” miatt olyan témák iránt kellene érdeklődniük, amelyeknek az állásait az MI nem fogja helyettesíteni.
Erre nem tudok biztos, általános tanácsot mondani (hisz ez a terület elképesztő ütemben fejlődik), de jól látható, hogy a kétkezi munka az, ami minimum egy évtizedig azért az emberek kezében marad. Robotizáció gyorsan fog terjedni, de az elején rendkívüli költségessége miatt szerintem még egy pék, gumis, lakatos, festő meg fog tudni élni. Tudom ezek a 21.században már nem “szexi” munkák, DE aki ezt a könyvet elolvasta és szeretne a jelen vagy jövőbeli kiszolgáltatottság helyzetéből kitörni, az minden fillért meg kell tudjon spórolni és azt a luxust nem engedheti meg magának, hogy diplomás munkanélküliként tengődjön. Az idő a legjobban ezen korosztály ellen dolgozik.

Egyetemista: Nekik az MI “forradalma” abszolút a legrosszabbkor jött és valószínűleg az egyetemen tanult tudása és végzettsége éveken belül feleslegessé válik, mivel őt egy MI tökéletesen helyettesíteni tudja majd. Ezt persze a jogi környezet még kérdésessé teszi, de ahogy az eddigi dolgokat alakulni látom, előbb-utóbb az “MI lobbi” fog nyerni.
Én mindenképp a lehető leghamarabb a szakmámban (esetleg diákmunkásként) elhelyezkednék. Kezdőként bármennyire is keveset keresnék, de azonnal mellette “kétkezi” átképzésben is gondolkodnék. A lehető leghamarabb olyan jól fizető kétkezi munkára váltanék, amit az MI első körben nem tud kiváltani.

Minden fillért félretennék, ami az alapvető megélhetéshez nem szükséges és/vagy ameddig egy biztonságos vagyon nem alakul ki, ami akár évek munkanélküliségét is fedezni tudná. Emellett nagy dolgokra (autó, ház, külföldi hosszú nyaralások, stb.) nem költenék.

Szakmunkás: Ő korunk egyik leglenézettebb dolgozója, mégis ma (2023) arányaiban az egyik legjobban kereső (a kereslet-kínálat szempontjából = kevesen vannak). Ő, mialatt a “belét is kidolgozza” célszerű lenne, ha nem élne nagy lábon, mert egy recesszió, egy piaci irányváltás vagy ne adj Isten egy tartós betegség, őt is bármikor keresőképtelenné teheti.
Neki is azt tudom javasolni, hogy ameddig egy biztonságos vagyon - ami akár évek munkanélküliségét nek is biztosítani tudná - nem alakul ki, nagy dolgokra (autó, ház, külföldi hosszú nyaralások, stb.) nem költenék.

Diplomás munkavállaló: Elméletileg ők keresnek a legjobban (kivéve az olyan piaci torzulásoknál, mint mondjuk a pedagógus), ha csak a KSH statisztikáit nézzük, akkor a covid után ők kapták a legtöbb béremelést és nekik lehet (!) némi megtakarításuk “felhalmozva”. Amennyiben te diplomás dolgozó vagy és ez nem így van, akkor javaslom, hogy a költségeidet most azonnal nézd át és szanáld amire nincs abszolút szükséged! Őszinte leszek, ezt a réteget úgy látom, mint egy ketyegő bombát, mert a legfrissebb MI teljesítménye őket célozza meg, mint a jövő “kiváltandó” célcsoportja. Nekik most nagyon luxus egy nyaralás, egy autóvásárlás, lakásvásárlás stb. Miért? Mert nekik is évekre kell egy olyan biztonságos vagyont kiépíteniük, amihez bármikor, egy esetleges munkanélküliség alatt vagy ameddig átképzik magukat, hozzá tudnak nyúlni. Másnak sem, de nekik tényleg nem javaslom a hitelből való vásárlást, mert amint a munkahellyel gondok lesznek nagyon komoly problémában találják magukat.

Nyugdíjas: Nekik a legnehezebb tanácsot adni, mert ők azok, akiknél zsigerből jön a kérdés hogy “miből”? Miből spóroljanak?
Szemét leszek, mert azt írom, hogy az “5%-os szabályom” (fentebb olvasható) az nekik is működni tud. Igaz, konkrétan lehet az élelemből vagy egyéb szükségletekből kell ezt a pénzt elvegyék. Ők lesznek (szerintem) a jelenlegi pénzügyi rendszer első tömeges vesztesei.

Jól láthatjátok, nincs csoda! Ez nem egy hogyan gazdagodjunk meg játék, hanem hogyan tudj talpon maradni akkor is, ha beüt a “gebasz”. Az most egy MI “forradalom” vagy egy lehetséges háború vagy csak simán egy munkanélküliség, az teljesen mindegy. Fontos hogy értékálló csereeszköz álljon rendelkezésre, amit AZONNAL (!) el tudsz adni/cserélni, ha majd igazán szükséged lesz valamire.

Michael Saylor-“féle” megtakarítási modell

Az én egyszerű 5%-os modellemről már írtam, de mivel nincs pénzügyi előképzettségem, ezért megosztom egy olyan sikeres üzletember modelljét, akit nagyon nagyra becsülök és a gondolkodása, beszédei mindig rabul ejtenek.

Először is néhány szó róla:

Michael Saylor egy amerikai üzletember, a MicroStrategy alapítója és volt vezérigazgatója (jelenleg igazgatósági tag és a Bitcoin befektetések felelőse). 1989-ben alapította a céget, amely üzleti intelligenciát és jelentéstételi (reporting) szoftvereket fejleszt. Saylor a Bitcoin egyik legnagyobb támogatója. Személyesen is, de a cégén keresztül is a Bitcoin-ba több milliárd dollárt fektetett be.

Michael Saylor “laikus” embereknek javasolt defenzív befektetési modellje viszonylag egyszerű.

Azt vallja, hogy mindenkinek arra kellene törekednie, hogy az átlagos havi költségkeretéből 6 hónap helyi pénzben (pl. forint), 3 év (36 hónap) USD-ban és az ezen kívüli összeg pedig Bitcoinban legyen. Midezeket arra alapozza, hogy bármely 4 éves periódust vizsgálva, elenyésző volt azon esetek száma, amikor ha az ember Bitcoint vett és rá 4 évre eladta, akkor a Bitcoin befektetése veszteséges lett volna. Ebből kifolyólag szerinte a fenti stratégiával a lehető legtovább lehet bevételi forrás nélkül úgy kibírni, hogy ha mégis Bitcoint kell eladni, akkor az nyereségesen történjen.

A BlackRock-“féle” befektetési modell

Bizonyos emberek számára ennek a befektetési vállalatnak a neve ismerős lehet, de akinek nem, íme néhány mondatban, hogy ki és mi is ez a BlackRock:

A BlackRock a világ legnagyobb vagyonkezelő cége, összvagyona 7,8 billió (7,800 milliárd) dollár felett van. A BlackRock a nyugdíj- és biztosítási alapok, a nonprofit szervezetek, a kormányzati ügynökségek és a magánbefektetők számára kínál befektetési szolgáltatásokat.

2018-ban Larry Fink a BlackRock vezérigazgatója azt mondta, hogy a Bitcoin "nem egy befektetés", hanem egy "spekulatív eszköz". Ugyanakkor azt is mondta, hogy a Bitcoin "érdekes technológia", és

hogy "figyelni kell rá". (*Esetleg már itt elszólta magát, hogy titokban vásárol?*)

2022-ben viszont gyökeres fordulat következett be és a BlackRock a Bitcoin-alapokba 200 millió dollárt fektetett be.
Larry Fink azt mondta, hogy a Bitcoin "egyre elfogadottabbá válik" és, hogy "a befektetők számára potenciálisan hasznos eszköz lehet".

2023-ban pedig már egy Bitcoin ETF* igénylést is benyújtott.

> **A Bitcoin ETF egy tőzsdén kereskedett alap, amely a Bitcoin árfolyamát követi. Az ETF-ek olyan befektetési eszközök, amelyek részvényekkel, kötvényekkel vagy más eszközökkel rendelkeznek, és a tőzsdén kereskedhetők. A Bitcoin ETF-ek a befektetők számára lehetővé teszik, hogy a Bitcoinba anélkül fektessenek be, hogy maguk a Bitcoinnak tulajdonosai lennének.*

Majd rövidesen a Bitcoin ETF igénylés után egy érdekes 2022-es BlackRock elemzés látott napvilágot, hogy szerintük egy portfólió esetében 84.9% az optimális Bitcoin befektetési arány.

Jól látható, hogy öt év alatt a BlackRock-nak a Bitcoinról kialakult publikus véleménye mennyire gyökeresen megváltozott.

Arany vs. Bitcoin

Nagyon sokan azt gondolják, hogy az arany már bizonyított és a pénzként való használatának funkciója bele van “kódolva”, ezért a

Bitcoin soha nem lehet jobb alternatíva, mert abba ez nincs bele “kódolva”.
Ezt jobbára a keynesiánus iskolát követő közgazdászok, illetve ezen emberek követői mondják, mert szerintük létezik olyasmi, hogy az áruba “az értéke bele van kódolva”.

Ludwig von Mises megértette, hogy a monetáris szerep sohasem volt az aranyba “kódolva”: Az érték, mint fogalom az emberi tudatosságon kívül nem létezik, ezért a fémek és az anyagok számukra olyan lényeges elemet, amely monetáris szerepet tudna rájuk ruházni, nem tartalmaznak. Szerinte az arany a monetáris státuszát kizárólag a stabil pénzre vonatkozó kritériumok (relatív ritka és független) miatt kapta:

*“A tiszta pénz elvének két aspektusa van: Elfogadható, ha a piac jóváhagyja, mint általánosan használt csereeszközt. Negatív, ha a kormány ezzel akadályozza, megzavarja a valutarendszert.”**
*Ludwig von Mises, The Theory of Money and Credit, 2nd ed. (Irvington-on-Hudson, NY: Foundation for Economic Education, 1971)

A fentieket figyelembe véve azt mondhatjuk, hogy vagy elfogadjuk azt, hogy a pénzként való használatának funkciója a Bitcoin-ba is bele van “kódolva” vagy azt mondjuk, hogy az aranyba sincs, mivel a Mises által vázolt kritériumoknak a Bitcoin is tökéletesen megfelel.

A realitásokhoz visszatérve, azaz miután az arany eme “kiváltságát” leküzdöttük, többféle kritérium alapján ténylegesen hasonlítsuk össze őket:

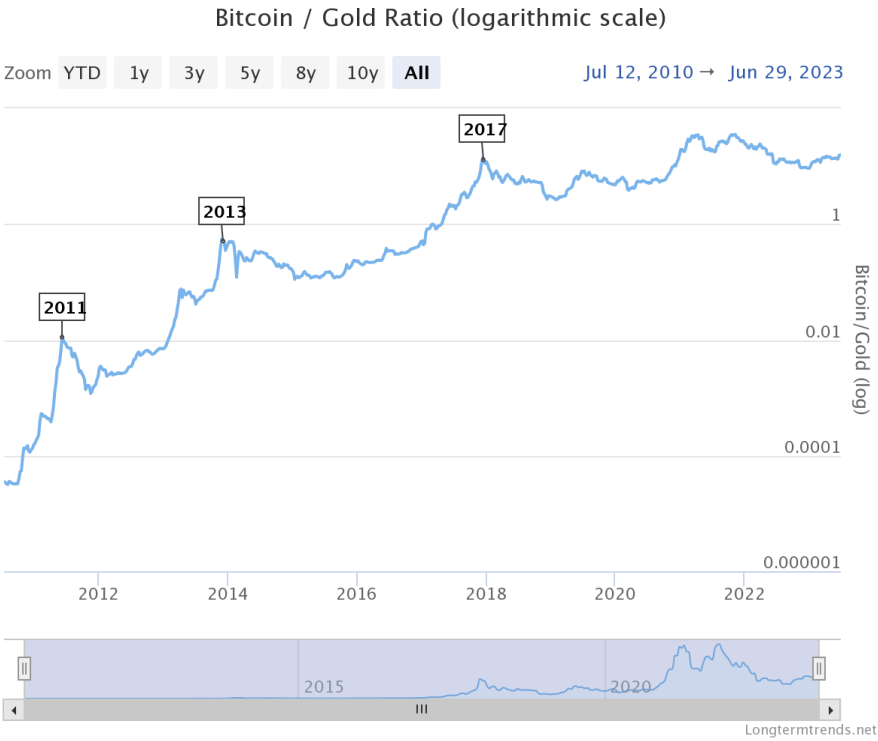
Kategóriák	**Arany**	**Bitcoin**
Maximális mennyiség (ritkaság)	Ismeretlen, de relatív ritka	21 Millió, ezért abszolút ritka
Tárolhatóság	Széf vagy egyéb költséges megoldás	Ingyenes (software) vagy viszonylag olcsó fizikai tárca
Szállíthatóság	Körülményes, magas költségek	Akár azonnal, rendkívül alacsony költségek
Oszthatóság	Rendkívül körülményes	1 Bitcoin = 100 Millió Satoshi (“fillér”)
Hamisíthatóság	Megoldható (lásd Tungsten)	Lehetetlen, az ingyenes ellenőrizhetőség miatt
Decentralizáltság	Rossz, mivel a nagyobb mennyiségeket bankokban tartják	Jó és évről évre javul, ahogy a véges (!) készlet egyre jobban, egyre több ember között eloszlik
Elkobozhatóság	Fizikai valója miatt elkobozható	A 12, 24 db speciális szó (seed) észbentartásával vagy egy biztonságos tárcával elkobozhatatlan
Tartósság	Nagyon tartós	Nagyon tartós
Bányászhatóság	Rendkívül magas költségekkel, környezetszennyezettséggel és csak állami “hátszéllel”, igazán gazdag cégeknek	Bárkinek, akinek van áram, internet és megfelelő “bányagépe” (általában pár ezer dollártól már “használható” vásárolható)
Elfogadottság	A világon bárhol (általában hivatalos átvevőhelyen bevizsgálva)	A világon javarészt bárhol, de egyelőre az aranynál jóval kevesebb helyen, viszont mindenféle extra bevizsgálás nélkül
Nyomonkövethetőség	Mint a készpénz, a fizikai valója miatt relatíve lehetetlen nyomon követni	Alapjába véve pszeudoanonim*, de léteznek rá megoldások, amivel a nyomonkövethetősége relatíve lehetetlenné tehető
Átruházhatóság	Fizikailag szükséges, ebből kifolyólag időigényes és jelentős költségekkel jár	Akár azonnal, a világ bármely pontjára
Ár manipulálhatóság	Magas, mivel az azonnali tőzsdei ügyletekben a valódi arany azonnal nem cserél gazdát	Közepes, mert a valós (SPOT) tőzsdei kereskedésben a Bitcoin azonnal gazdát cserél, így valós a kockázat, hogy a manipuláció (eladás) előtti mennyiség visszaszerzése nem sikerül
Programozhatóság	Lehetetlen	Digitális valója miatt magas és funkciói állandó bővítés alatt vannak

**Pszeudoanonim: A Bitcoin pénztárcák és a tranzakciók a technológia sajátossága miatt publikusak, viszont a hozzájuk tartozó tulajdonos kiléte nem. Addig, ameddig egyes pénztárcák tulajdonosai nem kerülnek felfedésre, a rendszer anonimitást biztosít.*

A táblázatos összehasonlítást vizsgálva 2023-ra a Bitcoin az aranyhoz képes, 14-ből 12-ben jobb, 1-ben ugyanolyan és 1-ben rosszabb (egyelőre). Úgy gondolom, hogy a Bitcoin ezen 14 év alatt meglehetősen sokat fejlődött és hamarosan (max. 1 évtized) abban az 1-ben, amiben még az aranynál rosszabb (Elfogadottság), abban is sokkal jobb lesz.

Jól látható, hogy amint a csereeszközök történelménél is bemutattam: senkinek sem kell megmondania, hogy melyik csereeszközt válassza, hanem a vagyont mindig az aktuális legjobb, a másodiktól, a harmadiktól és a sokadik legjobbtól organikusan “átszipolyozza”.

Az alábbi Bitcoin/arany grafikon jól mutatja, hogy a Bitcoin aranyban kifejezve, lényegében már az első Bitcoin tőzsdei ártól fogva, egyre több (uncia) aranyat képvisel.



A fenti grafikon (linkje a forrásoknál megtalálható) részletesebb elemzésénél látható, hogy 2010. október 11-én 1 Bitcoin 0,0001 uncia aranyat ért.

A könyv ezen részének írásakor (2023. június 30-án) 1 Bitcoin 16,2 uncia aranyat ért.Ugyanakkor 2021. október 21-én 1 Bitcoin 37 uncia aranyat is ért. Az előbbi (mai árfolyam) 13 év alatt 162 ezer (!) szeresére, az utóbbi (2 évvel ezelőtt) 370 ezer (!) szerese is volt. Ez aranyban kifejezve 162 000 000% és 370 000 000% érték növekedés. Úgy gondolom, a fenti grafikonon látható tendencia és a fenti számok kellően bizonyítják, hogy ez a trend tovább fog folytatódni. A szabad

piac pedig organikusan (mindenféle támadás/ellenzés ellenére) már jól láthatóan eldöntötte, hogy mi a korunk új, legértékállóbb csereeszköze.

Végére pedig a “zöld béke” képviselőinek: egy arany és egy Bitcoin “bánya”.

Fúj, kapitalizmus!

Muszáj erről beszélnem, mert évtizedek óta mindenki minden rosszat a kapitalizmusra kent, de biztos vagyok benne, hogy miután a könyvben idáig eljutottál nyitott vagy még egy dogma letörésére.

Először is tisztázzuk, mi is a *kapitalizmus*? Na nem az, amit ma minden mainstream közgazdásztól és politikustól hallasz.

> *Kapitalizmus (egy MI szerint): A kapitalizmus egy olyan gazdasági rendszer, amelyben a termelőeszközök magántulajdonban vannak, és a gazdasági döntéseket a vállalatok és az egyének hozhatják meg. A kapitalizmusban a vállalatok versenyeznek egymással a termékek és szolgáltatások piacán és a fogyasztók döntenek arról, hogy melyik vállalattól vásárolnak. A kapitalizmus célja a gazdagság növelése és az emberek életminőségének javítása.*

A fenti fogalomban hol található az “állam”, mint kifejezés? Na ugye, hogy sehol, na de akkor az életünkbe lépten-nyomon miért szól bele (adók, korlátozások, vám stb.)? Ha az állam beleszól, akkor egyáltalán kapitalizmusról beszélhetünk?
Érdekes kérdések ezek és mindenki elgondolkodhat rajta, de az én véleményem az, hogy kapitalizmus legalább 100 éve sehol sem létezik, mert mindenhol a gazdaság irányító szerepét az állam és a pénz területén pedig a központi bankok vették át.
Az állam a piac manipulációjával egyfajta szocialista világ alapjait építi. A szocialista ideológiára pedig a legjobb példa Klaus Schwab, a világgazdasági fórum (WEF) elnökének “freudi elszólása”: ”Semmit nem fogsz birtokolni, és boldog leszel.”

Kapitalizmus (valójában): “A kapitalizmus az, ami akkor történik, amikor az emberek elveszítik időbeli preferenciájukat, azaz elhalasztják az azonnali kielégülést és a jövőbe fektetnek be.” - Saifedean Ammous közgazdász

Érdekes, nem? Nem igen hallod ezt sem, mivel a könyvben eddig eljutva már rájöttél: a FIAT rendszer szolgái nem akarják, hogy a valódi kapitalizmus fogalmával megismerkedj, mert akkor nagyon sok kellemetlen kérdést fogsz feltenni.

"A munkanélküliség hullámának oka nem a kapitalizmus, hanem a kormányok, amelyek a vállalkozásnak megtagadják a jó pénz előállításának jogát." - Friedrich Hayek

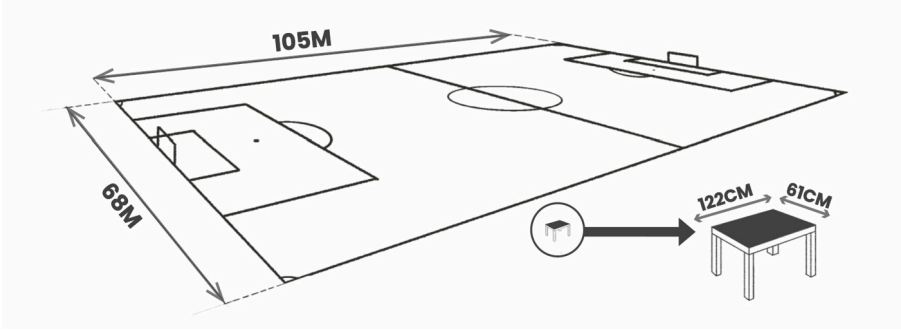
Ahhoz, hogy megértsük az emberi időpreferencia a kapitalizmusnak miért fontos, meg kell ismerkednünk a szűkösség fogalmával.

Az az általános vélemény, hogy az erőforrások szűkösek és korlátozottak, teljesen félreértelmezik a szűkösség természetét, amely a közgazdaságtan kulcsfogalma.

Julian Simon, A Végtelen Erőforrás 2 könyve alapján, Saifedean Ammous a legújabb, A Közgazdaságtan Alapelvei könyvében érthető hasonlatokkal szenzációsan bemutatja, hogy a mainstream médiából ömlő hiszti, miszerint hamarosan mindenből kifogyunk, mennyire alattomos és hazug állítás:

“A Föld felszíne 510,1 millió km2, a 2000 és 2017 között a bányászathoz használt teljes területet 57 277 km2-re becsülték, ami

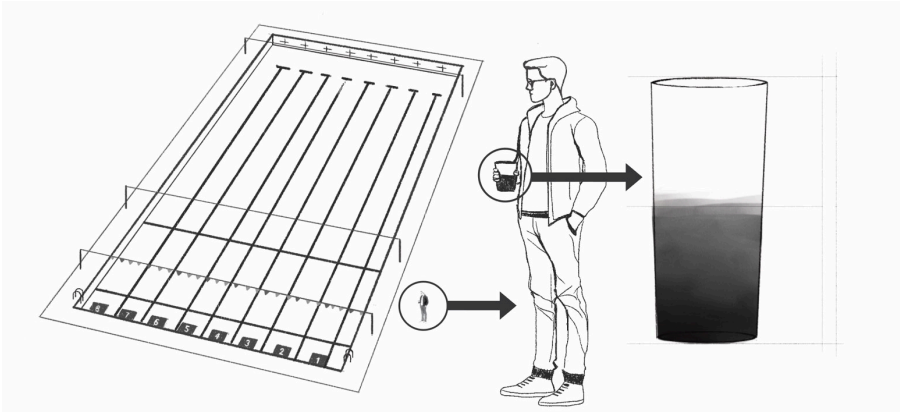
a bolygó felszínének 0,011%-a. Perspektívikusan, ha a Föld akkora lenne, mint egy futballpálya (105 m × 68 m, vagyis 7 140 m2), a világ összes bányájának felülete 0,785 m2 lenne, nagyjából akkora, mint egy kis íróasztal (egy 122 cm × 61 cm-es íróasztal felülete 0,744 m2).



A Föld átmérője 12 742 kilométer. Ezzel szemben a világ legmélyebb bányája, a Johannesburg melletti Mponeng aranybánya „csak” 3,16–3,84 km mély, vagyis a Föld átmérőjének 0,024–0,03 százaléka. A perspektíva szempontjából, ha a Föld egy 1 méter átmérőjű golyó lenne, a kérgébe valaha ásott legmélyebb lyuk 0,027 cm mély lenne, ami kevesebb, mint ezen könyvk három lapjánakvastagsága.
Mindazok az erőforrások, amelyeket az emberiség az évezredek fogyasztása és kiaknázása során felhasznált, csak egy töredéke annak a bőségnek, amely a Föld átmérőjének felületi 0,027%-ában elérhető.

A legtöbb bánya mélysége megközelíti a 300 métert. Az érvelés kedvéért egy igen nagyvonalú, 1 km-es átlagos bányamélységet tételezzünk fel. Ez azt jelentené, hogy a 2000 és 2017 közötti időszakban a bányák teljes mennyisége 57 277 km3 volt. A Föld térfogata 1 083 206 916 845,80 km3 (körülbelül egy billió köbkilométer). A világ összes bányájának térfogata tehát a Föld térfogatának 0,00000529%-a. Más szóval, a Föld 18 911 725,8-szor

nagyobb, mint a rajta létező összes bánya, amelyből minden erőforrásunkat eddig kitermeltük. Ha a Föld térfogata egy olimpiai uszoda térfogata lenne, akkor a világ összes bányája nagyjából fél pohár méretű lenne.”



A fenti kis “kitenkintő” után már tudjuk, hogy a Földben jelen lévő összes nyersanyag abszolút mennyisége túlságosan nagy, hogy emberi lényként akár meg tudjuk mérni vagy csak felfogni. Ebből kifolyólag semmiképpen sem jelent valódi korlátot, mert ahogy fentebb látjuk, a szükséges ásványok keresésekor a Föld felszínét alig karcoltuk meg. Tehát minél többet keresünk, és minél mélyebbre ásunk, annál több erőforrást találunk. Mi szab ennek határt?

Az emberi erőforrás szab határt, hogy miből mennyit tudunk találni és kitermelni, mert ez bármely erőforrás mennyiségének gyakorlati és realisztikus korlátja. (Ez az állítás egészen a Bitcoin feltalálásáig igaz volt.)

Julian Simon a késői közgazdász, A végső erőforrás mesteri könyvében elmagyarázza, hogy az emberi idő az egyetlen korlátozott

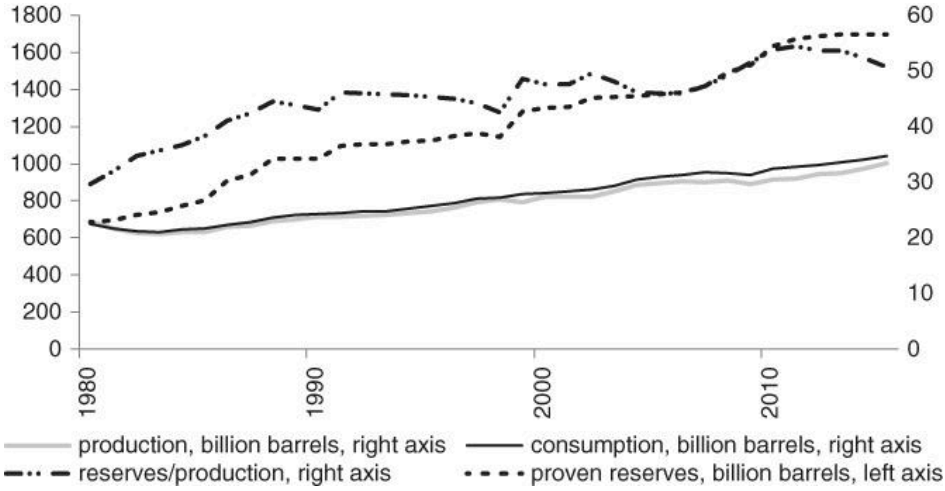
erőforrás és az az egyetlen dolog, amelyre az erőforrás, mint kifejezés vonatkozik. Miért?

Valójában, ha belegondolunk logikus, hogy a Földön minden embernek korlátozott ideje van és ez az egyetlen hiány, mellyel mindannyian foglalkozunk. Ugyanez igaz a társadalom szintjén is, mert az egészére vonatkozóan csak véges idő áll rendelkezésre, hogy különféle áruk és szolgáltatások előállítására használják.

Az egész emberiség története során soha nem fogytunk ki egyetlen nyersanyagból vagy erőforrásból sem. Gyakorlatilag minden erőforrás ára ma alacsonyabb, mint a történelem korábbi pontjainál volt, mert a technológiai fejlődésünk számunkra lehetővé teszi, hogy korunk szempontjából, őket alacsonyabb költséggel előállítsuk.
Nem csak az, hogy nem fogytunk ki az alapanyagokból, hanem idővel ahogy a fogyasztásunk növekedett, az egyes erőforrások létező tartaléka is csak nőtt.

Magyarul bármilyen áru mindig előállítható, ha az emberi időt ráfordítják. Tehát egy áru valódi költsége, mindig annak alternatív költsége, azaz az idő alatt meg NEM termelt áruk mennyisége.

Egyik példa, az olaj. A készlet-folyósítás arány fogalmánál megtanultuk, hogy az olaj ezen értéke kb. 1, mert egy adott évben mindig kb. annyit termelünk, amennyit el is használunk. Mivel a modern élethez létfontosságú, ezért nagyon megbízható statisztikával rendelkezik.



A fenti grafikon a globális olajfogyasztás, termelés, valós készletek és a készletek aránya az éves termeléshez viszonyítva, 1980–2015. (forrás: BP Statistical Review)

Amint az ábra is mutatja (külön megvizsgáltam a 2015-2021 időszakot is), még ha a fogyasztás és a termelés évről évre növekszik, a meglévő készletek még gyorsabban növekednek.

A BP statisztikai áttekintése szerint pl. 2015-ben az éves olajtermelés 46% -kal volt magasabb, míg a fogyasztás 55% -kal volt magasabb, mint az 1980-as szint. Az olajkészletek viszont 148% -kal növekedtek, mindezzel együtt a termelés és a fogyasztás körülbelül háromszorosára növekedve.

Sok példát lehetne fémekkel illetve egyéb árukkal is hozni, mert mindegyiknél - ahol van megbízható adat - az jön ki, hogy minden attól

függ, hogy mennyit termelünk, és az ára alapján mennyi erőforrást szánunk rá.
Ha magas az ár, akkor több erőforrást szánnak rá, ami miatt többet termelnek és ez végül az ár csökkenéséhez vezet. Fordítva is igaz, ha alacsony az ár, akkor nem éri meg bizonyos erőforrásokat rá áldozni, ezért kevesebbet termelnek, mint a majdani piaci igény, ami majd ennek következtében ismét áremelést fog okozni.
Erre legjobb példa az arany, amely a legritkább fém. Évezredek óta bányásszák, mégis a technológia fejlődésének következtében továbbra is növekvő mennyiségben tudják bányászni.

Az arany nem összekeverendő a többi fémmel, áruval, mert a tartóssága miatt az emberiség történelme során az összes kibányászott arany megtalálható, így a növekvő kitermelés miatt a készlet-folyósítási aránya csak kis mértékben változik.

Visszatérve a kapitalizmus fogalmára, ha hagyják működni, akkor a kapitalizmus tökéletesen tud működni, de valójában a történelem során csak nagyon rövid ideig, inkább mondhatni egyáltalán nem hagyták működni.
Mi kell ahhoz, hogy tudjon működni? Szabad piac! Szabad piac nélkül egyszerűen lehetetlen pontos árakat használni, ezzel az embert, mint véges erőforrás a, termeléshez hozzárendelni.

Ehelyett mit kapunk? Különféle szabályozásokat, vámokat, adókat és sok ezer egyéb trükköt, ahogy a különböző kormányok a mindennapi életbe és a gazdaság működésébe beleszólnak.
Ők és a követőik azt hazudják, hogy minden, ami a gazdaságban rossz történik, az a kapitalizmus hibája és “fúj gonosz kapitalizmus”! Közben

pedig csak annyi történik, hogy egy szocialista világot építenek, amihez a többség a média agymosása következtében asszisztál.

A Bitcoin és a CBDC-k

A CBDC-k (angolul: Central Bank Digital Currency), magyarul a központi bankok digitális pénze lesz valószínűleg a leendő “új” FIAT pénz (remélhetőleg az utolsó), amely a jelenlegi digitális pénznél annyival fog többet tudni, hogy “programozhatóvá” válik. Mit jelent ez?

Ámbár a könyv írásakor még a nemzeti bankok tagadják, hogy ezt az új digitális pénzt a kínai mintára készítenék (ezáltal az emberek feletti totális orwelli kontrollt biztosítva), de sajnos minden jel arra utal, hogy mégis ez a végcél.

Kezdjük ott, hogy mindent - még a legutóbbi pandémiát is - megragadnak ahhoz, hogy a készpénzt kivezessék.
Jó példa erre, hogy a külföldi országok folyamatosan csökkentik a készpénzben kifizethető összeg mértékét. A lakosságot ezáltal is arra kényszerítve, hogy digitális tranzakcióval fizessenek, amelyet természetesen nyomon lehet követni.
Az újfajta digitális központi banki pénzt még nem lehet tudni, hogy milyen sanyargató funkciókkal fogják ellátni, egyelőre csak becslések vannak:

- Lejárati idő: Mivel majd minden egyes “fillért” meg lehet majd “jelölni”, ezért ezekhez akár lejárati időt is lehet rendelni (lásd Kína), ami után ha az ember határidőre nem költi el, akkor X% azonnali adót levon belőle. Ezzel ellehetetlenítve a vagyon

felhalmozását és elősegítve a keynesiánus közgazdászok által preferált, “költés alapú” “gazdaságélénkítést”.

- Büntetések: A rendszerellenes cselekedet (pl. kormányellenes komment) után azonnali pénzbeli büntetés kiszabását teszi lehetővé főleg, ha ezt egy “intelligens” MI (Mesterséges Inteligencia) rendszerre bízzuk. Természetesen minden egyéb büntetést is azonnal érvényesíteni lehet.
- “Ezt (már) nem veheted meg”: A nemzetközileg is terjedő “klíma hisztit” kihasználva különböző korlátozásokat lehet majd kivetni, amit ehhez a tárcához/profilunkhoz lehet kapcsolni. Pl. a Google Flights a CO2 kvótát már évek óta számolja, tehát esetlegesen egy bizonyos évi kvóta felett már repülő jegyet se lehet majd venni. De ez bármilyen egyéb olyan termékekre vagy szolgáltatásokra is kibővíthető, amelyeknek tömeges megvásárlása infláció növelő hatással bírna, így egy teljes nemzetre kiterjedő dinamikus korlátozással az inflációt (szerintük) féken lehetne tartani.

Ezekre az “orwelli” világban lévő elnyomás ellen csak a Bitcoin az utolsó mentsvár, mivel ez esetben a jelenlegi készpénz szerepét venné át. Ezután a valós infláció, azaz a termékek ára Bitcoin-ban lesz mérhető (lásd a mostani hiperinfláló országok feketepiacát), mivel azok nem lesznek kormányzati korlátozások alapján mesterséges árszinten tartva.
Ez utóbbi az olyan nemzetek számára, mint pl. Argentína, ahol az argetín peso helyett az USD-ban lévő árak a mérvadóak, ismerősen fog csengeni, mert az argentín peso és az USD árfolyama a központi bank által mesterséges szinten van tartva. Természetesen tilos az USD elfogadása és bármilyen feketepiaci kereskedelme, mégis a lakosság igyekszik ezt használni. Ugyanez lenne a Bitcoin esetében is, ha mondjuk 10 tojás lenne a limit, de te mondjuk 20-at akarnál venni,

ekkor a +10 tojást a kistermelőtől “feketén” vennéd meg, amiért az új digitális FIAT pénz helyett Bitcoin-ban fizetnél. (Főleg úgy, hogy ha esetleg az a 10 tojá,s amit az új FIAT pénzzel fizetnél még a CO2 kvótádat is csökkentené.)

Nincs “új/jobb” Bitcoin!

Először is pár alapvető dolgot tisztázzunk. A kizárólag Bitcoin tulajdonosok között van egy angol mondás: “There is NO second best!” (magyarul: Nincs második legjobb!)

Ez arra vonatkozik(e könyv írásának befejezéséig, 2023. nyara): Nincs olyan, hogy “új” Bitcoin; ,nincs olyan hogy “jobb, mint a Bitcoin” és jelen ismeretek szerint, valószínűleg nem is lesz.

Az internetet böngészve, ha az ember a “Bitcoin” szóra rákeres, akkor onnantól kezdve szinte minden platformon olyan reklámokkal fog találkozni majd , ami ennek a pénznek az erejét “meglovagolva” a gyanútlan felhasználót egy “alternatívára” próbálja rávezetni.

Gyakran használnak olyan kifejezést, mint a “crypto” vagy “altcoin”, de ezek valamennyien csak arra szolgálnak, hogy az újoncokat valami új technológiai frázis ismételgetésével “megkopasszák”. Miért?
Azért, mert amikor az ember azt látja, hogy egy Bitcoin ára 30 000 USD, akkor könnyebben hisz annak, aki azt mondja, hogy “Itt ez az ÚJ Bitcoin, amit XYZ-nek hívnak. Ez SZEBB, ZÖLDEBB, GYORSABB, mint a már elavult Bitcoin és ha most veszel, akkor nagyon korai beszállóként csak 0,03 USD-ért megkapod.”

Azt próbálják neked sugallni (tudat alatt befolyásolni), hogy majd 1-5-10 év alatt ebből is lehet 30 000 USD árfolyam, és akkor behozod a “lemaradást”, te is ugyanolyan gazdag leszel, mint az aki 10 éve Bitcoint vett és azóta a csodával határos módon nem adta el.

Volt lehetőségem konferencián, illetve az interneten keresztül is kötetlenül 1-2 ilyen “crypto” fejlesztővel beszélgetni. Kivétel nélkül (!) mindegyik azt vallotta, hogy azért csinálja, hogy a végén az amit képvisel több Bitcoint érjen, azaz effektíve amikor eladja a saját “termékét” több Bitcoin-ja legyen. Nem állítom, hogy nincs olyan, aki ezt máshogy gondolja, de abszolút érthető ez a cél is. Miért?

Ezek a bennfentesek azaz, akik a ma ismert vezető “alternatívákat” fejlesztik tudják, hogy a blokklánc technológia értelmesen kizárólag egy dologra használható, arra amire anno a Bitcoin-t kitalálták. Hogy mi az az egy dolog?
A pénz szuverenitásának biztosítása. Minden más esetre egy központosított megoldás (pl. felhőalapú szerver) sokkal jobb választás, mint egy lassú blokklánc technológia, ami ráadásul (ezekben az esetekben) energiapocsékolás útján valósítható meg.

Persze ilyeneket is mondogatnak, hogy: “Az én “új” Bitcoin pénzem sokkal jobb, mert 200x több tranzakciót tud naponta feldolgozni, sokkal “okosabb”, sokkal egyszerűbb használni, elég az email címedet megadni stb.”
Egy dolgot viszont elfelejtenek, amit egyik ilyen “új találmány” (nagy részük egymást másolja) sem tud biztosítani. Ez pedig továbbra is a legfontosabb: a pénz szuverenitása.

A “kriptopénzéről” bárki bármit hazudhat, de a szuverenitáshoz biztosított decentralizáltságot (kellően sok csomópont és bányász,

kellően sok országban szétszórva) egyik ilyen “új találmány” sem tudja maradéktalanul, de még csak megközelítőleg sem biztosítani.
Ez pedig az adott “alternatíva” birtokosait egy olyan veszélynek teszi ki, hogy ha a kormányzat részéről kellő figyelmet kap bármikor kötelezhetik, hogy olyanra alakítsák, ami a mindenkori kormányzat számára megfelelő lesz. Rosszabb esetben csak simán lekapcsolják.

Sok ilyen annyira központosított (egy maroknyi ember irányítja), ami miatt konkrétan olyanok, mint egy vállalat. A vállalatokat pedig gyerekjáték külsőleg befolyásolni, irányítani.

Én az embereknek azt javaslom, hogy a nehezen megkeresett forintokat NE ilyen szerencsejáték szintű dolgokkal “kaszinózzák el”, hanem inkább további edukációra vagy esetlegesen értékálló befektetésre fordítsák.

A Bitcoin Nyert!

Sokan akiket, a Bitcoin előretörése zavar (pl. begyepesedett aranyat tartók), azoknak ez a rész nagyon fájdalmas lesz.

Valójában a Bitcoin már most nyert és akár itt abba is hagyhatnám ennek a résznek az írását, mert amikor ezt írom (2023 nyarán) kvázi az összes “nagy” név (pl. Larry Fink - BlackRock, Jamie Dimon - JP Morgan, Jerome Powell - FED, stb.), aki évekig a Bitcoint utálta a véleményét pozitív irányba változtatta meg. Na, de félreértés ne essék nem azért, mert hirtelen “megtértek” és a továbbiakban az emberek szuverenitását, vagyoni stabilitását tartják fontosnak, hanem mert

továbbra is nagyon sok pénzt akarnak ~~keresni~~ csinálni és nem akarnak ebből a “buliból” sem kimaradni. Nekik ez csak egy eszköz a sok közül.

Viszont játszunk el a gondolattal, hogy a Bitcoin globálisan elterjedt és több tíz trillió dollárnyi vagyon áramolt már bele.
Amikor a Bitcoin egy “kritikus tömeget” (ezt senki se tudja mikor van) elér, akkor a vagyon beáramlása hirtelen nagyon felgyorsul. Ezt nevezik hiperbitcoinizációnak. Mi történik ekkor?

Tegyük fel, hogy ez a pont akkor van, amikor a Bitcoin 10 trillió dollár (3,5 millió milliárd forint) össz értékkel bír és egy Bitcoin 500 000 USD értéket képvisel. Ekkor mindenki azt várná, hogy esni fog, hisz mondjuk pár hét alatt 100 000 USD árról ment fel és a meredek emelkedés után azt várják, hogy újra akár 80%+ esés következik. (A következő események, amiket írok, vélhetően majd párhuzamosan történnek.)

Ez a várt esés most viszont elmarad, mert az amerikai lakosság (jelenleg a legtehetősebb nemzet) gazdagabbik része megunja, hogy hülyének vannak nézve és folyamatosan azt mondják neki, hogy a Bitcoin egy lufi, ami kipukkad. Rendszeresen azzal szembesül, hogy a vagyonát a különböző adók megtépázzák (pl. jövedelem adó, ingatlan adó stb.), de az a bizonyos “Bitcoin lufi” soha nem pukkan ki sőt, aki anno bevásárolt továbbra is őrült ütemben gazdagodik.

Ugyanakkor egy másik “lufi” hirtelen kipukkan, amit vélhetően a következő lépések lavinaszerű folyamata okoz:
a tehetős amerikai állampolgár, látva a Bitcoin elképesztő 500 000 USD árát az ingatlan birtoklását sújtó adók és költségek elől menekülve az 5 ingatlanából 4-et elad, hogy majd belőlük is Bitcoint vegyen.

Ahogy a Bitcoin ára tovább emelkedik, úgy lesz egyre “sürgetőbb” ez a vétel, mert az ingatlanok az értéküket, egyre gyorsabban kezdik veszíteni. Miért? Egyszerűen azért, mert ahogy egyre több ember jön rá, hogy neki elég 1 ingatlan, amiben éppen lakik és a többiből nem keres annyit, mintha a vagyonát “csak” Bitcoinban “parkoltatná” (mindezt minden egyéb költségek nélkül), akkor az ingatlanpiaci “lufi” kipukkan és az ingatlanok árai tartósan meredek esésbe kerülnek.

Tegyük fel, hogy egy olyan 90%-os áresés után az ingatlanpiac kiegyenlítődik, ahol az emberek már csak lakhatásért vásárolnak ingatlant és nem üzleti befektetés céljára. Ez a már már globálisan megszűnő középosztályt fogja segíteni, mert a történelemben talán most először az ingatlanok árát a Bitcoin tartósan elérhető árucikké teszi.

A globális aranypiac a Bitcoinnal szemben már most folyamatosan veszít.

Nem meglepő, hogy ez a csak pár év alatt elért jelentős értékvesztés előbb-utóbb fel fog gyorsulni, mert valójában az arany ipari célra való felhasználása jelenleg a teljes kitermelésnek csak a 11%-a. Az összes többi az úgynevezett “pénzbeli prémium”, ami az évezredeken keresztül (vélt) legjobb értéktárolási tulajdonsága miatt van.

Az emberek, ahogy a fenti grafikont is látva tömegével (!) rájönnek, hogy az arany a Bitcoinnal szemben elvesztette a legjobb értéktároló “címet”, akkor vélhetően egy 89%-os értékcsökkenéssel a vagyon az aranyból a Bitcoinba átvándorol. Ez a majdani alacsony arany ár a mai modern chipgyártásra, ékszerek áraira pozitívan fog hatni és újra fellendülőbe teszi a szép aranyból készült művészeti alkotásokat is.

Az emberek az inflációval szembeni örökös harcot megunják és azok, akik eddig részvényekben, kötvényekben némi megtakarítással rendelkeztek, látva az inflációval szembeni veszteségeiket, a Bitcoin kecsegtető hozamai miatt ezekből is Bitcoint vásárolnak.
Ez nem csak a globális pénzpiacokat, hanem a cégek méreteit is tartósan újrarajzolja, mert cégek fognak összezsugorodni (részvényük értékvesztése miatt) és néhányan közülük csődbe fognak menni. Azoknak a cégeknek, amelyekk az emberek számára pozitív értékkel bíró eszközöket/szolgáltatásokat fognak előállítani, értéke növekedni fog, mert az emberek a részvények áraitól függetlenül a termékeikért vagy szolgáltatásaikért FIAT valutát vagy a későbbiekben Bitcoint fognak adni.
A továbbiakban egy cég értékét nem a klasszikus tőzsde fogja mutatni, mert a Bitcoinnal szemben (ahogy most is) az értékük folyamatosan csökkenni fog hanem, hogy mennyi Bitcoint tud a minőségi szolgáltatásai, termékei miatt majd felhalmozni.

Az emberek a Bitcoinjaikhoz jobban fognak ragaszkodni, mert tudják, hogy mához képest holnap többet fog érni. Ugyanúgy, ahogy az aranykorban az arany esetében volt.
A Bitcoin képes lesz egy új modern aranykort létrehozni, mert az értékes Bitcoinról az emberek kizárólag akkor fognak lemondani (lásd pozitív időpreferencia), amikor legalább olyan értékesnek gondolt tárgyat vagy szolgáltatást fognak érte kínálni. Ez majd globálisan

minden személyt és vállalatot megversenyeztet, ami arra fogja őket sarkalni, hogy a lehető legjobb minőséget gyártsák, szolgáltassák.

A fenti állításomat alátámasztva, itt egy idézet Saifedean: Principles of Economics könyvéből:

"*A jelenben való fogyasztás szükséges a túléléshez. Az egyéneknek a pénzük értéké, nem kell ahhoz megsemmisíteniük, hogy fogyasszanak; a természet a túlélés érdekében, fogyasztásra kényszeríti őket. Ahogy a jövő számára való megtakarítás megbízhatóbbá válik, a marginális fogyasztásukat csökkenthetik, de a fogyasztástól nem tudnak teljesen elzárkózni. A fogyasztásnak ezen csökkenése a marginális fogyasztási cikkek előállítása terén a foglalkoztatás csökkenését eredményezheti, de nem a foglalkoztatás teljes összeomlását. Másrészt, az erőforrások fogyasztásának csökkenése megszabadítja őket a fogyasztási cikként való felhasználástól és lehetővé teszi beruházási javakként való hasznosításukat. A pénzmegtakarítás a gazdasági erőforrások fogyasztástól való megmentésének felel meg, így több lehetőség nyílik arra, hogy a munka a gazdasági termelés korábbi szakaszaira irányuljon. Az a társadalom, amely a fogyasztást folyamatosan késlelteti valójában egy olyan társadalom lesz egy alacsony megtakarítású társadalomhoz képest, amely hosszú távon többet fogyaszt, mivel az alacsony időpreferenciájú társadalom többet fektet be, így tagjainak több jövedelmet termel. Még akkor is, ha az alacsony időpreferenciával rendelkező társadalmak bevételének nagyobb hányada megy megtakarításra , hosszú távon magasabb fogyasztási szintet és nagyobb tőkeállományt eredményeznek. A fogyasztás csökkentése távol áll attól, hogy nyomort idézzen elő. Ellenkezőleg. Ez az egyetlen út a bőséghez!*"

Gondoltam azt írom, hogy "ne csak pozitív gondolatot írjak a leendő Bitcoin jövőjével kapcsolatban, hanem negatívat is…", de közben rájöttem, hogy az amit most írok, az nem negatív lesz, hanem abszolút pozitív.

A Bitcoin "győzelmével" az első rétegen olyan szintű forgalom lesz, hogy a dinamikus utalási díjak miatt a nagy többség SOHA nem fog rajta utalni.

Az első réteg, amelyet lényegében ma a többség használ valószínűleg országok, bankok fogják naponta egymás közötti elszámolásra használni. Miért? Mert kb. a világon 10 000 kereskedelmi bank van és hozzá 214 központi bank. Ezek egymás közötti napi elszámolásai miatt a kb. 500 000 napi utalási korlát után nem valószínű, hogy másoknak sok helyet hagynak. Ami marad, azt a tőzsdék, különböző egyéb magán elszámoló házak, cégek fogják felszippantani. Nekik nem lesz gond (a FIAT devizában számolva) az esetleges 1 000 USD, 10 000 USD vagy még nagyobb értékű utalási díj megfizetése.

A többieknek, azaz nekünk ott lesz majd a második és sokadik további réteg. Ahogyan az elején írtam, ez számunkra pozitív lesz, mert ebben a rendszerben a majdani bankrendszer nem fog tudni "feszültséget" felhalmozni, hiszen "pénznyomtatással" nem lehet majd őket kimenteni. Így a piacról relatíve kisebb bank- és cég csődökkel a tisztességtelen cégek és bankok eltűnnek majd.

Ezekből arra lehet következtetni, hogy a "jó" bankok nem szűnnek meg. Igen, én sem számítok a bankrendszer teljes megszűnésére, mert nagyobb valószínűségnek látom azt megtörténni, hogy úgy, mint régen (az indulásuknál) csak és kizárólag betéti bankolásra váltanak át és a betétesek Bitcoinjait fogják "őrizni". Ez egy kényelmes szolgáltatás lesz, amiért az emberek hajlandók lesznek fizetni és amit a nagy többség (sajnos) használni is fog, így ezen személyek a Bitcoint a bank által biztosított rendszeren keresztül fogják fogadni, tartani és utalni.

A fentiek, a világ várható átalakulásához mérve, csak egy kicsiny szelet, ami pusztán csak azért történhet meg, mert az emberek a Bitcoint, mint harmadik féltől független, abszolút ritka, tökéletes értéktárolót organikusan felfedezik. A könyv ezzel körbeért, mert a történelem önmagát pozitív értelemben ismétli majd és pusztán az emberek önös érdekből, ahogy a bartertől az aranypénzig eljutottak, úgy a FIAT világtól a Bitcoin világához is eljutnak majd.

Angolul erre a Bitcoin-erek egy évtizede ezt mondják: “Bitcoin is inevitable.” magyarul: “A Bitcoin elkerülhetetlen.”

Utószó

Who the “F…” is Alice, azaz ki vagyok Én? :)

A fenti cím egy ismert Smokie dal 90-es évekbeli feldolgozása (aki nem ismeri, keressen rá). Nehéz magamról írnom, mert olyan típusú ember vagyok, aki szeret a háttérben maradni és nem magát futtatni, de azért nézzünk néhány releváns tényszerű adatot:

- 7 éves korom óta a számítógép által nyújtott világ rabja vagyok,
- 20 évesen saját IT vállalkozást indítottam és a társammal közel 10 évig sikeresen üzemeltettem,
- 29 évesen váltottam, de az informatika világát képtelen voltam elengedni és először “alternatív”, majd Bitcoin bányászatával foglalkoztam,
- 30 évesen egy közel 1 MW összteljesítményű “bányászfarmot” terveztem és kiviteleztem,
- 36 évesen írom ezen könyvet. :)

Ui.: Ehhez a könyvhöz nem lett volna elég ez a durván 7 év, amit a Bitcoin világában töltöttem, hanem kellett hozzá az a több, mint 100 könyv elolvasása is, ami kellően szerteágazóan a világ napfényes és sötét oldaláról is felvilágosított.
Ezen könyvek is nagymértékben motiváltak, hogy ezt a könyvet megírjam, mert úgy gondolom, hogy a Bitcoin legalább alapszintű megismerésére a magyar lakosságnak szüksége van.

Végül pedig, ahogy az elején írtam, ez a könyv nem egy mindenre kiterjedő iromány szeretett volna lenni, mert arra ott van pl. a The

Bitcoin Standard, amely már magyarul is megjelent, illetve a címben jeleztem is, hogy ez az első rész, amely úgy gondolom, ha elnyerte a tetszéseteket, akkor folytatódni fog.
A folytatást pedig a Ti visszajelzésetek alapján fogom írni. Szóval az alábbi oldalon megtalálható elérhetőségeim bármelyikén tudtok számomra visszajelzést küldeni, amit én előre is nagyon szépen megköszönök!

https://bitcoinmagyarul.com/#kapcsolat

Források:

https://www.pbs.org/wgbh/nova/article/history-money/
https://hu.economy-pedia.com/11032129-cantillon-effect
https://academy.binance.com/hu/articles/what-is-fiat-currency
https://www.longtermtrends.net/bitcoin-vs-gold/
https://buybitcoinworldwide.com/volatility-index/
https://batcoinz.com/bitcoin-by-energy-source/
https://www.investopedia.com/terms/1/51-attack.asp
https://bitcoinarchive.co/blackrock-bitcoin-allocation-portfolio-84/
https://datarecovery.com/rd/what-are-the-odds-of-someone-getting-the-same-bitcoin-seed-phrase/
https://www.cointribune.com/en/can-someone-discover-my-bitcoin-seed/
https://energyeducation.se/germany-near-blackout/
https://porkopolis.io/basemoney