Sík Zoltán Nándor
alelnök
Nemzeti Hírközlési és Informatikai Tanács

A blockchain filozófiája, avagy a fennálló társadalmi rendek felülvizsgálatának kényszere

Csak egy forradalmi innováció a sok közül?

Blockchain – jobb fordítás híján magyarul blokklánc[1]. A blockchain egy olyan információtechnológiai innováció, amely nevének már csak a hallatán is minden vezető állam, államszövetség politikai és gazdasági vezetőinek megremeg a szája széle. A jelen cikk írásának idejére gyakorlatilag a világ minden vezető hatalma tett már valamilyen nyilatkozatot blockchain „ügyben".

Tiltani, tűrni, vagy támogatni. Senki nem tudja, mit kezdjenek vele, de a témában valamilyen állásfoglalásra kényszerült már Donald Trump[2] amerikai elnök, Vlagyimir Putyin[345] orosz elnök, Kína[6] vezetői, az EU több tagállama[78910], Christine Lagarde[11] az IMF vezetője, Jim Yong Kim[12] a Világbank vezetője, Mario Draghi[13], az Európai Központi Bank elnöke. Ugyanígy megszólaltak más banki és pénzintézeti vezetők, mint pl. Jamie Dimon[14] a JPMorgan vezetője, vagy a nagy multicégek vezetői, mint pl. Bill Gates[15], és sorolhatnánk. Sőt, a blockchain még a politika középpontjába is került.[16] Naponta születnek nyilatkozatok, vélemények, állásfoglalások, leginkább abban a tekintetben, hogy hogyan lehet a blockchain-t kordában tartani, az erre alapuló megoldásokat szabályozni.

Mindemellett már számos tanulmány is foglalkozik a jelenlegi és a várható hatásokkal. Legyen elég csak egynek a címét itt idézni: *„How blockchain technology could change our lives"*, azaz *„Hogyan változtathatja meg az életünket a blockchain technológia"*. Ezt a tanulmányt 2017 februárjában készítették – ezért a jelen cikk írásának idején[17] már elég *„réginek"* tekintendő –, kiadója nem más, mint az Európai Parlament Kutatói Szolgálata (EPRS)[18].

Egy azonban biztos. Forradalom zajlik, infokommunikációs technológián alapuló forradalom, amely jól láthatóan különbözik minden eddigi forradalomtól, mind céljában, mind eszközrendszerében. Ez a forradalom, bár technológián alapul, de nem technológiai. Azaz nem a technológiát reformálja meg, hanem a technológia felhasználásával egész éle-

[1] Jelen cikkben szándékosan a blockchain szót használom, a magyar fordítás még nem elterjedt.

[2] *Trump White House Doubles Down on US Commitment to Blockchain* – https://www.coindesk.com/trump-white-house-doubles-us-commitment-blockchain/

[3] *Vladimir Putin Mandates New Rules for Cryptocurrencies and ICOs* – https://www.coindesk.com/vladimir-putin-mandates-new-rules-cryptocurrencies-icos/

[4] Putin: *‚We Want To Build Disruptors'* – https://www.forbes.com/sites/kenrapoza/2017/10/25/putin-we-want-to-build-disruptors/#5de8d23d7c73

[5] Vladimir Putin: *Cryptocurrency Poses ‚Serious Risks'* – https://www.coindesk.com/vladimir-putin-cryptocurrency-poses-serious-risks/

[6] *Blockchain ICOs: Can China Issue The Death Penalty For Illegal Fundraising?* – https://www.forbes.com/sites/leonhardweese/2017/08/30/blockchain-icos-can-china-issue-the-death-penalty-for-illegal-fundraising/#6826fd556225

[7] *UK Government Considers A "Digital Strategy" Plan* – http://ftreporter.com/uk-government-considers-a-digital-strategy-plan/

[8] *Estonia wants to launch its own government-backed cryptocurrency called ‚estcoin'* – https://www.cnbc.com/2017/08/23/estonia-cryptocurrency-called-estcoin.html

[9] Germany's Central Bank: *Consumers Won't Use Blockchain for Payments* – https://www.coindesk.com/germanys-central-bank-consumers-wont-use-blockchain-payments/

[10] *France Is Close to Issuing a Position on ICOs* – https://www.coindesk.com/france-close-issuing-position-icos/

[11] *IMF's Lagarde: Ignoring Cryptocurrencies ‚May Not Be Wise'* – https://www.coindesk.com/imf-head-christine-lagarde-it-may-not-be-wise-to-dismiss-virtual-currencies/

[12] *World Bank President: Everyone Is Excited About Blockchain* –https://www.coindesk.com/world-bank-president-everyone-excited-blockchain/

[13] Mario Draghi: *European Central Bank Has ‚No Power' to Regulate Bitcoin* – https://www.coindesk.com/mario-draghi-european-central-bank-has-no-power-to-regulate-bitcoin/

[14] *JPMorgan CEO Jamie Dimon says bitcoin is a ‚fraud' that will eventually blow up* – https://www.cnbc.com/2017/09/12/jpmorgan-ceo-jamie-dimon-raises-flag-on-trading-revenue-sees-20-percent-fall-for-the-third-quarter.html

[15] Bill Gates: *Bitcoin Is ‚Better Than Currency'* – https://www.entrepreneur.com/article/238103

[16] *How Bitcoin Could Free Catalonia From Spain's Dictate* – https://cointelegraph.com/news/how-bitcoin-could-free-catalonia-from-spains-dictate

[17] 2017. október-november

[18] Philip Boucher et al.: *„How Blockchain Technlogy Could Change Our Lives – In-depth Analysis"*, European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA), PE.581.948, February 2017.

tünket, lehet, hogy évszázados, évezredes bevett társadalmi berendezkedéseinket változtathatja meg[19].

Alvin Toffler „A harmadik hullám"[20] c. könyvében leírta azokat a társadalmi formákat, amelyek kialakulásához valamilyen technológiai újítás vezetett. Az első hullám a mezőgazdasági társadalmak kialakulása volt, amelyek az ősközösségből alakultak ki a földművelés és állattenyésztés elterjedésével. Ehhez nyilván az adott kornak megfelelő innovációkra volt szükség (eke, öntözőrendszerek, stb.). A második hullám az ipari társadalmak kialakulása volt, amelyhez szintén technológiai innovációk vezettek (pl. gőzgép). A harmadik hullám az információs társadalmak kialakulása, azé az információs társadalomé, amelyben ma is élünk, és természetesnek vesszük azt, hogy ehhez is innovációk sorozata vezetett (pl. informatika, internet). Ezen hullámok egymás mellett, vagyis inkább egymásra halmozódva (szuperponálódva) léteznek és határozzák meg jelen társadalmunkat. Jelen cikk azt próbálja fejtegetni, hogy most jön-e el a negyedik hullám, egy olyan technológiai innováció, amely új társadalmi formákat hoz létre, vagy sem. Pontosabban nem egy innováció, hanem az innovációknak egy olyan halmaza, amelyeket értelmes módon összekapcsolva – akarva, akaratlanul – mélyre ható társadalmi változások következnek be. Ezen innovációk mintegy *„zászlóshajója"* a blockchain, és bár nem kizárólag ez az innováció hozhat, vagy hoz társadalmi változásokat, ma a blockchain nevével fémjelzik mindazt, amelyből a jelen forradalom táplálkozik.

Anarchia?

De miről is beszélünk? Egyáltalán mi ez, és miért pont a blockchain[21] az, amelyik ilyen módon igyekszik felforgatni a világot? Egyáltalán miért teszi? Tudatos, vagy véletlen a hatása? De mielőtt a blockchain világába bepillantunk, érdemes szólni arról is, hogy mi is az, amit felforgat a blockchain-en alapuló innováció *„csomag"*, magának a technológiának az alkalmazása. A válasz sommásan annyi, hogy mindent. Ez a *„minden"* azonban nem egyszerre minden, ez attól függ, hogy a blockchain-t mire használjuk. Az már ma is látszik, hogy a blockchain, mint innováció gyakorlati alkalmazása igyekszik függetlenedni mindentől, ami a mai, bevett, hierarchiára épülő társadalmi rendeket jellemzi. Függetlenedni a bankoktól, az ügyvédektől, de a bíráktól, az állami végrehajtó hatalomtól (kormányoktól), a törvényalkotó hatalomtól is. Azaz mindattól, ami a Montesquieu-i hatalommegosztási elvekben szerepel. A blockchain függetlenedni kíván a hatalomtól, a hierarchiától. A blockchain filozófiája ellentmond annak, amit *George Kennan*[22] fogalmazott meg a kormányokról, végső soron a hierarchiára épülő társadalmakról:

> *„…a kormány életre hívása vagy tudomásulvétele nem mérlegelő választás tárgya. Az egyetlen elgondolható alternatíva az anarchia, ami önpusztító volna a közösségre – valójában nincs mi között választani."*
>
> *„…a kormányzattal mindig együtt jár, tőle elválaszthatatlan a hatalom. Nincs kormányzás hatalom nélkül. Egyetlen kormány sem tud meglenni nélküle. A kormány leglényegibb tulajdonsága a hatalma. A kormány fogalma pontosan azt fejezi ki, hogy benne testesül meg egy ország legjelentősebb hatalmi központja."*[23]

A blockchain filozófiája szerint mindenki, aki a technológiát (vagy arra épülően annak akár csak egy speciális részét) használja, közvetlenül részt vesz a *„közösség"* életében, és mindenki mással egyenlő módon gyakorolja a hatalmat. Mondhatnánk, hogy ilyet már láttunk, leginkább az athéni demokrácia[24] lehetett hasonló. Vagy – korlátozásokkal bár –, de akár *Karl Marx* osztály nélküli társadalma (az eredeti kommunizmus, nem a sajnálatos módon ténylegesen megvalósult, totalitárius diktatúrák). De végső soron leginkább az anarchiára hasonlít a blockchain világa. Alapvető különbség, hiszen ez nem káosz, hanem egy *„rendezett"*, logikai alapon kikényszerített szabályokon, mindenki egyenlőségén alapuló anarchia.

Ez az anarchia alapú megközelítés talán nem is volt meglepő azoknak, akik magát a technológiát kitalálták, hiszen *Timothy C. May*[25] már 1992-ben leírta mindezt az általa jegyzett *„Kripto Anarchista Kiáltvány"*[26]-ban. Azt, hogy miért *„kripto"*, és hogy ebben az esetben a *„kripto"*-nak, mint elrejtés fogalomnak semmi köze a földalatti mozgalmakhoz, miután teljesen más értelemben használja, a későbbiekben még látni fogjuk. Azt azonban a történelem eddigi folyásából tudjuk, hogy az anarchia többnyire átmeneti állapot, amely általában egy új, az eddigiektől gyökeresen eltérő, de mégis hierarchikus rend kiépítésének kezdeménye.

Mi az a blockchain?

Visszatérve a fenti kérdésre, mi is az a blockchain, vagy blokklánc? Ezt és a kapcsolódó fogalmakat mindenképpen meg

[19] Ez nem egy atombomba, amely szintén tudományos és technológiai innováción alapult, de míg az atombomba társadalmakat képes eltörölni a föld színéről, ez az innováció a társadalmi berendezkedés, a jelen hatalmi struktúrák felülvizsgálatára kényszerít.

[20] Alvin Toffler: *A harmadik hullám*, Információs társadalom A-tól Z-ig sorozat 2. kötet, Budapest, 2001, ISBN 963-9326-21-6

[21] Vinay Gupta: *A Brief History of Blockchain* – https://hbr.org/2017/02/a-brief-history-of-blockchain

[22] George F. Kennan (1904–2005), amerikai diplomata, történész, több amerikai elnök tanácsadója, jelentős szerepe volt a hidegháború céljainak kidolgozásában.

[23] George Kennan: *Around the Cragged Hill (New York: W. W. Norton, 1993), chapter 3: On Government and governments*, pp. 53–74. Idézi: Sík Zoltán Nándor: *Információs hadviselés*, E-Government Tanulmányok XXIX., Budapest, 2009, ISBN 978-963-9753-17-4

[24] Itt is csak akkor, ha kizárólag az athéni állampolgárokat tekintjük, akik politikai jogkörökkel rendelkeztek, és eltekintünk a nőktől, a rabszolgáktól és azoktól a szabad *„idegenektől"*, akiknek a nagyszülei még nem Athénben születtek.

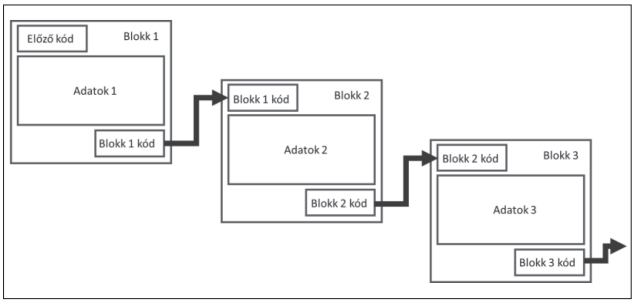
[25] Timothy C. May, ismertebb nevén Tim May, technológiai és politikai író, villamosmérnök, korábban az Intel alkalmazottja volt, ahol az ún. *„alfa-részecske probléma"* megoldása fűződött nevéhez. A *„Kripto Anarchista Kiáltvány"* megfogalmazója

[26] Crypto Anarchist Manifesto – https://www.activism.net/cypherpunk/crypto-anarchy.html, http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html

kell értenünk ahhoz, hogy a fenti állítások, ha nem is teljes mértékben bizonyíthatók, de minimum valószínűsíthetők legyenek. A fogalmak megértése nélkül nem érthető meg sem a filozófia, sem annak hatásai. Ezért ezeket a fogalmakat, a technológiai innováció ezen elemeit nem informatikai, jogi, vagy gazdasági szaknyelven, hanem remélhetőleg mindenki számára érthetően kívánjuk leírni.

A blockchain egy informatikai fogalom, legalábbis mai felfogásunk szerint. Azt jelenti, hogy különböző adatokat ún. blokkokba foglalunk. Egy blokkban maximált mennyiségű adat tehető be. Az így *„blokkosított"* adatokból képezünk egy, csak erre az adathalmazra[27] jellemző, de a teljes befoglalt adatnál lényegesen rövidebb ellenőrző kódot (hogy mi ez, és hogyan készül, a későbbiekben szólunk). Ezek után a következő blokk elejére ezt a kódot építjük be, majd csak utána jön a többi adat, ami ezt a bizonyos következő blokkot alkotni fogja, és így tovább. Így végül is ebből az adatoknak egy adott láncolata keletkezik, amelyre az a jellemző, hogy ami adat ebben a láncolatban szerepel, az nem változtatható meg visszamenőleg[28] sem direkt, sem véletlenül, mert akkor az egész blokklánc logikailag *„borul"*.[29] Ebből tehát az következik, hogy az az adat, amely a blokkláncba bekerül, az valamilyen módon hitelesnek tekinthető és tekintendő.[30] Mindezt tehát informatikai megoldással kínálja a blockchain rendszer úgy, hogy ez nem egy *„egyszerű"* adatbázis.[31]

Szintén mondhatjuk, hogy ilyet már láttunk, hiszen, ha megnézzük bármely pénztárkönyv egymást követő lapjait, az egyes bevételek, kiadások utáni egyenleg oszlop lap alján történő összegzését átvitelnek hívjuk, ami a következő lap tetején ugyanaz az összeg, mint áthozat szerepel, és onnan folytatjuk a bejegyzéseket. Ezzel is biztosítjuk azt, hogy a pénztárkönyvből ne lehessen csak úgy lapot kitépni, hiszen akkor már nem stimmel az egész. Ha mégis ilyet látunk, a pénztárkönyv tételeinek visszakövetésével látni fogjuk, hogy az elejétől számítva meddig folytonos a tételek (tranzakciók) sorrendje, és hol van az a pont, ahol megszakad, ahol valami probléma keletkezett. Addig jó azonban, amíg mi magunk jövünk rá erre, és nem a főkönyvelő, vagy akár a revizor. Szándékosan említettem pénztárkönyvet, de a vállalati főkönyvek is hasonlóan működnek, de a főkönyv szó hallatán sokak úgy gondolják, hogy innen mély pénzügyi és számviteli ismereteket igénylő fejtegetés következik.[32] Ezt elkerülendő mostantól a főkönyv kifejezést fogjuk használni.



1. ábra
Egyszerű blockchain

A fentiekhez azonban tartozik még egy megjegyzés: a pénztárkönyvet, főkönyvet kiadások és bevételek, egyéb pénzmozgások, vagy azzal egyenértékű, pénzben kifejezett értékek mozgásainak tranzakciói alkotják. Ráadásul minden tranzakció után kiszámolják az aktuális egyenleget. A blockchain esetében, mint ahogy fentebb volt már róla szó, bármilyen adatot beleírhatunk az adott blokkba, és az a speciális „egyenleg", csak az adott blokk végén van kiszámolva. Ezt az egyenleget viszont igen speciális módon számolják ki, a blokkban foglalt adatokból egy zanzát, vagy kivonatot készítenek, amit a gyakorlatban a hash angol kifejezéssel említünk. Ennek a kiszámítási módnak igen nagy jelentősége van a blockchain szempontjából (lásd később).

Egyetlen, nyílt főkönyv

A blockchain tehát hasonlóan működik a fent leírtakhoz, de technológiai megoldása egyszersmind biztosítja azt, hogy mindenki, aki ezt a technológiát használja, egyszersmind főkönyvelővé, sőt revizorrá is válik azzal, hogy mindenki ellenőrzi mindenki adatait. De hogyan, és miféle adatokat? Egyáltalán miért ellenőrzi mindenki mindenkinek a főkönyvét, hiszen az abban lévő tranzakciók, adatok mindenki magánügyét képezik. És itt a blockchain másik újítása, amely azt mondja, hogy a rendszer akkor működik egyenrangú felek között, ha mindenki látja mindenki tranzakcióit, és csak egyetlen főkönyv van, amelybe mindenki tranzakcióit felvezetjük. Az egyszerűség kedvéért hívjuk minden, egy adott blokkba bekerült adatot tranzakciónak, a későbbiekben látjuk, hogy ezt miért tesszük.

Tehát a blockchain egyik újítása az, hogy csak egy főkönyv van, és mindenki azt az egy főkönyvet *„vezeti"*. De honnan tudjuk, hogy mely tranzakciók kerültek már be a főkönyvbe (azaz melyek vannak már lekönyvelve), és melyek nem kerültek még sorra. Legalább ekkora probléma az is, hogy egy tranzakció csak egyetlen alkalommal legyen lekönyvelve. Ennek megértéséhez további innovációkkal, valamint azok alapfogalmaival kell megismerkednünk.

[27] Az adathalmaz kifejezést itt nem matematikai értelemben használjuk, csak jelezzük vele, hogy sok adatról van szó.

[28] Kivéve, ha a változásban érintett blokktól kezdve az összes későbbi blokk, összes másolatához hozzáférünk, aminek – mint a későbbiekben látni fogjuk – igen kicsi a valószínűsége.

[29] Azaz a blokkokra meghatározott szabályok megsérülnek; ráadásul ennek a ténynek az ellenőrzésére bárki képes, aki hozzáfér a blochchain-hez.

[30] Vágujhelyi Ferenc: *Blockchain a közigazgatásban*. In: Új Magyar Közigazgatás, Budapest, 2017 szeptember, 10. évfolyam 3. szám, pp. 63–69., ISSN 2060-4599

[31] Egy adatbázisnál, ha valami hiba van, az vagy ki se derül, vagy ha egyáltalán kiderül, az adatbázis egy jó részének, vagy a teljes adatbázisnak az átvizsgálása, netán újraépítése szükséges. A blockchain esetében bármilyen hiba azonnal kiderül és egy adott blokk összeállítása, *„lezárása"* után biztosított, hogy az előzmények nem tartalmaznak hibát. Ha mégis, akkor csak addig kell *„visszafejteni"* a blokkláncot.

[32] Megjegyezzük, hogy a számvitel évezredes dolog, a kettős könyvvitel sem mai találmány, Luca Pacioli írta le először *Summa de arithmetica, geometrica, proportioni et proportionalita* c, 1494-ben megjelent könyvében, sőt elvei azóta is változatlan formában használatosak.

Egyenrangú felek közötti – peer-to-peer – kommunikáció

Az egyik ilyen innováció annak elérése, hogy az érintett résztvevők úgy tudjanak kommunikálni, hogy nincs köztük olyan központi szerv, vagy rendszer, amely ezt a kommunikációt, mintegy *„felülről"* vezérelné. Ha kellene ilyen, akkor értelmét vesztené az az igény, hogy a rendszerhez ne legyen szükség megbízható harmadik félre. Igaz, hogy ez a harmadik fél *„csak"* technikai támogatást nyújt, ha a kommunikációt biztosítja, tehát nem érinti a blockchain *„lelkét"*, azonban akkor is egy olyan szükséges dolog lenne, amely a filozófiát tenné kétségessé.

Szerencsére ilyen kommunikációs forma, az ún. peer-to-peer kommunikáció, azaz egyenlő felek közti kommunikáció egy már régen létező technológia. Legismertebb megtestesítői a fájlmegosztók egyik népszerű fajtája, a *„torrent"* rendszerek. Ennek a technikai részleteit jelen cikk keretei közt nem érdemes áttekinteni. Csak annyit érdemes megjegyezni róluk, hogy sok ilyen, kipróbált és jól működő rendszer létezik a világon, valamint azt, hogy itt az ezen rendszerekben alkalmazott kommunikáció típus alkalmazására van szükség. Ez egyszersmind biztosítja, hogy bárki csatlakozhasson az adott blockchain-hez, egyenrangú félként, úgy, hogy nem kell előtte sehova *„bejelentkeznie"*, vagy *„regisztrálnia"* magát valamely központban, hiszen ilyen központ nem létezik. A közösség tagjai mind ugyanilyen szabályrendszeren alapuló szoftvert futtatnak (ezt hívjuk csomópontnak, azaz *„node"*-nak), és automatikusan becsatlakozik az új tag, amikor elindítja saját szoftver rendszerét.

Megjegyezzük, hogy a később tárgyalandó több blockchain típus nem mindegyikében feltétlenül szükséges a peer-to-peer kommunikáció biztosítása, csak az ún. publikus blockchain-nél, mégis mindegyik rendszer erre a technológiára épül.

A kivonat – hash – fogalma

Egy másik innováció, amellyel foglalkoznunk kell, a már fentebb érintett hash kód, és annak elkészítése, generálása. Ez az a kód, amely az adott blokkban lévő tranzakciók összességét, illetve a tranzakciókban lévő adatok sértetlenségét, ha nem is biztosítja, de ellenőrzi. Ilyen ellenőrző összegek egyébként sok helyen előfordulnak egyszerűbb formában, pl. a személyi szám, az adóazonosító jel, illetve a bankszámlaszámok is tartalmaznak ilyen ellenőrző összegeket. Ezek funkciója azonos. Mégpedig az, hogy fény derüljön az egyes hibákra (pl. elírt bankszámlaszám esetén).

Bizonyítható, hogy vannak olyan ellenőrző összegek, amelyek csak jelzik a hibát, de vannak olyanok is, amelyeket felhasználva javítani is lehet azt. A hash kód is hasonló azzal, hogy annak segítségével az eredeti adat nem állítható helyre sőt, ebben az esetben értelmét vesztené. A hash kód ugyanis egy olyan, igen bonyolult algoritmus alapján számolt, megfelelően hosszú számsorból álló ellenőrző összeg, amely gyakorlatilag megjósolhatatlan módon megváltozik, amennyiben azokban az adatokban, amelyekből ez a lenyomat, a hash készült, csak egyetlen egy bitben is megváltozik.

Gyakorlatilag a hash-t előállító algoritmusok (mert természetesen ilyenből is több van[33]), olyanok, hogy visszafelé nem működnek. Azaz, amíg az adott adathalmaz hash kódja az alkalmazott – bár eléggé bonyolult – algoritmussal, viszonylag egyszerűen kiszámolható, addig a hash kódból az eredeti adathalmaz nem található ki.[34] Pontosabban kitalálható, de ehhez irreálisan sok számítási kapacitás igénybevétele szükséges, ráadásul az eredmény nem lenne egyértelmű. Ráadásul, ha a technika fejlődik, és mégis lehetséges reális időn belül és annyi anyagi ráfordítással kitalálni az eredeti szöveget, hogy az mégis csak megérje, addigra kitalálnak egy újabb, sokkal bonyolultabb hash képző algoritmust, és a *„kitalálásra"* szánt technika megint csak hátrányba kerül. Mondhatjuk tehát azt, hogy ez egy egyirányú folyamat, a hash képzése adott adathalmazból, akár szövegből, akár tranzakciókból, de bármilyen más adatból is egyszerű, visszafelé pedig gyakorlatilag lehetetlen.

Sőt, adott hash algoritmus alapján készített hash kód bármilyen méretű adathalmazra kiszámolható úgy, hogy a hash kód hossza ugyanannyi (pl. az SHA256 esetén 256 byte), de gyakorlatilag nem létezik két olyan adathalmaz, amelynek egyezne a hash kódja. Ez a lenyomat tehát egyértelműen azonosítja azt az adathalmazt, amiből készült. Feltéve természetesen, ha tudjuk, hogy mely hash képző algoritmussal állították elő. A hash tehát ujjlenyomat[35] módjára azonosítja azt az adathalmazt, amelyből készítették. A blockchain-ben a hash-t tehát arra használják, hogy egy adott blokkban lévő adatokból képezzenek egy ilyen kivonatot, lenyomatot, amely, mint azt fentebb is jeleztük, méretében sokkal kisebb, mint maga az összes adat, amelyből ez előállt.

A blockchainben tehát ezt a hash-t képezzük az adott blokkban szereplő adatokból, elhelyezzük a blokk végére, és – azért, hogy a lánc kialakuljon – a következő blokk előállításakor ez a hash lesz a következő blokk első adata. Így ez is beépül a következő blokkba[36], következésképpen a lánc logikailag megszakíthatatlan. Viszont ezzel még nem értük el azt, hogy a sok résztvevő, akik mind *„könyvelnek"* ilyen módon, mindig ugyanazt a főkönyvet fejlesszék tovább, hiszen csak egy főkönyvet vezetünk, amelynek lapjai egymás után következnek, és egy lap után csak egy következő lehet. Ezt a főkönyvet tehát mindenkinek látnia kell, és mindenkinek ezen a főkönyvön kell dolgoznia. Ez a mindenki által látott, és mindent tartalmazó főkönyv egységes, minden résztvevőnél ugyanaz a főkönyvi példány van meg. Ezt hívják elosztott főkönyvi technológiának, Distributed Ledger Technology-nak (DLT).

De a hash képzéssel még mindig nem biztosítottuk, hogy csak egy főkönyv, csak egy blokklánc létezzen, mindenféle elágazás nélkül. Ezt kétféleképpen érhetjük el, azaz vagy van egy központi hatalom, amely megmondja, hogy melyik

[33] Ilyen, ma használatban lévő (alap) algoritmusok pl. az SHA256 (pontosabb nevén SHA2-256), az SHA3 (más néven Keccak), a Scrypt, az Ethash, az Equihash, Groestl, X11, Cryptonote, Lyra, Lbry, Blake, Pascal, Skunkhash, valamint ezek különböző változatai.

[34] Pontosabban: algoritmikusan nem számítható ki.

[35] Megjegyzendő, hogy ezt használják pl. az elektronikus aláírásoknál is.

[36] Azaz a következő blokk hash értékének kiszámításához ez az adat is felhasználásra kerül

lesz a következő főkönyvi lap, vagy pedig a központi hatalom kikapcsolásával az egyenrangú *„könyvelők”*, valamilyen módon, valamilyen szabályrendszer alapján döntik el, hogy ki készítheti az új főkönyvi lapot. Ez egyszersmind biztosíték arra is – sőt ez az egyik fő funkciója annak –, hogy az egyes tranzakciók egyszer és csak egyszer kerüljenek bele a főkönyvbe. Pénzügyi szemlélettel vizsgálva ez az a probléma, hogy pl. egy adott összeget a tulajdonosa csak egyszer tudjon elkölteni. Másik szemléletes példa pl. az, hogy egy embernek csak egy születési anyakönyvi kivonata legyen.

Privát és publikus blockchain

Annál a blockchain típusnál, ahol valamilyen központi *„hatalom”* mondja meg a szabályokat, viszonylag egyszerű a dolog a fentiek szerint. Ilyen blockchain-ek léteznek, licence-elt, vagy privát blockchain-nek nevezzük őket.[37] Ezeknek lehet egy, vagy akár több üzemeltetője is, de ez mindenképpen egy zárt, jól definiálható közösség. A közösség tagjai egymás közt, valamilyen algoritmusban megegyezve döntik el, hogy melyikük jogosult megmondani a következő főkönyvi lap tartalmát (ezt pl. un. Proof of Stake (PoS), azaz érdekeltségi alapon döntik el). Ezekkel a blockchain típusokkal a továbbiakban csak érintőlegesen foglalkozunk, figyelmünket a központ nélküli, az egyenlőség elvén működő, ún. publikus blockchain-ekre fordítjuk.

A publikus blockchain-eknél mindenképpen kell tehát valamilyen konszenzus, hogy ki az, aki készítheti a következő blokkot, és mindenki ahhoz fog ezek után igazodni. Ezt a résztvevők olyan konszenzussal határozzák el, hogy az adott blockchain-ben adott szabályrendszert fogadnak el, természetesen konszenzusos alapon. Aki ezt nem fogadja el, azt a többiek – egészen pontosan maga a szabályrendszer – automatikusan kizárják a blockchain-ből.[38] De az is előfordulhat, hogy azok kerülnek többségbe, akik nem fogadják el az adott szabályrendszert, és másikat kezdenek követni. Ezt hívják a szakirodalomban 51%-os támadásnak (51 % attack). Természetesen erre a problémára is van megoldás, mégpedig az, hogy az adott 51%-os támadás esetén kettészakad (ezt fork-nak hívják), és különálló életet kezd élni a két fele egy adott blokktól számítva. Ezután az egyik, vagy másik lánc elsorvadhat, vagy párhuzamosan éli külön életét azzal, hogy valaha közös gyökere volt.

A munkabizonyíték – Proof-of-Work

Ahhoz, hogy ezt a konszenzust hogyan lehet elérni, meg kell ismerkednünk a munkabizonyíték, a Proof of Work (PoW) fogalmával. A Proof of Work ideológiáját és első alkalmazását 1992-ben írta le Cynthia Dwork és Moni Naor[39] és eredetileg a spam-ek, a junkmail-ek kiszűrésére, a spam-elés megnehezítésére, megakadályozására, valamint a szolgáltatás megtagadásos számítógépes támadások [Distributed Denial of Service (DDoS)] ellen fejlesztettek ki. Ennek alapján 1997-ben *Adam Back*[40] alkotta meg az ún. hashcash algoritmust, amely hasonló elven működik. Az alapötlet az az, hogy ahhoz, hogy bizonyos informatikai műveletet végre lehessen hajtani, előbb be kell bizonyítani azt, hogy az illető hajlandó *„foglalkozni”* valamilyen probléma megoldásával azért, hogy ezután megengedjék neki az eredetileg kért művelet végrehajtását. Ez a spam-ek elkerülésénél úgy néz ki, hogy mielőtt elküldünk egy email-t, az email továbbító szerver gép egy viszonylag egyszerű matematikai feladatot ad fel nekünk, pl. hogy adjunk össze két kétjegyű számot. Ez nyilván nem okoz nehézséget a számítógépnek, de mégis pár milliszekundumnyi időt igénybe vesz. Egy email elküldésénél ezt észre sem vesszük, azonban amikor valaki spam-elni akar, és milliós nagyságrendben akar egyszerre email-eket kiküldeni, minden egyes címzetthez való elküldés előtt egy ilyen művelet elvégzése már annyira lelassítja a folyamatot, hogy a spam-elés gyakorlatilag meghiúsul, vagy legalábbis időben nyilvánvalóvá válik a spam-elési szándék az ez elleni fellépésre kifejlesztett számítógépek célszoftverei előtt, és be tudnak avatkozni.

Az egyetlen odaillő szám – nonce

A Proof-of-Work alkalmazása a (publikus) blockchain-ek esetén egészen hasonlót takar. Azonban itt sokkal bonyolultabb feladatot kell megoldani ahhoz, hogy valaki előállíthassa a következő blokkot, majd ezután a közösség minden tagja az ő általa előállított blokkot fogadja el hivatalosnak, és ahhoz csatlakoztassák a következőt. Ehhez tehát a résztvevők (egészen pontosan a fentebb említett csomópontok, azaz node-ok[41]) versenyeznek. A mára már klasszikussá vált Proof-of-Work megoldás tehát egy versenyt generál a résztvevők között (hogy miért hajlandók részt venni a szereplők ebben a versenyben, arról a későbbiekben szólunk). Ez a feladatmegoldó verseny azonban erősen összefügg a fentiekben leírt hash képzéssel is. Egyszerű lenne a dolgunk például kockadobással eldönteni, hogy kinek van joga a következő blokk összeállításához. Azonban sok versenyző esetén ez már bonyolult feladat. Ezért azt találták ki, hogy az adott összeállítandó – tehát még készítés alatt lévő – blokkhoz, a benne lévő adatokon, valamint az előző blokk hash kódján kívül hozzá kell tenni még egy számot (ezt ún. nonce[42]-nak hívják), amelynek a blokkba való beillesztésével és a blokkon ezzel a számmal együtt képzett hash kóddal a teljes készülő blokk

[37] Az SAP cég egyenesen négyféle blockchain típusról beszél a Leonardo nevű projektje keretében. Ezen típusok közül három az általunk csak privát blockchain-nek nevezett kategóriába tartozik (SAP terminológia szerint: konzorciumi blockchain, félig privát blockchain, privát blockchain, ezen felül a publikus blockchain). Lásd: https://www.sap.com/products/leonardo/blockchain.html

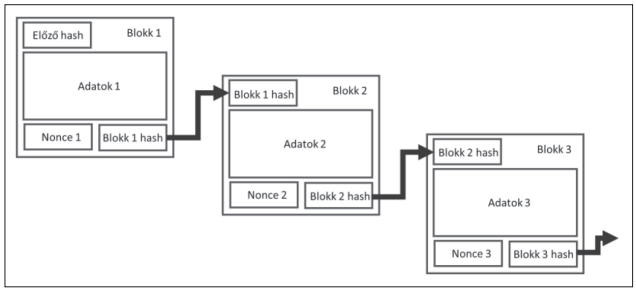
[38] Ez az ún. *„Bizánci generálisok problémája”*

[39] http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp_abs.html

[40] https://en.wikipedia.org/wiki/Adam_Back

[41] Azért e megkülönböztetés, mert a blockchain rendszer résztvevői nem minden esetben node-ok is egyúttal, egy node program futtatása a blockchain rendszernek egy szükséges és elengedhetetlen funkciója, de nincs minden résztvevőnek szüksége node programra (a Bitcoin rendszernél ráadásul megkülönböztetünk full-node-ot, és lite-node-ot is)

[42] Nonce, amely az N once kifejezésből adódik, és azt jelenti, hogy az adott N szám egyszer fordul elő. Ezt kell kitalálni, hogy mi lehet ez az N szám.



2. ábra
Blockchain a nonce-okkal kiegészítve

hash kódja speciális értéket vesz fel: például legyen ennek a megkívánt értéke 8 (nyolc) darab nullával kezdődő. A fent leírtak szerint azonban egy bit adat változtatása a blokkban szereplő adatokon az új létrejövő hash kódot megjósolhatatlanná teszi.

Bányászat – mining

Úgyhogy nincs mit tenni, próbálkozni kell. Méghozzá nagyon sokat kell próbálkozni. Hogy mennyire sokat, arra álljon itt egy példa, amely a blockchain első sikeres, és mára legsikeresebb alkalmazása, a Bitcoin rendszer esetében releváns adat (a bitcoinról és a Bitcoin rendszerről később szót ejtünk még). Ennél az alkalmazásnál az ún. SHA256 hash képző algoritmust használják. A rendszer – minden résztvevő által elfogadott – szabályai viszont megkövetelik, hogy kb. 10 percenként a résztvevők (a versenyzők) valamelyike egy sikeres megoldással álljon elő, azaz egy blokk létrehozására ennyi idő áll rendelkezésre. Ahhoz, hogy ezt a számot, a nonce-ot kitalálják, iszonyatosan sok próbálkozásra van szükség. Ez a cikk írásának idején kb. 10,800,000 terahash másodpercenként (TH/s)[43]. Más néven 10,8 exahash/másodperc, azaz kicsit lefelé kerekítve is 10^{18} hash/másodperc. Kiírva: 10.000.000.000.000.000.000 hash kiszámítása másodpercenként. Ez azért igen sok kockadobással jönne össze. Viszont így biztosítható, hogy kb. 10 percenként mégiscsak feltegye a kezét valaki a résztvevők közül, és az övé legyen a következő blokk, azaz főkönyvi lap. Ekkor mindenki eldobja a saját összeállított blokkját, amelybe egyébként szintén sok munkát ölt, hogy övé lehessen az elsőség, és a folyamat kezdődik elölről.

Jogos a kérdés, hogy rendben, hogy összeállítjuk a blokkot, de mi értelme van? Hiszen mindenki ugyanazt a blokkot szeretné összeállítani. Ez azonban nem így van. Egy adott főkönyvi lap sorai is végesek, így egy blokk mérete is véges, abba csak bizonyos mennyiségű adat fér bele, a Bitcoin rendszerben véges számú tranzakció. De ahogy a rendszer működik, sokkal több tranzakció keletkezik, mint amennyit egyszerre le tudnak könyvelni, és miután minden résztvevő egyenrangú, bárhol is tartózkodik a világon, nem is biztos, hogy időben eljut hozzá minden olyan tranzakció, amelyet valakik egymás között kezdeményeztek. Ezért képzeljük el, hogy a tranzakciók bekerülnek egy nagy fazékba, amelyből mindenki, aki blokkot szeretne létrehozni, egy merőkanálnyi tranzakciót kimer, és azokból, valamint az előző blokk hash kódjából, illetve a fáradságos munkával találomra kiválasztott nonce-szal együtt igyekszik egy blokkot összeállítani.[44] Akinek sikerült ez a művelet, az ő blokkjában lévő tranzakciók véglegesen lekönyvelésre kerültek, az összes többi *„vesztes”* a nála lévő tranzakciókat visszadobja a fazékba, mielőtt a következő 10 perces versenyfutam elindul. Ezt a versenyfutást hívja a szakirodalom mining-nak, azaz bányászatnak, amelyet az aranybányászat mintájára vezettek be (hogy miért hasonlítják ehhez, erről is később szólunk).

Nagyon ritkán előfordulhat, hogy véletlenül ketten, vagy többen is sikeresen állítják össze kis időkülönbséggel a következő blokkot, részben eltérő tranzakciókból. Ők a többi csomóponthoz (node-hoz) igyekeznek eljuttatni saját maguk által összeállított blokkot. A node-ok egy része az egyiket, más része a másikat fogadja el érvényesnek, például azon az alapon, hogy melyikről szerzett először tudomást. Ez esetben a szabályrendszer szerint az lesz a végleges nyertes, akinek a blokkjához adott idő alatt több blokkot csatlakoztattak. Ez manapság azt jelenti, hogy kb. plusz 6, hasonlóan előállított blokk csatlakoztatása egy adott blokkhoz[45] már elég ahhoz, hogy a végleges győztest ki lehessen hirdetni.

Ezzel a módszerrel tehát láttuk, hogy minden résztvevő pontosan ugyanazon a főkönyvön dolgozik, és csak egy főkönyv létezhet. Ez a főkönyv viszont mindenkinél megvan egészen a főkönyv első lapjáig visszamenőleg (ezt hívják genezis blokknak). Tehát egyenlő felek konszenzusos megegyezésén alapszik mindaz, amit ma blockchain-nek nevezünk.

Ezt a konszenzust tehát csak a fentebb már említett 51%-os támadással lehet *„megtörni”*, aminek – mindamellett, hogy nincs sok értelme –, a fenti óriási szám ismeretében igen nagy ára van. Ha viszont még valaki rá is áldozná az összeget, akkor sem érné meg, legalább két dolog miatt. Az egyik az, hogy ez olyan, mint ha valaki összevásárolnál a lottószelvények több mint felét. De attól még lehet, hogy nem ő fog nyerni, hanem valaki más, aki csak egy lottószelvényt vett. Igaz, itt 10 percenként van a *„lottósorsolás”*, így ettől még lehet, hogy megérné a kockázatot. Azonban ahogy kiderül, hogy valaki megváltoztatta a szabályokat az 51 % birtokában, például úgy, mintha a lottó szabályait változtatnánk meg olyan módon, hogy mindig egy valaki nyerjen, akkor többé soha senki nem venne lottószelvényt. Hiszen úgysem nyer, vagy pedig az 51% birtokosa szabhatná meg – teljesen önkényesen –, hogy valaki más nyer-e, vagy sem. Ezért teljesen elértéktelenedne maga a lottózás, nem lenne nyeremény. Itt is hasonlóan történne, azaz mindenki más otthagyná azt a blockchain-t, amelyik így bányászik, és a bányászatért felajánlott *„jutalom”* (lásd később a Bitcoin tárgyalásakor) nem érne semmit. Ezért van az, hogy a publikus blockchain-eknél minden résztvevő csak a mindenki által konszenzusosan elfogadott szabályrendszerben[46] hisz, és azt is csak addig, amíg

[43] https://blockchain.info/charts/hash-rate

[44] A példa kicsit sántít, mert többen is kimerhetik ugyanazt a tranzakciót a fazékból, de ez most részletkérdés.

[45] Ez Bitcoin esetén igaz, más rendszereknél más szám lehet a meghatározó.

[46] Amely szabályrendszer végső soron valamilyen szoftver kódjában ölt testet.

eléggé diverzifikált a résztvevők száma, nehogy valaki erőszakosan megváltoztassa a szabályokat[47].

Arról, hogy egyáltalán miért éri meg ez a verseny, ez a *„játék"*, az alkalmazásoknál még szó lesz, hiszen itt most csak költségekről beszélünk, de hol itt a hozadék, mi végre ez az egész?

A blockchain önmagában mit sem ér alkalmazások nélkül. Voltak már rá próbálkozások, pl. *Wei Dai*[48] az ún. b-money elektronikus pénz projektjét 1997-ben ennek alapján dolgozta ki, felbuzdulva a már említett *Timothy May* kiáltványán. *Wei Dai* viszont pontosan tisztában volt vele, hogy miért teszi mindezt, hiszen a b-money a banki szolgáltatásokat tette volna feleslegessé. Tehát ő a pénzpiaci szolgáltatásokat akarta úgy megoldani, hogy ne kelljen hozzá „megbízható harmadik fél" (trusted 3rd party), azaz ne kelljenek a bankok. Voltak korábban is elektronikus pénz bevezetésére irányuló próbálkozások, az első ilyen ismert *David Chaum*[49] DigiCash projektje 1983-ban, azonban ez még igénybe vette a központok jelenlétét, azaz banki funkcióként szolgálta volna.

A Bitcoin rendszer, mint blockchain alkalmazás

Mindezen kísérletek után az első, és máig az egyik, ha nem a legnagyobb hatású projekt szintén a pénzvilághoz, a központ nélküli fizetéshez, a bankok kikerüléséhez kapcsolódik. Ez pedig a Bitcoin[50] rendszer[51], amelynek saját pénzneme is van, a bitcoin (BTC). Ezt a rendszert 2008. október 31-i keltezéssel, egy *Satoshi Nakamoto*[52] álnéven publikáló, máig nem azonosított személy írta le *„Bitcoin: a Peer-ro Peer Electronic Cash System"*[53] c. híres dolgozatában, amelyet *„Bitcoin White Paper"* néven is ismer a világ. Ennek a rendszernek a bemutatásával kíséreljük meg összefoglalni azokat a további innovációkat, amelyek a blockchain filozófia megértéséhez szükségesek. Hangsúlyozni kell azonban, hogy a blockchain és a Bitcoin rendszer nem ugyanaz. A blockchain egy innováció, amely sok másik innovációval egységes egészbe foglalva több blockchain alkalmazást (implementációt) ad eredményül, melyek közül egy a Bitcoin.

A blockchain-en alapuló főkönyv vezetése előtt tehát már nincs akadály, mindenki pontosan ugyanazt a főkönyvet vezeti, az abba bekerült *„tételek"* tehát mindenki által igazoltan hitelesek. Ez a blockchain legnagyobb előnye. Más kérdés, hogy ennek az az ára, hogy lassan és drágán működik a rendszer. Viszont olyan robosztus, hogy bárki csatlakozik hozzá, vagy szünteti meg csatlakozását, a rendszer stabil és ép marad, a benne tárolt adatok továbbra is ugyanazok minden résztvevőnél, és hitelesnek tekinthetők.

Kérdés azonban, hogy kinek van kedve olyan főkönyvbe adatokat tennie, ahol mindenki mindent lát? Így az adatok, illetve a tranzakciók bizalmassága nem biztosított. Hogyan lehet mégis megoldani azt, hogy bár mindenki által hitelesítve legyen egy tranzakció, egy adathalmaz, azokat mégis csak azok tudják értelmezni, akikre az tartozik?

Nyílt kulcsú rejtjelezés – public key cryptography

A fenti kérdés megoldása szintén, egy már létező technológiai innováció, a nyilvános kulcsú rejtjelezés (public key cryptography (PKC)), valamint az erre épülő infrastruktúra (public key infrastructure (PKI)) alkalmazása[54]. Ennek a rendszernek az alapjait *Whitfield Diffie*[55] és *Martin Hellman*[56], valamint tőlük függetlenül *Ralph Merkle*[57] tette le, még 1978-ban. Ezeket a rendszereket alkalmazzák ma is pl. az elektronikus aláírásnál is, de egyszerű titkosításra is alkalmazzák. A legismertebb, és legtovább – még ma is – alkalmazott megoldás *Ron Rivest*[58], *Adi Shamir*[59] és *Leonard Adleman*[60] nevéhez fűződik, ezt a szerzők nevének kezdőbetűjéből alkotott mozaikszó alapján ma mindenki RSA[61] algoritmusnak nevezi. Ez a rendszer azonban jogilag védett[62] módszert, algoritmust használ, valamint hierarchikusan működik, így *Philip Zimmermann*[63] kitalált egy ugyanilyen algoritmuson működő, de központ nélküli rendszert, a PGP-t, amely a *„pretty good pri-*

[47] Megjegyzés: Ezt az igen nagy árat mind számítástechnikai kapacitásban, megfelelő célszámítógépek alkalmazásának árában, mind az általuk felhasznált óriási mennyiségű áram felhasználásában lehet mérni. A mai célhardverek kb 10-13 terahash/másodpercet (TH/s) tudnak. (Ilyen pl. a Bitmain nevű, kínai vezető gyártó Antminer S9-es típusjelzésű gépe. Ezeket a célgépeket ASIC-nak (Application Specific Integrated Circuit), magyarul BOÁK-nak (Berendezés Orientált Áramkör) hívják, ezzel is utalva arra, hogy egy ilyen gép semmi mást nem tud, csak amire kifejlesztették.) Ha pl. 10TH/s-nek veszünk egy gépet, akkor a hálózat fentebb említett kapacitása kb. darab 100 000 ilyen gépet jelent. Az 51%-os támadáshoz valakinek legalább a felével rendelkeznie kell a kapacitásnak, tehát, ha a hálózaton csak ilyen csúcsgépek dolgoznának, akkor is több, mint 50 000 ilyen gép kellene hozzá. Mai áron egy ilyen gép ára kb. 3000 USD, azaz mintegy 150 millió USD egyszeri befektetést igényelne azzal, hogy a gépek kapacitása rohamosan fejlődik, és mire megérné ezekkel a gépekkel elkövetni az 51%-os támadást, már régen nem érné meg. És akkor még nem beszéltünk az ezen gépek által fogyasztott villamos energiáról, amely 0,1 USD/kWh árral számolva, valamint gépenként 1,2 kWh fogyasztást véve havi 4,3 millió USD villanyszámlát jelentene. Az USA-ban kb. 0,1 USD/kWh a villanyáram ára, de pl. Kínában vagy Izlandon sokkal olcsóbb. Magyarországon jelenlegi árfolyammal számolva 0,14 USD/kWh jön ki, ami 40 %-kal drágább, mint az USA árai.

[48] https://en.bitcoin.it/wiki/Wei_Dai

[49] https://en.wikipedia.org/wiki/David_Chaum

[50] Ha a Bitcoin rendszerre hivatkozunk, azt nagy *„B"*-vel írjuk, magát a bitcoin-t, mint a rendszeren belüli fizető eszközt pedig kis *„b"*-vel.

[51] A téma iránt érdeklődőknek lásd: Andreas M. Antonopoulos: *Mastering Bitcoin, 2nd Edition* – https://www.bitcoinbook.info/

[52] https://en.wikipedia.org/wiki/Satoshi_Nakamoto – bár többen szóba jöttek már, hogy ők rejlenek az álnév mögött (Hal Finney, Nick Szabo, Wei Dai, stb.), meg nem erősített hírek szerint eddig csak az amerikai NSA-nek sikerült azonosítania egy négy fős csoportot idén augusztusban, hogy ők állhatnak a név mögött. Erről azonban még folyik a vita, annak ellenére, hogy Satoshi Nakamoto 2013 óta már nem publikál, visszavonult, és a Bitcoin – nyílt forráskódú – kódját a közösségre hagyta.

[53] https://bitcoin.org/bitcoin.pdf

[54] A téma iránt érdeklődőknek lásd: Bruce Schneier: *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source*, John Wiley & Sons, 1996, ISBN: 0471128457

[55] https://hu.wikipedia.org/wiki/Whitfield_Diffie

[56] https://hu.wikipedia.org/wiki/Martin_Hellman

[57] https://en.wikipedia.org/wiki/Ralph_Merkle

[58] https://en.wikipedia.org/wiki/Ron_Rivest

[59] https://en.wikipedia.org/wiki/Adi_Shamir

[60] https://en.wikipedia.org/wiki/Leonard_Adleman

[61] https://hu.wikipedia.org/wiki/RSA-elj%C3%A1r%C3%A1s

[62] A védelem 1999-ben járt le.

[63] https://hu.wikipedia.org/wiki/Philip_R._Zimmermann

vacy" szavak mozaikszava. Ez utóbbi lényege, hogy a benne szereplő felek, mintegy *„kulcskarikán"* gyűjtik mindazoknak az ún. nyilvános kulcsait, akikben ilyen, vagy olyan módon megbíznak. Azaz itt nincs meg az a típusú hierarchia, amely a fenti rendszer alapvető működési feltétele.

De mivel az innováció innovációt szül, így mára már az RSA és az ahhoz hasonló algoritmusok (pl. a fenti *Diffie–Hellmann*[64], vagy DH algoritmus) kissé elavultnak tűnnek, és bevezetésre került, egyre jobban terjed az ún. elliptikus görbéken alapuló, nyílt kulcsú rejtjelezés [elliptic curve cryptography (ECC)[65]], amely ugyanazt a biztonsági szintet gyorsabb algoritmussal, és főleg rövidebb titkosító/megfejtő kulcspárral tudja elérni. De mi is ez egyáltalán?

Maga a nyílt kulcsú rejtjelezés abból az igényből fakad, hogy a régi, ún. szimmetrikus kulcsú rejtjelezésnél a kommunikáló felek titkos kommunikációjának indítása igen nehézkes volt. Szükségszerűen találkozniuk kellett egyszer vagy személyesen, vagy megbízható futár útján, hogy megbeszéljék, hogy hogyan, és milyen rejtjelező kulccsal fognak titkosan kommunikálni[66]. Ebben az időben a rejtjelezés, és a rejtjelezett kód megfejtése ugyanazzal a kulccsal történt. Ennél a megoldásnál azonban a lebukás veszélye igen nagy volt, hiszen, ha valaki megszerezte a kulcsot, az egész kommunikációt észrevétlenül le is tudta hallgatni (lásd a II. világháború német Enigma rejtjelező gépét, és annak az angol *Alan Turing*[67] és csapata általi megfejtő gépét, az Ultrá-t). Másrészt ma, az internet korában az, hogy előre találkozni kelljen és meg kelljen beszélni, hogy mi a rejtjelezés/megfejtés kulcsa, szinte elfogadhatatlan, különösen, ha a kommunikáló felek távol vannak egymástól, sőt, lehet, hogy nem is ismerik egymás személyesen.

A nyílt kulcsú rejtjelezés erre nyújt megoldást, mégpedig úgy, hogy olyan, eléggé bonyolult matematikai műveletsoron alapuló rejtjelezési technikát dolgoztak ki, ahol az adott üzenet, adatcsomag titkosítása nem ugyanazzal a kulccsal történik, mint annak megfejtése. Ez elsőre furcsán hangozhat, de vannak ilyen eljárások. Sőt, a rejtjelezéshez használt kulcsból soha[68] nem jósolható meg, vagy számolható ki a megfejtésre használatos kulcs, és ez viszont is igaz. Ráadásul igaz az is, hogy egy rejtjelező kulcshoz pontosan egy[69] megfejtő kulcs tartozik. Ezt a két kulcsot, azaz kulcspárt viszont elő lehet állítani egyszerre.[70] De aki ezt a kulcspárt előállítja, az a megfejtő kulcsot (az ún. privát kulcsot) magánál tartja, azt nem adja ki senkinek, semmi körülmények között, a másikat, a rejtjelező kulcsot (az ún. nyílt, vagy publikus kulcsot) pedig mindenkinek elérhetővé teszi (pl. az interneten). Mire jó ez? Arra, hogy a kulcspár előállítójának, azaz a privát kulcs gazdájának bárki tud titkosított üzenetet küldeni, hiszen a publikus kulcs mindenkinek a rendelkezésére áll, de az üzenetet megfejteni csak az tudja, aki rendelkezik a privát kulccsal. Azaz úgy lehet üzenetet küldeni, hogy a feleknek soha nem kellett találkozniuk, megbeszélni, hogy mi legyen a közös titkosító, illetve megfejtő kulcs. Ahhoz azonban, hogy az illető válaszolni is tudjon az üzenetre, a másik félnek is rendelkeznie kell ilyen kulcspárral, amelynek publikus tagját szintén mindenki ismeri. Ha a felek biztosak lehetnek abban, hogy tényleg egymásnak küldenek üzenetet (ezt biztosítja pl. a hierarchikus PKI rendszer), akkor a titkosított kommunikáció bármely két résztvevő között biztosított.

Elektronikus aláírás

Mielőtt a nyílt kulcsú rejtjelezésnek a Bitcoin rendszeren belüli alkalmazását taglalnánk, néhány mondatban az elektronikus aláírást is tárgyalnunk kell. Az elektronikus aláírást ma már egyre többen használják, anélkül akár, hogy tudnának róla. Ma már ilyen minden egyes alkalmazás, amelyet, pl. Windows operációs rendszerre telepítünk, a fejlesztője által elektronikusan „alá van írva", ezzel is biztosítva, hogy az nem vírusos, a készítőjétől származik stb.

De mi is az elektronikus aláírás? Jogi értelemben az is, ha pl. egy általam elküldött e-mail üzenet alá odaírom a nevemet, de ez attól még nem biztosítja azokat a funkciókat, amiért az elektronikus aláírást kitalálták. Funkciója az, hogy az adott adathalmaz (pl. e-mail üzenet, programkód, egyéb adat) hitelességéről adjon biztosítékot, azaz igazolja, hogy az *„aláírt"* adat nem sérült, sőt igazolja, hogy az a küldőjétől származik, sőt, a küldő által letagadhatatlan, ráadásul mindezt bárki tudja ellenőrizni. Az elektronikus aláírás tehát nem arról szól, hogy titkosan küldjünk adatokat, hanem arról, hogy amit küldünk, az egészen biztosan hiteles legyen mindenki számára elfogadhatóan.

Az elektronikus aláírás a nyílt kulcsú rejtjelezésen alapszik, csak pontosan fordítva, mint ahogyan rejtjelezünk. Mindamellett felhasználja még a fentebb taglalt hash algoritmusokat is. Az elektronikus aláírás tehát nem az, hogy ezt és ezt az adatot én saját kezűleg aláírtam, hanem az „aláíráshoz" nyílt kulcsú rejtjelezést használtam.

A működés a fentiek ismeretében nem olyan bonyolult. Tegyük fel, hogy szeretnénk egy elektronikusan kelt szerződést, vagy nyilatkozatot elektronikusan aláírni. Itt fontos az a feltétel, hogy az a szerződés vagy nyilatkozat elektronikusan létezzen. Ahhoz, hogy ezt az aláírást megtegyük, mindenekelőtt készítenünk kell egy kulcspárt, méghozzá olyat, amelyet elektronikus aláíráshoz fogunk használni, nem pedig rejtjelezéshez (hogy miért, az jelen szempontból lényegtelen, de amúgy fontos kritérium). Amikor előállítottuk a kulcspárt, akkor nem a szerződést, vagy nyilatkozatot titkosítjuk vele, hiszen itt nem az a lényeg, hogy azt senki se tudja el-

[64] https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

[65] https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

[66] Ezt úgy nevezik, hogy a kulcsot valamilyen megbízható, de amúgy *„nyílt csatornán"* kellett kicserélni.

[67] Alan M. Turing a modern számítástudomány egyik atyja, aki a kiszámíthatóság elveit is lefektette (Turing-gép). Róla nevezték el az ún. Turing tesztet, amely olyan kérdések sorozatát feltételezi, amelyből kideríthető, hogy a kérdésekre választ adó az ember, vagy pedig mesterséges intelligencia. Lásd még: https://hu.wikipedia.org/wiki/Alan_Turing

[68] Illetve igen hosszú idő alatt számolható csak ki, ami – tekintve a számítástechnika jelenlegi fejlettségét, milliárd években mérhető.

[69] Pontosabban egy jól meghatározott matematikai halmazba, ún. *„maradékosztály"*-ba tartozó kulcs.

[70] Egészen pontosan, ha a kulcspár titkos (privát) kulcsát sikerül előállítanunk, abból a nyílt (publikus) kulcs előállítható, fordítva viszont nem, azaz a publikus kulcsból a privát kulcs nem állítható elő.

olvasni a címzetten kívül, hanem az, hogy mindenki meg tudjon győződni annak betű szerinti hitelességéről, és arról, hogy az „aláírás" és csak annak a szerződésnek/nyilatkozatnak az aláírása tőlünk származik. Mindezekért a szerződés/nyilatkozat adattartalmából valamilyen hash algoritmussal létrehozunk egy hash kódot (zanzát, lenyomatot, kivonatot, a fentiek szerint). Az, hogy mely algoritmust használtuk, azt mindenképpen nyilvánossá kell tennünk, mivel ennek ismerete nélkül senki nem fogja tudni ellenőrizni az aláírásunkat. Most, hogy a hash kód, mint a szerződés/nyilatkozat fix hosszúságú kivonata rendelkezésünkre áll, ezt, és csak ezt a hash kódot fogjuk az előzőleg elkészített kulcspárunk titkosító (privát) kulcsával titkosítani. Azaz jelen esetben nem az titkosít, aki nekünk akar üzenetet küldeni, hanem mi titkosítunk. De csak a hash kódot. Ezek után elküldjük az érdekelt másik feleknek, de akár az egész világnak a szerződésünket/nyilatkozatunkat, hozzácsatolva az immár titkosított hash kóddal. Így az elektronikus aláírás már rendelkezésre áll, azaz a szerződés/nyilatkozat a részünkről elektronikusan alá van írva.

A mi elektronikus aláírásunk bárki más általi ellenőrzése viszonylag egyszerű. A világ ismeri a mi publikus kulcsunkat, amelyet ez esetben a megfejtésre lehet használni, valamint ismeri a szerződést/nyilatkozatot, amelyet aláírtunk, a mellé küldött, titkosított hash kóddal együtt, és végül ismeri azt a hash algoritmust, amellyel a szerződésünk hash kódját (kivonatát) elkészítettük. Mindezek után bárki, aki ellenőrizni akarja elektronikus aláírásunkat, nincs más dolga, mint ugyanazzal a hash algoritmussal, amellyel mi elkészítettük a szerződésünk/nyilatkozatunk hash kódját (kivonatát), ő is megteszi ugyanezt. Neki akkor elő fog állni egy hash kód, amely – ha minden jól megy – ugyanaz lesz, mint amelyet mi készítettünk eredetileg a szerződésből/nyilatkozatból, még a hash kód titkosítása (azaz aláírása) előtt. Ezután az, aki ellenőrizni akarja elektronikus aláírásunkat annyit tesz, hogy előveszi a szerződésünkhöz/nyilatkozatunkhoz csatolt, általunk titkosított (azaz aláírt) hash kódot, és a rendelkezésére álló publikus kulcsunkkal megfejti azt. Ha tényleg mi voltunk az aláírók és semmi sem sérült meg (szándékosan, vagy véletlenül) a szerződés /nyilatkozat szövegében, akkor az a hash kód, amelyet épp most fejtett meg, és az a hash kód, amelyet saját maga állított elő a szövegből, teljes egészében meg fog egyezni. Ezzel igazolttá vált, hogy az elektronikus aláírás tőlünk származik és a bizonyítottan sértetlen dokumentumot sajátunknak ismerjük el.

Természetesen jogos a kérdés, hogy honnan tudjuk, hogy az, aki aláírt, és a világnak elküldte a publikus kulcsát, azok tényleg mi vagyunk. Azaz ténylegesen ki az aláíró személye? Erre több megoldás kínálkozik. A legelterjedtebb egy hierarchikus rendszer, ahol, mintegy telefonkönyvben fel vannak sorolva az egyes aláírók publikus kulcsai, egyéb azonosítóikkal együtt, és mindezt egy megbízható harmadik fél tartja nyilván (hitelesítés szolgáltató – Certification Authority – CA). Ez azonban hangsúlyozottan egy hierarchikus rendszer, ahol ezek a megbízható harmadik felek egymásról is igazolják egymás valódiságát, és/vagy egy végső, pl. állam által felügyelt harmadik fél az, aki minden ilyen igazolót viszontigazol (ez az u. n. gyökér hitelesítés szolgáltató – root CA). Van olyan megoldás is, ahol már a kulcspár előállítását is *„felügyelik"*, ezek a regisztrációs szolgáltatók (Registration Authority – RA). Ez a rendszer a nyílt kulcsú infrastruktúra (PKI) része. Azonban létezik olyan megoldás is, mint a korábbi fejezetben már bemutatott PGP rendszer, ahol mindenféle hierarchia nélkül az egyes aláírók egymásról igazolják, hogy melyik kinek az aláírása. Sőt, van olyan rendszer, ahol az aláíró hitelesítésére semmi szükség, elég, ha az aláíró felek tudják egymásról, hogy melyik kinek az aláírása.

Ez utóbbit használja a Bitcoin rendszer[71], hiszen ebben a rendszerben, amikor a felek egymásnak *„pénzt"* küldenek, nem a személyazonosság igazolására van szükség, hanem arra, hogy az egyik féltől a másikhoz megérkezzen a bitcoin. Ha valaki rossz tranzakciót indított, az nem fog megérkezni a másik félhez, rossz esetben valaki máshoz viszont megérkezik. A Bitcoin rendszerben tehát mindenki a saját digitális aláírásáért felelős, pontosabban annak titkos (privát) kulcsáért. Ez az a kulcs, amelyet a Bitcoin rendszerben *„pénztárca"* alkalmazásban (wallet) tárolnak, és jelszóval védve titokban tartanak a felhasználók. Ha ez elvész, soha többet nem jutunk a pénzünkhöz (olyan, mintha elvesztenénk a pénztárcánkat), ha ellopják a kulcsunkat (pl. a mobiltelefonunkkal együtt, amelyben bitcoin pénztárcánkat nem őriztünk gondosan jelszóval), akkor az olyan, mintha ellopták volna a készpénzzel teli pénztárcánkat.

Anonimitás és privacy a Bitcoin rendszerben

A Bitcoin esetében ezt a rendszert használják fel ahhoz, hogy bár mindenki tudja ellenőrizni a blockchain-ben, mint főkönyvben lévő tranzakciók hitelességét, valódiságát, mégsem tudják megmondani, hogy kik, és milyen célból cseréltek adatokat, a bitcoin esetében ún. kriptopénzt. Az adatok tehát látszanak, hitelesek, csak azt nem lehet tudni, hogy kik vannak mögöttük, kivéve természetesen azokat, akik a tranzakciók szereplői. Mélyebb részleteket is taglalhatnánk, azonban a lényeg megértéséhez most elég ennyi azzal kiegészítve, hogy a tranzakciókban részt vevő felek a Bitcoin rendszer esetén egy majdnem, hogy véletlenszerűen generált adatsorral azonosítják magukat. Ezeket a véletlen számokat azonban a másik fél tudomására hozzák, hogy feljogosítsák őket arra, hogy nekik kriptopénzt (bitcoint) utalhassanak. Ezt az azonosító adatsort nevezik pénztárcának a Bitcoin rendszerben, és erre az adatsorra kell hivatkozni, ha valaki utalni szeretne nekünk bitcoint, természetesen a fentiek szerint elektronikusan aláírva a tranzakciót. És ez minden irányban működik, hiszen, ha én szeretnék utalni valaki másnak, meg kell tőle kérdeznem az ő pénztárcájának a hosszú, gyakorlatilag megjegyezhetetlen karaktersorozatát (Bitcoin rendszerben pl. így néz ki egy ilyen pénztárca cím: 3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r[72], vagy pl. a 14KtKV6iw8SRZbgJpDJxTjuMH-

[71] Egészen pontosan az elliptikus görbékre alapuló digitális aláírási rendszert (Elliptic Curve Digital Signature Algorythm – ECDSA)

[72] Ez egy létező cím, a Bitfinex kriptotőzsde ún. *„Cold Wallet"*-je, amely ma a világon a legtöbb bitcoint tartalmazó „pénztárca", jelenleg több, int 165 000 bitcoinnal (kb. 1 milliárd USD). Lásd: https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html

nhi65mhoX[73] pénztárca azonosító is), és az elektronikus aláírás funkció igénybe vételével bármikor tudok neki küldeni kriptopénzt. Ezt a tranzakciót pedig a blockchain rendszer a fentiek szerint egyszer és mindenkorra lekönyveli, úgyhogy az letagadhatatlan, a dolog ezzel el is van intézve.

Duplán költés – double spending

A blockchain könyvelési rendszere ráadásul megoldást ad egy fő problémára, az ún. kétszer történő költés (double spending) megakadályozására, illetve megelőzésére. Míg a fizikai világban, ha átadunk egy bankjegyet, vagy értékpapírt, árut valaki másnak, az már fizikailag nála lesz, ő birtokolja, mi pedig a továbbiakban nem. Az információs rendszereknél azonban ez nincs így, egy adott adathalmazt mindenki le tud másolni és mindenkinél meglesz, annál is, akiről másolták, és azoknál is, akik lemásolták.

Amennyiben a bitcoint fizetési eszközként szeretnénk felhasználni, meg kell akadályozni, hogy egy adott bitcoint, amelyet egy, a fentiek szerint titkosított hosszú adatsor testesít meg, kétszer is *„el lehessen költeni”*. A blockchain elosztott, mindenki (pontosabban minden csomópont, node[74]) által átnézett[75] könyvelési rendszere pontosan ezt biztosítja. Ha egy adott bitcoint megtestesítő adatsort már egyszer felhasználtak egy tranzakcióban, azt többé már nem lehet, hiszen csak egy főkönyv van, és abban minden tranzakció szerepel, és mindegyiket ellenőrizték, azaz *„lekönyvelték”* egy blokkban[76]. Így végeredményben maga a szabályrendszer (a protokoll) biztosítja azt, hogy az internet világában létezhessen pénzhez hasonló tulajdonságokkal rendelkező fizetési eszköz, mindez úgy, hogy a fizikai világban nem létezik. Ezért mondják azt, hogy a rendszer mögött *„csak”* a matematika, a konszenzuson alapuló protokoll betartása van, az ebben a világban létező pénznek nincs semmi más fedezete (se arany, se valamilyen fizikai pénz, ún. fiat).

Ezzel gyakorlatilag végére értünk a blockchain, és az azon alapuló egyik fő alkalmazás *„madártávlatból”* történő technikai, technológiai ismertetésének. De mire jó ez az egész? Pl. bitcoin esetében mitől lesz bármilyen értéke is ennek a kriptopénznek, vagy kriptovalutának?

A bitcoin használata

Eleinte, 2009-ben, amikor a Bitcoin rendszer első számítógépes kódját, mint nyílt forráskódot közzétették, a bitcoinnak még gyakorlatilag semmi értéke sem volt. Azonban az idő múlásával elkezdték ezt használni, és bitcoint venni igazi valutáért (fiat-ért), bitcoint adni fiat-ért, árut cserélni bitcoin értéken, sőt a blockchain könyvelési rendszer könyvelőit is *„kifizetni”* velük pár tized vagy század százalékért minden egyes tranzakcióból. Így már kezd érthetővé válni, hogy miért is van az, hogy egyre többen szeretnének könyvelni, hiszen bitcoint kapnak fáradozásuk után. Méghozzá úgy, hogy azt, hogy ezt a *„jutalékot”* megkapják, a rendszer szintén automatikusan biztosítja, ugyanolyan tranzakcióként, mint azt a tranzakciót, amelyet éppen lekönyvelnek, azaz blokkba építenek.[77]

A bányászat jutalma – mai aranyláz

Van a rendszernek még egy sajátossága, mégpedig az, hogy a mindenki által betartott szabályrendszer szerint minden egyes blokk sikeres összeállítása (a fentiek szerint *„kibányászása”*) után a rendszer a *„semmiből”* generál egy kriptopénz (bitcoin) jutalmat annak, aki az adott blokkhoz sikerrel megtalálta a fent már leírt *„megoldást”*. Azaz annak, aki megtalálta azt a számot, a nonce-t, amellyel a blokk végső hash kódja a kívánt tulajdonságokkal rendelkezik (emlékezzünk: pl. nyolc darab nullával kezdődjön). Ez a jutalom nem kevés: a rendszer indulásakor még 50 bitcoin volt, amely akkor még nem sokat ért, de akik hittek benne, ezért is hajlandók voltak bányászni. A rendszer úgy van megállapítva, hogy bizonyos időközönként (pontosabban minden 216.000 blokk kibányászása után) a jutalom már csak a fele legyen. Ez eddig kétszer történt meg, legutóbb 2016-ban, így ma egy blokk *„kibányászásáért”* már csak 12,5 bitcoin a jutalom[78]. A jutalom következő *„felezése”* 2020 júniusára várható. A rendszer úgy van kitalálva, hogy végül összesen 21 millió bitcoin legyen, sem több, sem kevesebb. Ezt ezzel az időnkénti felezős módszerrel érik el, és a jóslatok szerint kb. 2050-ben kerül sor arra, hogy mind a 21 millió bitcoin rendelkezésre álljon a rendszerben. Ez hasonló ahhoz, amikor az adott ország jegybankja csak adott mennyiségű készpénzt nyomtat, illetve veret, egyébként elszabadulna az infláció (arra most ne térjünk

[73] Ez utóbbi a szerző egyik saját pénztárca azonosítója.

[74] A Bitcoin rendszerben a teljes főkönyvet a már említett nulladik, vagy genezis blokktól számítva csak az ún. teljes csomópontok, (full-node-ok) tartalmazzák. Ezek képesek arra, hogy a blokkokat végigellenőrizzék, és állandóan *„szinkronban”* maradjanak a rendszerrel, tehát minden ilyen full-node-nál pontosan ugyanaz a blockchain, mint adathalmaz legyen meg. Ez az egyik fő előnye a rendszernek, hogy ha egy node-ot kiiktatunk, még mindig rengeteg helyen lesz meg az a bizonyos *„főkönyv”*. A rendszer tehát rendkívül megbízható, robosztus. A cikk írásának az idején a világon több, mint 11 ezer full-node működik, ebből Magyarországon jelenleg 37 full-node. Lásd: https://bitnodes.earn.com/#global-bitcoin-nodes-distribution. A full-node-ok száma folyamatosan változik, de eléggé elosztott geográfiailag ahhoz, hogy a rendszer igen megbízhatóan, gyakorlatilag heti 7×24 órában működjön. (A szerző is futtatott egy ideig full-node-ot, tesztelési céllal, de bányászási funkciók nélkül).

[75] A könyvelés átnézését nem úgy kell elképzelni, hogy egyszerre minden node-nál rendelkezésre áll minden tranzakció, amit le kell könyvelni. A tranzakciók *„szétterjedése”* a hálózaton egy folyamat, amelyet a résztvevők biztosítanak a fentiekben leírt peer-to-peer kommunikáció révén, és a full-node-ok azok, amelyek – azon felül, hogy ők a tranzakciók fő szétosztó csomópontjai – beillesztik ezeket a blockchain-be.

[76] A blockchain a blokkokat folyamatos sorszámmal látja el, és úgy tekinti, mintha egymásra tették volna a blokkokat (hasonlóan a téglákhoz), ezért az aktuálisan elkészült blokk számát a blokk *„magasságának”* hívják.

[77] Azzal a különbséggel, hogy ebből a tranzakcióból már nincs további jutalék, különben a végtelenségig osztódna a jutalék, és egy tranzakció könyvelésével lenne elfoglalva az egész rendszer – ez hasonlít a klasszikus teknősbéka és a futó esetéhez.

[78] Lásd: http://www.bitcoinblockhalf.com/

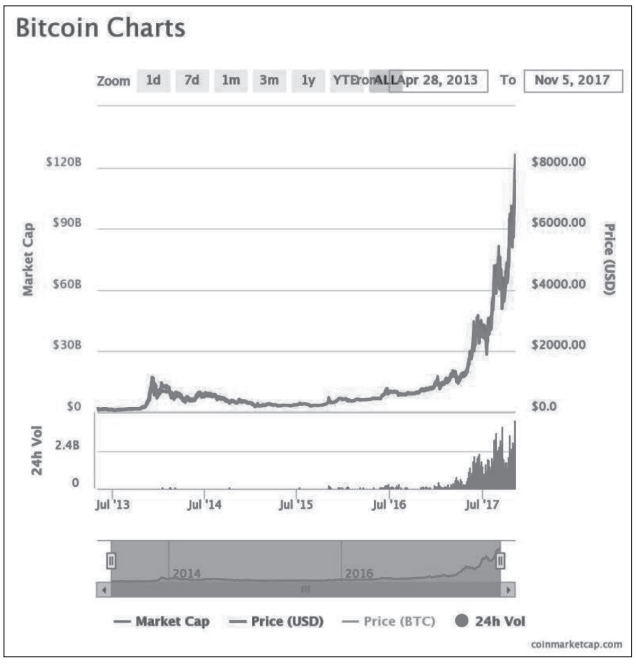
ki, hogy ebben a bitcoin világban mit is takarhat egyáltalán az infláció fogalma).

A használat erősödése

Az idők folyamán egyre inkább kezdték használni a bitcoint, mint olyan fizetési eszközt, amelyhez nem kellenek a bankok, biztonságos, azaz tényleg végrehajtódik a tranzakció, és tényleg csak egyszer, valamint nem mellékesen az egymásnak fizető felek kiléte titokban marad (a fizetett összeg nem, hiszen azt könyveli a rendszer). Ezért nem más, mint az alvilág kezdte el használni a pénzt a fegyver- és drogkereskedők, de még a ma *„divatos"* számítógépes zsaroló vírusok is bitcoinban kérik a fizetséget, vagy, ha úgy jobban tetszik, a váltságdíjat. A felek utalnak egymásnak, az árumozgást akkor bonyolítják le, ha a blockchain rendszer lekönyveli a tranzakciót, és mindez mindenféle felső hatalom, központ, bank, pénzintézet előtt titokban zajlik. Ez az, amiért elkezdték használni a bitcoint adóelkerülési céllal is, hiszen ez kiváló eszköze volt a pénzmosásnak, illetve a pénz eltüntetésének, a világ másik felére történő, nyomtalan transzferálásának, azaz átutalásának). Ez viszont igencsak kezdte felértékelni a bitcoint. Mindamellett a bányászatért kapott jutalom is egyre többet ért. Sőt, elkezdték használni a bitcoint még egy dologra, induló (startup) cégek finanszírozására, amely tovább növelte a bitcoin értékét, de erre később még visszatérünk.

A bitcoin piaci kapitalizációja és árfolyama

Amíg 2010-ben valaki 10 ezer bitcoinért tudott venni két pizzát, ez mai árfolyamon 57 millió USD-nek, közel 16 milliárd forintnak felelne meg. Egy bitcoin árfolyama a cikk írásakor kb. 5700 USD. Így a blokk bányászatért történő 12,5 bitcoin sem ér keveset, ez ma kb. 20 millió forint. És mivel átlagosan 10 percenként kerül egy blokk kibányászásra (azaz lezárásra), az azt jelenti, hogy 10 percenként nő a rendszer piaci kapitalizációja 71,250 USD-ral, azaz kb. 20 millió forinttal. Így nem csoda, hogy a cikk írásakor a Bitcoin rendszerben lévő bitcoinok teljes piaci kapitalizációja USD 94,770,872,359, azaz majdnem 100 milliárd USD, amely megegyezik egy közepesnél nagyobb multi vállalat piaci kapitalizációjával. Ami ebben az érdekes, az az, hogy milyen ütemben növekszik ez a kapitalizáció.



3. ábra
A bitcoin piaci árfolyamának alakulása
Forrás: coinmarketcap.com

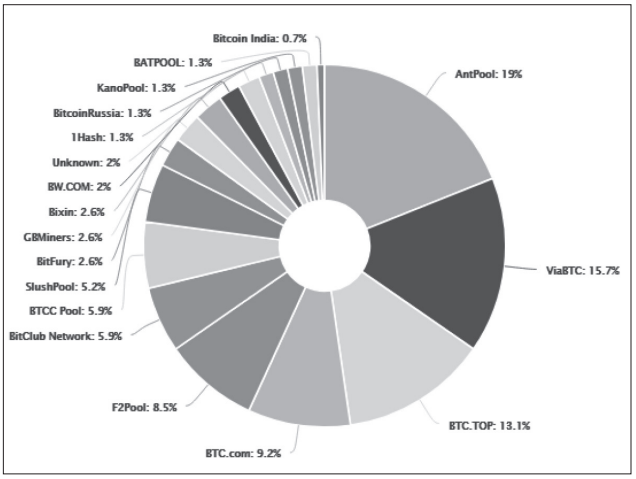
Ez az az összeg azért már igen jól *„látható"*, még akkor is, ha ma nem tudjuk, hogy a matematikai algoritmuson kívül mi mögötte a *„fedezet"*, ha egyáltalán van ilyen. Nyilvánvalóan van kereslet/kínálat, hiszen nem értékelődött volna fel így a bitcoin árfolyama pár hónap alatt. Jellemző, hogy az árfolyam 2016 októberében még csak kb. 600-650 USD volt, 2013-ban pedig csak 150 USD. Ez másként kifejezve azt jelenti, hogy 2016 és 2017 októbere között a bitcoin mintegy 1000%-os hasznot hozott, 2013 és 2017 október között pedig 4000%-os hasznot hajtott[79].

Mindenki könyvelni/bányászni akar – farmok, pool-ok

Nem csoda tehát, ha a bitcoin blockchain alapú könyvelési rendszerébe is egyre többen szállnak be, immár nem önkéntes könyvelőként, hanem az óriási haszon reményében, mivel a könyvelők egyben a bányászok is, és tranzakció is egyre több van. Ez így azt is jelenti, hogy egy-egy blokk kibányászásához egyre nagyobb számítástechnikai kapacitás áll rendelkezésre, mégis tartani kell azt a szabályrendszer szerint, hogy kb. 10 percenként kerüljön csak egy blokk kibányászásra (egyébként tényleg elszabadulna az infláció a Bitcoin rendszerében, ha másodpercek alatt, ráadásul ismétlődően lehetne hozzájutni mintegy 20 millió forinthoz). Ezért a szabályrendszer úgy lett megalkotva, hogy akármekkora is a számítási kapacitás, amely a blokk kibányászásához tartozó feladatot megoldja, a feladat nehézségének (bonyolultságának) automatikus változtatásával egy blokk még így is kb. 10 perc alatt lesz kibányászva, és így lezárva. Ez azt jelenti, hogy olyan nonce számot kell találni, amely már nem 8 darab nullát biztosít az adott lezárandó blokk hash kódjának elején, hanem pl. 10-et, 12-t, vagy akár többet is.

Azonban ne higgyük, hogy ez az óriási számítástechnikai kapacitás, ami a bányászathoz kell, mind egy-egy jól meghatározott helyen áll elő. Eleinte ez így volt (ezt hívják *„solo mining"*-nak), de a fentiek miatt már az egyes csomópontok mögött lévő, és kifejezetten erre a célra létrehozott (és

[79] Julian Assange, a WikiLeaks alapítója külön megköszönte az USA kormányának, hogy minden pénzintézetnek megtiltotta, hogy a WikiLeaks felé bármilyen tranzakciót végrehajtson. Ezért a WikiLeaks bitcoinban volt kénytelen finanszírozni magát, ami mára mintegy 50 000% (ötvenezer százalék) hasznot hajtott. Lásd: https://www.cnbc.com/2017/10/16/wikileaks-julian-assange-bitcoin-50000-percent-return-thanks-to-us-government.html



4. ábra
A legnagyobb bitcoin bányász pool-ok
Forrás: blockchain.info

megfelelően titkos helyen lévő) ún. bányász *„farmok”*[80] sem voltak elegendőek, illetve nem minden résztvevő tudott akkora összeget invesztálni, hogy saját bányász farmja legyen. Ezért, illetve a farmok mellett párhuzamosan kialakultak az ún. *„pool”*-ok, azaz olyan – természetesen valakik tulajdonában lévő – webhelyek, amelyekre bárki csatlakoztathatja a saját bányász gépét/gépeit. Ezek a pool-ok többségükben úgy jelennek meg a rendszerben, mint egy-egy csomópont, ami mögött szintén egy bányász farm van. Ténylegesen azonban kis, egyedi felhasználóktól *„megveszik”* az általuk felajánlott számítástechnikai kapacitást, és ha egy ilyen pool-nak sikerül összeállítania egy blokkot, akkor az érte kapott jutalomból és a blokkban lévő tranzakciók könyvelési jutalékából minden résztvevő, hozzájárulása arányában részesül. Ezért ma a bányászat nem pár csomópontra koncentrálódik, hanem a világon bárki bányászhat[81]. Megjegyzendő, hogy ma már mindent pool-nak hívnak, hiszen a rendszer nem tudja megkülönböztetni, hogy koncentrált bányász farmról, vagy elosztott pool-ról, vagy bármilyen más konstrukcióról van-e szó.

További alkalmazások – altcoinok

A Bitcoin 2011-ben még nem volt olyan sikeres, mint ma, de már akkor is többen fantáziát láttak benne. Ezért egyesek úgy gondolták, hogy a Bitcoin rendszer alapjain más alkalmazásokat is kifejlesztenek. Ezek az alkalmazások legtöbbször szintén digitális fizetőeszközként jelentek meg. Ezeket a fizetőeszközöket kriptovalutaként szokták említeni, holott a *„valuta”* szó egy pénznek kifejezetten a fizikai formájára utal, a virtuális világban viszont pont az a lényeg, hogy fizikailag nem létezik a pénz. Ezért inkább kriptodevizaként lenne érdemes hivatkozni ezekre. Bár ez sem teljesen helyes, hiszen ezek a fizetéshez használható eszközök nem rendelkeznek mindazon tulajdonságokkal, amelyek közgazdaságtanilag a pénz fogalmát körülírják[82]. Mindemellett az elterjedt név miatt kriptovaluta, vagy kriptopénz elnevezéssel illetjük őket.

Mindemellett a bitcointól való megkülönböztetésként minden más ilyen kriptopénzt *„altcoin”* kifejezéssel is szoktak illetni. Sőt, miután rengeteg ilyen létezik, a tőzsdéken szokásos rövidítésekhez hasonlóan mindegyiknek rövidítése is van. A bitcoin rövidítése a BTC. Természetesen vita van arról, hogy ha ilyen eszközök a normál devizatőzsdéken (foreign-exchanges – ForEx) megjelennek, akkor hogyan is kellene ezeket megkülönböztetni a fizikai világban létező devizáktól (fiat-októl). Erre csak egy ajánlás született, mégpedig az, hogy minden ilyen kriptovaluta rövidítése kezdődjön X-szel, annak érdekében, hogy meg lehessen különböztetni, hogy egy a kriptovaluták világából származó *„eszköz”*. Ezt – néhány kivételtől eltekintve – senki nem tartja be, igaz, a bitcoin-nak is van ilyen rövidítése, az XBT.

Az első altcoin – a Namecoin

Az első ilyen altcoin, amely a bitcoin után megjelent, a Namecoin (NMC) volt, amelyet 2011 áprilisában vezettek be. Ezt a Bitcoin rendszerből ágaztatták le (ezt a leágaztatást nevezik *„fork”*-nak), azaz ugyanazzal az algoritmussal, bányászási technikával, stb. rendelkezik, mint a bitcoin. Kérdezhetnénk, hogy akkor minek? A válasz az, hogy a Namecoin fő innovációja az elosztott, tehát központi hatalom nélküli hálózatoknak egy másik felhasználási területe volt. Mégpedig az, hogy az interneten használatos ún. felső szintű domain (top-level-domain – TLD) név kiterjesztések mellett (mint pl. a *„.com”*, *„.org”*, *„.net”*, vagy akár az országoknak kiosztott név, pl. a *„.hu”*), amelyeket végső soron egy USA-ban bejegyzett magán szervezet, az ICANN[83] oszt ki és ellenőriz, egy új, felső szintű domain név kiterjesztését tudja elérni, és használatba venni. Mindezt függetlenül mindenféle felső hatalomtól, megbízható harmadik féltől, valamint az ICANN által kiosztott domain név kiterjesztéseket felismerő és üzemeltető ún. DNS[84] rendszertől. Ez a domain név kiterjesztés a *„.bit”*. Mivel a NMC alapvetően nem pénz helyettesítő, illetve fizetési eszköz funkciójú, így ennek népszerűsége és természetesen az árfolyama is messze elmarad a bitcoinétól. Az NMC árfolyama a cikk írásának idején 1 NMC = 0,0001762 BTC[85]

[80] Ezeket óriási szervertermeknek képzeljük el, teli kifejezetten bányászatra kialakított gépekkel. Áramfogyasztásuk viszont sokszorosa egy normál szerverteremnek, ezért nem csoda, hogy ezek a farmok főleg olyan helyekre lettek telepítve, ahol a villanyáram ára olcsó (pl. Kína, vagy Izland).

[81] Mindemellett az utóbbi időben kialakult az ún. *„cloud mining”*, azaz bányász felhők rendszere is. Ezeknél a bányásznak már otthon nem is kell, hogy bányász gépe legyen, hanem a felhőből megveszi a számítástechnikai kapacitást, a másik oldalon pedig eladja azt egy pool-nak. Természetesen ezért kevesebb bitcoin-t lehet kapni, mert a bányász felhőt üzemeltető cég is él valamiből, mindenesetre ez a modell is működőképesnek látszik.

[82] A pénznek jogi fogalma nincs is.

[83] Internet Corporation for Assigned Names and Numbers – lásd: https://www.icann.org/

[84] DNS – Domain Name System, amely végső soron a világon 13 fő szerverre bízza az internet domain neveinek üzemeltetését, gyakorlatilag a mai internet működését (ezek a roor name server-ek, A-tól M-ig, lásd: https://en.wikipedia.org/wiki/Root_name_server)

[85] Az altcoin árfolyamokat általában bitcoin egyenértékben fejezik ki, így mi is ezt tesszük, hacsak külön nem jelezzük, hogy más egységben adjuk meg.

(kb. 1,08 USD), piaci kapitalizációja valamivel elmarad a 2600 BTC mögött (kb. 16 millió USD)[86].

Könnyített bitcoin – a Litecoin

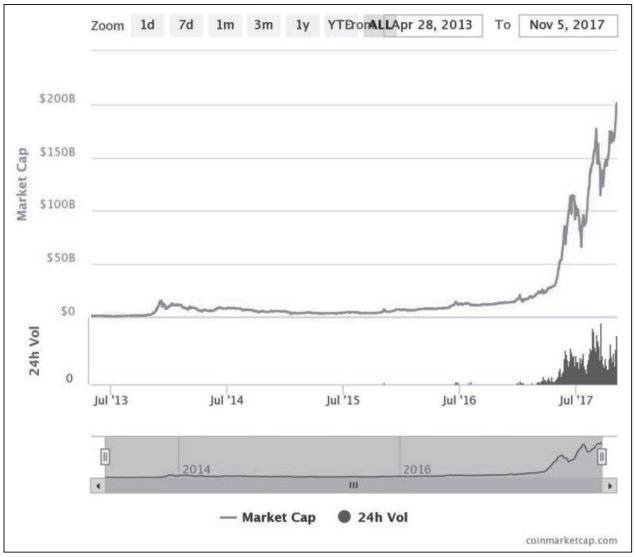
Bár további altcoin-ok is születtek időközben, ezek nem lettek annyira sikeresek, mint a 2011 októberében, egy volt Google alkalmazott, *Charles Lee* által bevezetett Litecoin (rövidítése: LTC)[87]. Ennek legfontosabb újítása az volt, hogy míg a Bitcoin rendszerben a bányászathoz már igen erős, specializált gépekre volt szükség, addig a Litecoin egy másik, jóval egyszerűbb hash algoritmust használt, a Scrypt-et (a bitcoin az SHA256-ot használja). Ezzel a bányászok dolga is könnyebb lett, egyszerűbb gépekkel[88] is lehet bányászni, sőt ezzel a blokkok, azaz új főkönyvi lapok előállításához szükséges időt is lerövidítették, a bitcoinnál szokásos 10 perctől 2,5 percre. Ezzel tehát az egyes tranzakciók átlagosan sokkal gyorsabban tudtak teljesülni. Egyéb paraméterek is mások, mint Bitcoinnál, hiszen itt nem 21 millió, hanem 88 millió lesz a végül kibányászott Litecoin-ok száma, és ehhez igazodóan a bányászati jutalom feleződése 840 000 blokkonként következik be (az eredeti jutalom 50 LTC volt). A cikk írásakor az árfolyam 1 LTC=0,009095 BTC volt (kb. 56 USD). A piaci kapitalizáció azonban jelentős, több, majdnem 490 000 BTC, azaz több, mint 3 milliárd USD[89].

Egy valós idejű elszámolási rendszer – a Ripple

A Ripple (XRP) egy más megközelítésű, de blockchain-t alkalmazó teljes rendszer, amelyet 2012-ben vezettek be. Jellegzetessége, hogy valós idejű elszámolást tesz lehetővé (kb. 3-5 másodperces *„késleltetési"* idővel), nem *„bányászható"*, mert a teljes, a rendszerben található Ripple, mint pénzegység, már előre, a rendszer indulásakor ki lett bányászva. Ezért ezzel kereskedni, elszámolni lehet, ezért bankok is használják, pl. a Unicredit, a UBS, vagy a Santander. A rendszer szintén olyan, mint a többi publikus blockchain, nem lehet leállítani, állandóan működik. A blokkok ellenőrzői cégek, de pl. köztük van egy egyetem is, a Massachusetts Institute of Technology (MIT)[90]. A Ripple árfolyama a cikk írásakor: 1 XRP=0,00003289 BTC (kb. 0,2 USD). Viszonylag kis értéke ellenére azonban piaci kapitalizációja jelentős, mintegy valamivel az 1,3 millió BTC alatt van, amely mintegy 7,8 milliárd USD-nek felel meg.[91]

Egyéb altcoin-ok, tokenek, kriptoeszközök

Mára rengeteg féle altcoin alakult ki, egyesek a fizetés gyorsaságára[92], vagy az anonimitás megőrzésére (pl. Monero, Dash) koncentráltak. Mindemellett létrejöttek egyes speciális fejlesztési, kutatási területek, startup-ok finanszírozására az ún. token-ek, amelyekről a későbbiekben részletesebben is szó esik.[93] A fentiekből egyúttal az is következik, hogy nem minden ún. kriptoeszköz egyúttal kriptovaluta is, sőt, mivel a blockchain technológia felhasználási területe egyre szélesebb, újabb eszközök megjelenése is várható. Talán közös vonásként lehet mondani a legtöbb alkalmazásról, hogy piaci értelemben értéke van, amelyet valamilyen módon kriptoeszközök testesítenek meg, sőt ezek az eszközök a később tárgyalandó kriptotőzsdék segítségével könnyen egymásba átalakíthatók. A *„kriptovilágban"* fellelhető fontosabb kriptovaluták és tokenek száma mára meghaladta az 1200-at[94]. A teljes piaci kapitalizációjuk pedig meghaladta[95] a 200 mil-



5. ábra
A kriptopénzek piaci kapitalizációjának alakulása
Forrás: coinmarketcap.com

liárd USD-t[96]. Ellenben van egy innováció, amely külön utat kezdett járni (mára már mások is ennek útjára léptek), és ennek az innovációnak a saját kriptovalutája mára a második legnagyobb piaci kapitalizációval, mindamellett óriási további innovációs kilátásokkal rendelkezik. Ezért erről külön kell szóljunk.

[86] https://coinmarketcap.com/currencies/namecoin/

[87] Részletesebben lásd: https://hu.wikipedia.org/wiki/Litecoin

[88] Ezek természetesen számítógépek, de boltban megvásárolható eszközökből összeállítható, igaz, nem olcsó konfigurációk.

[89] https://coinmarketcap.com/currencies/litecoin/

[90] Részletesebben lásd: https://en.wikipedia.org/wiki/Ripple_(payment_protocol)

[91] https://coinmarketcap.com/currencies/ripple/

[92] https://themerkle.com/4-cryptocurrencies-with-much-faster-block-times-than-bitcoin/

[93] Lásd később az ICO-ról szóló részt.

[94] https://coinmarketcap.com/all/views/all/, bár egyes más oldalak 2800 kriptoeszközt is felsorolnak.

[95] A cikk írásának elején még 180 milliárd USD volt, a lektoráláskor (2017. november 5.) már a szövegben jelzett 200 milliárd USD.

[96] Ezzel a számmal, ha a világ 10 legnagyobb cége közt nem is, de a legnagyobb 20-ban – ha cég lenne – mindenképpen ott lenne a helye a *„kriptovilág"* kapitalizációjának. A dinamikát tekintve a szerző jóslata szerint pár 3-5 év múlva az első 10-ben is ott lesznek.

A Bitcoin kihívója – az Ethereum

2013 végén a Bitcoin rendszerbe bedolgozó egyik fiatal, *Vitalik Buterin*[97], orosz származású, USA-ban tanult, de ma Szingapúrban élő programozó kitalált egy fejlesztést, amely a Bitcoin rendszert alapul véve új utat jelölt ki. Ez a rendszer, amelynek alapjait *Vitalik Buterin* 19 évesen tette le, az Ethereum. Pénzneme az Ether (ETH) amely ma a világ második legnagyobb piaci kapitalizációjával bíró kriptovaluta (altcoin), a cikk írásakor árfolyama kb. 0,05 BTC (kb. 308 USD), piaci kapitalizációja viszont több, mint 4,7 millió BTC, azaz közelíti a 30 milliárd USD-t.[98] De mit is tud az Ethereum, amit a Bitcoin rendszer nem tud? És mi az, ami indulásától számítva pár hónap[99] leforgása alatt az Ethereum rendszert ilyen magasságokba repítette?

Ez az innováció az, hogy az Ethereum rendszer (vagy ahogy a fejlesztői hívják, Ethereum Virtual Machine – EVM), magán a rendszeren belül számítógépes program kódok futtatására alkalmas, azaz gyakorlatilag bármilyen számítás elvégezhető vele. Természetesen itt nem magára az Ethereum rendszer kódjára gondolunk, mert az maga az, amely program kódokat futtat. Itt arra gondolunk, hogy az Ethereum rendszer képes arra, hogy egy speciális programnyelven[100] megírt kódot saját maga futtasson. De mire jó mindez?

Mindenekelőtt meg kell jegyezni, hogy már a Bitcoin rendszerben is volt egy speciális *„programnyelv"*, amely direkt arra volt kifejlesztve, hogy a tranzakciók, az átutalások végbe tudjanak menni, pénztárcákat létre lehessen hozni, egyéb kiegészítő funkciókat végre lehessen hajtani. Azonban a Bitcoin belső programnyelve nem volt ún. *„Turing-complete"*. Ez magyarul azt jelenti, hogy a fent már említett Alan Turing által körülírt kiszámíthatósági kritériumokat nem tudta teljesíteni, azaz nem volt alkalmas minden olyan dolog kiszámítására, amit Turing kiszámíthatósági elmélete tartalmazott. Egészen pontosan nem volt benne ún. ciklus utasítás, amely egy programkód többszöri végrehajtását tenné lehetővé (zenei analógiával ez olyan, mint a kottában az ismétlőjel – ha ez nincs, akkor annyiszor kell leírnunk a dallamot, ahányszor el kell azt játszani).

Ennek a *„hiányosságnak"* azonban megvolt a maga jól átgondolt oka. Ha ugyanis megengednénk, hogy a Bitcoin rendszer akárhányszor végrehajtson egy adott kódot, az ahhoz vezetne, hogy vagy véletlenül kerül a rendszer olyan állapotba, hogy végtelenségig csinál valamit, vagy az is lehet, hogy valaki direkt bírja rá a rendszert ilyen *„rendellenes"* működésre. Ilyen indíték lehet pl. az is, hogy valaki spam-eket küldjön szét, vagy szolgáltatásmegtagadásos (DDoS) támadást intézzen egyes számítógép rendszerek ellen. És ebben a fent már említett munkabizonyíték (Proof of Work) rendszer sem segítene, hiszen akkor a bányászok is mind ennek a rendellenes működésnek a szolgálatába állnának, tudtukon kívül. Ezért a Bitcoinból kihagyták az ún. ciklus utasítást (azaz az ismétlőjelet).

Az Ethereum rendszerben azonban ezt a problémát sikerült megoldani, és a megoldás további távlatokat nyitott az Ethereum felhasználása terén[101]. A megoldás pedig az volt, hogy mégiscsak bevezetik a ciklus utasítást, ezzel *„Turing-complete"*-té téve az Ethereum belső programnyelvét. Viszont ennek van egy ára. És itt az árat szó szerint kell érteni. Az Ethereum fejlesztői ugyanis azt találták ki, hogy minden egyes számítási lépésnek, amelyet az Ethereum végrehajt, előre megszabott ára van. Megmondták minden egyes funkcióra, hogy ez-és-ez mennyibe fog kerülni. Az árat megtestesítő fizető egységet pedig *„gas"*-nek, magyarul üzemanyagnak, benzinnek nevezték el, mivel a robbanómotort is üzemanyag hajtja. Ugyanígy, az Ethereum, mint gép is csak addig működik, amíg ki nem fogy az üzemanyag, a gas. Ez az, amiért tehát az Ethereumban bárki bármilyen programkódot szeretne végrehajtani, bármilyen célból is, azért valamilyen módon fizetnie kell. Amennyi gas-t rászán valaki egy adott kód futtatására, az Ethereum azt addig hajtja végre[102]. Ahogy azonban fentebb írtuk, az egyes számítási lépések ára gas-ban fixálva van. Ha viszont sokan vannak, akik program kódot szeretnének végrehajtani, akkor versengés indul el, hogy ki az, aki egy adott gas mennyiségért többet hajlandó fizetni (ez olyan, mint a benzin ára, az autó fogyasztása fix, viszont a benzin ára a kereslet/kínálat függvényében változik). A gas ára (a *„gas-price"*) viszont az Ethereum fizetőegységében, Etherben (ETH) változhat, és változik is. Ha tehát verseny van az Ethereum működtetéséért, akkor a gas ára Etherben feljebb fog menni, amely egyszersmind azt is jelenti, hogy az Ether ára is feljebb megy fiat-ban (azaz fizikai világbeli fizető eszközben, pl. USD-ben).

Ez eddig rendben is volna, de mire is használjuk az Ethereumot? Fizetési rendszerként, tranzakciók végrehajtására ugyanúgy használható, mint a Bitcoin, azzal, hogy itt a *„könyvelő"*, a blokk összeállítójának tranzakciókba beépített fizetsége gas-ban már előre fixálva van, hiszen egy fizetési tranzakció végrehajtása is valahány, előre meghatározott számú számítási lépésből áll[103]. De az Ethereum másra is használható. Ahogy írtuk, az Ethereum gyakorlatilag bármely programkód futtatására alkalmas, ha azt a belső programnyelve lehetővé teszi. És itt jön az Ethereum újítása, az ún. *„okos-szerződések"* (smart contracts).

---

[97] https://en.wikipedia.org/wiki/Vitalik_Buterin

[98] https://coinmarketcap.com/currencies/ethereum/

[99] A tényleges, már használható, élesben futó Ethereum rendszer a Homestead (ma is ez működik), amely 2016. március 14-én indult, azaz a jelen cikk írását megelőzően másfél évvel. A korábbi rendszerek (Olympic, Frontier inkább teszt rendszerek voltak). Lásd: https://en.wikipedia.org/wiki/Ethereum#Milestones

[100] Ezeket a nyelveket ún. script nyelveknek hívják az ilyen rendszerekben

[101] Az Ethereummal kapcsolatosan szokták emlegetni a Web 3.0 kifejezést is, utalva arra, hogy ezzel ismét valami újat hoz az internet világa.

[102] Nem pontosan, mert ha a gas pont olyankor fogy el, amikor a gép egy olyan állapotban áll le, ami *„értelmezhetetlen"*, akkor a gépet a rendszer visszaállítja az utolsó *„értelmes"* pontra és a maradék gas-t visszatéríti annak, aki befizette.

[103] Plusz, egy Ethereum blokk kibányászásáért 5 ETH a jutalom, amely 15 másodpercenként *„keletkezik"*, mivel a blokkok bányászási ideje eddig tart.

Okos szerződések az Ethereumban

Az okos szerződés egy olyan szerződés, amelyben bizonyos, jól meghatározott részek pl. adott szolgáltatás mennyisége, ellenértéke, fizetés esedékessége, fizetség mennyisége, a szerződés hatálya, nem másban, mint programkódban vannak leírva. Tehát nem szabad szövegesen, mint azt általában egy szerződésben olvashatjuk, hanem az Ethereum saját programnyelvén. Mit jelent mindez? Azt, hogy ha a szerződő felek megállapodtak, a szerződés ezen részeit maga az Ethereum, mint gép, automatikusan hajtja végre, mindezt több ezer csomópont (node) által azonos módon ellenőrizve, validálva (de pl. egy fizetést természetesen csak egyszer végrehajtva). Azaz itt nincs fizetési késlekedés, nincs sorban állás, lánctartozás, egyéb, likviditás hiányból adódó fizetési nehézség. Adott esemény bekövetkeztekor az Ethereum automatikusan végrehajtja azokat a programkódokat[104] (jellemzően pl. feltételtől függő átutalásokat), amelyeket az okos szerződés előír (természetesen csak akkor, ha a szerződő felek, vagy legalábbis az a fél, amelyik a másik teljesítésében érdekelt, kifizette a gép működéséért járó megfelelő gas-t). Így tehát nincs szükség ügyvédre, bíróra, fizetési felszólításra, faktorálásra, pénzbehajtókra, az Ethereum végrehajtja az okos szerződést (a fentiekben írt megfelelő *„díjazásért"*, de ez nagyságrendileg kevesebb, mint pl. egy peres eljárás, vagy egy végrehajtás díja).

Az Ethereum kihasználása ezzel azonban még messze nem érte el a csúcsát, hiszen további alkalmazások[105] írhatók és hajthatók végre az Ethereummal. Ezeknek egy részéről ma még nem tudjuk mi lehet. Mindenesetre azt meg kell jegyezni, amit az Ethereum fejlesztői is mindig hangoztatnak, de ez igaz a legtöbb publikus blockchain alkalmazásra is: nagyon lassú[106], nagyon drága a működtetése, azaz a bányászás[107], de ami ebben a rendszerben benne van, az hiteles, és az mindig is az marad, mindenki által ellenőrizhetően, és mindig elérhetően[108].

Befektető toborzás – ICO

Már az Ethereum bevezetésekor a fejlesztők kezdtek szervezni egy *„céget"*, vagy inkább szervezetet, amelynek a The DAO[109] nevet adták. A DAO a Decentralized Autonomous Organization rövidítése, azaz egy központ nélküli, önműködő szervezetet szerettek volna létrehozni. Ehhez a rendszer saját kriptopénzében, Etherben befektető finanszírozókat kerestek, oly módon, hogy – hasonlóan a részvénytársaságok megalakulásakor a részvényjegyzéshez (ez az ún. Initial Public Offering, vagy IPO[110]) – saját maguk bocsátottak ki részvényhez hasonló token-eket (zsetonokat), amelyeket Etherért lehetett jegyezni. A különbség annyi, hogy míg a részvény tulajdonviszonyt is megtestesít, egy ilyen token csak hitelviszonyt testesít meg, ezért közelebb áll a kötvényhez. A kötvényhez képest viszont az a különbség, hogy a kötvény csak a lejáratkor fizet, a token azonban a részvényhez hasonlóan, évente fizet, a szervezet által elért nyereség arányában (szelvényvagdosás). Tehát egy ilyen token-nel úgy juthat a befektető a cég nyereségéhez évről évre, hogy egyébként nem válik tulajdonossá.

Ilyen módon való befektető toborzás (crowdfunding) manapság rengeteg van, és ezt a módszert a fent említett IPO mintájára ICO-nak, azaz Initial Coin Offering-nek, magyarul leginkább a részvényjegyzés mintájára *„tokenjegyzésnek"* mondhatnánk.

Bár ez a fajta befektető toborzás ma virágkorát éli, már havonta tucatszám indulnak különböző ötletek, startup-ok finanszírozására ICO-k[111], mégis meg kell jegyezzünk ezzel kapcsolatban pár dolgot.

Az egyik az, hogy itt a *„befektetőknek"* nem sok információ áll rendelkezésére, maximum egy rövid koncepció (white paper) egy adott innovációról, amelyhez befektetőket keresnek. Másrészt semmi biztosíték arra, hogy ez az innováció

[104] Nick Szabo (az okos szerződések mint fogalom és mint kifejezés kitalálója – lásd: https://en.wikipedia.org/wiki/Nick_Szabo) ezt hívja ún. *„dry code"*-nak (száraz kódnak), szemben a jogászok, ügyvédek által szabad szövegesen, pontosan, vagy pontatlanul megfogalmazott szerződésekkel, amelyeket *„wet code"*-nak (nedves kódnak) nevez.

[105] Egy ilyen alkalmazás pl. az Ethereum Name Service (ENS – https://ens.domains/), amely – a Namecoin-hoz hasonlóan – domain név kezelésre specializálódott, de egy másik domain név kiterjesztés, a *„.eth"* vonatkozásában. A domain nevek használatát itt Ether-ben kiírt aukciókon lehet elnyerni, egy éves időtartamra. Jellemző azonban a nem világos működésű ökoszisztémára az, hogy néhány domain-ért horribilis összegeket voltak hajlandók kifizetni. A csúcsot a darkmarket.eth és az openmarket.eth domain nevek tartják. Ezeket, és pár további domain-t egyetlen pénztárcából fizettek ki. Mind a dakmarket.eth, mind az openmarket.eth domain-ért egyenként 28.555 ETH volt a csúcs licit, amely, kb. 8,5 millió USD-t jelent egy-egy domain név vonatkozásában. Lásd még: https://www.reddit.com/r/ethereum/comments/6ep63n/darkmarketeth_and_openmarketeth_new_ens_records/

[106] Igaz, amíg a Bitcoinnál egy blokk kibányászásához 10 perc kell, addig az Ethereumnál ez 15 másodperc, azaz sokkal gyorsabban hitelessé válnak az egyes műveletek, mint a Bitcoin esetén.

[107] Az Ethereum ismét más hash algoritmussal dolgozik, mint a Bitcoin. Ezt az algoritmust eredetileg Dagger-Hashimoto-nak hívták, mára a tovább fejlesztett változatát átnevezték Ethash-ra. Az alapvető változás a Bitcoin és az ahhoz hasonló kriptopénzekhez képest, hogy úgy tervezték meg az algoritmust, hogy az *„ellenálljon"* mindenféle célszámítógépek fejlesztésének (a rendszer ún. ASIC resistence), azaz ne lehessen olyan célgépet készíteni, amely sokkal gyorsabban hajtja végre a műveleteket (a bányászást), mint a normálisan, boltban kapható számítógép alkatrészekből összerakott számítógép. Ehhez memória intenzív műveleteket használ (aciklikus irányított gráfok használata – Directed Acyclic Graph – DAG) , mivel a számítógép memóriák mérete és ára nagyjából proporcionális összefüggést mutat. Manapság egyébként félig célgépeket használnak, ún. *„rig"*-eket, amely egy normál számítógép, de rengeteg csúcskategóriás grafikus kártya (videokártya) van bennük, amelyek processzora (GPU) nem játékok képének megjelenítésére szolgál, hanem ún. párhuzamos feldolgozással a *„bányászat"* szolgálatába állították. A szerző saját tapasztalata alapján ezek a gépek hosszú ideig működőképesek és profitábilisak maradhatnak, mivel többféle hash algoritmusra programozhatók. Így, ha az egyik altcoin bányászata nem éri meg, egy másik hash algoritmussal működő még megérheti és viszont. Végső soron pedig egy ilyen *„rig"* sztenderd számítástechnikai alkatrészekből van összeállítva, amelyek akár más célra is felhasználhatók, akár értékesíthetők a későbbiek folyamán.

[108] Ha az anonimitást (itt inkább a magánélet védelmét – privacy) is szem előtt tartjuk, mint minden más publikus blockchain alkalmazásban, mondhatjuk, hogy teljesíti az információbiztonság három alapelvét: bizalmasság, sértetlenség, rendelkezésre állás (Confidentility, Integrity, Reliability – az ún. CIA alapelv).

[109] Lásd: https://en.wikipedia.org/wiki/The_DAO_(organization)

[110] Lásd: http://www.investopedia.com/university/ipo/ipo.asp

[111] Lásd: https://tokenmarket.net/ico-calendar

egyáltalán megvalósul, vagy legalább kísérletet tesz arra, hogy megvalósítsák, csak egy weblap van, amely mögött senki nem tudja, hogy ténylegesen komoly szándékú innovátorok, vagy egyszerű csalók, netán szerencselovagok vannak. Ezért is nem véletlen, hogy Kína idén szeptember elején egyszerűen betiltotta az ilyen típusú *„pénzgyűjtést"*[112], és meg is indokolta a lépést[113].

A „The DAO" hacking

Az ICO-val kapcsolatosan van már sajnálatos rossz tapasztalat. Amikor az Ethereum blockchain használatával megkezdődött a The DAO nevű szervezet létrehozásához a token kibocsátás és így az Etherben való kriptopénz gyűjtés 2016 májusában, máig nem azonosított személy, vagy személyek hibát fedeztek fel a programkódban[114], és 2016 júniusában az addig összegyűlt 11,5 millió Ether mintegy egyharmadát, kb. 3,6 millió Ether-t *„kiszívták"* a rendszerből, magyarul eltulajdonították. Ez, tekintve, hogy a publikus blockchain-ek egyik kulcs összetevője az anonimitás, oda vezetett, hogy máig ismeretlen a *„The DAO hacker"* személye.

Nem kevés pénzről beszélünk, az Ether egyenértéket átszámolva, akkori árfolyamon mintegy 50 millió USD összeg volt az, amelyet így sikerült ellopni, és ezzel nyomtalanul eltűnni. Ez a lopás több mint 18 ezer befektetőt érintett, akik 2016. június 20-án kénytelenek voltak azt a döntést meghozni, hogy *„meg nem történtté"* teszik az esetet, azaz azt a blokkot (könyvelési oldalt), és minden utána lévőt, törölnek a rendszerből, mintha meg sem történt volna a lopás. Ezt a befektetők többsége támogatta. Egy jelentős kisebbség viszont úgy gondolta, hogy a kód az, amely *„szent"*, és ők továbbra is azt a könyvelést tekintették valódinak. Így az Ethereum blockchain hirtelen kettévált (ennek a neve: hard fork), és két főkönyv alakult ki belőle. Akik azt mondták, hogy vissza kell fejteni a könyvelést a lopás előtti időig, ők vitték tovább az Ethereum-ot, akik pedig a lopást elviselve, és így valamilyen módon még *„legitimizálva"* is azt, folytatták a másik főkönyvet, új kriptopénzt hoztak létre, amelyet ma Ethereum Classic (ETC) néven ismerünk. A hatás azért nem maradt el, az Ethereum Classic ma kb. 1/10-ét éri a normál Ether-nek. De valahol a *„The DAO hacker"* most is tulajdonol, ha nem is 50 millió USD-t – merthogy az Ethereum rendszer nem ismeri el az ellopott pénzt –, de – mivel az Ethereum Classic rendszer elismeri –, így is 5 millió USD-nek megfelelő kriptopénzt (ETC-t). Ráadásul ezt az ismeretlent (vagy ismeretleneket) a kriptovilág egyik vezető online magazinja, a CoinDesk a blockchain technológia terén 2016 leginkább befolyásos emberének választotta[115], mintegy 2000 olvasó válasza alapján.

Kriptotőzsdék, és váltók

A kriptopénzek világa óriási ütemben bővül, annyira, hogy ma már külön tőzsdék (ún. kriptotőzsdék) specializálódtak ezekre az eszközökre. Ezek a kriptotőzsdék csak az interneten léteznek, ráadásul – a normál tőzsdékkel szemben – bárki tagja lehet és közvetlenül kereskedhet, aki számlát (pénztárcát, vagy pénztárcákat) nyit egy ilyen tőzsdén. Néhány ilyen kriptotőzsdén csak egymás közt lehet ezekkel kereskedni (pl. Poloniex, Cryptopia), de van olyan is, ahol kriptopénzt fiat-ra is lehet váltani és viszont (pl. Kraken, Cex.io). Ezeken a tőzsdéken azonnali kereskedés, limit kereskedés, sőt határidős kereskedés, illetve kriptopénz kölcsönzés is lehetséges.[116] Sőt, ezen tőzsdék mindegyike nyit a felhasználóinak saját *„pénztárcát"*, azaz kezeli a felhasználók adott pénztárcájának titkos kulcsát is.[117] Ezen tőzsdék legtöbbje az adott állam vagy államok tőkepiaci, vagy bankfelügyeleti szervének engedélyével működik. A kriptotőzsdék forgalma naponta összességében 1 milliárd USD felett van[118].

Vannak azonban olyan szolgáltatók is, amelyek kizárólag pénzváltásra szakosodtak, ilyen pl. a Shapeshift, vagy a Changelly. Mindemellett a világon üzemelnek Bitcoin pénzváltó automaták is (ATM-ek), Budapesten is van ezekből kettő.

A Mt. Gox és a BTC-e esete

Szólnunk kell azonban a tőzsdékkel kapcsolatos visszaélésekről is. Ahol nagy pénzek forognak, ott általában megjelenik a bűnözés. Az első ilyen nagyobb eset az ún. Mt.Gox[119] eset volt, amely egy japán bitcoin tőzsde volt, egyszersmind a legnagyobb. A világ bitcoin forgalmának 70%-át kezelte még 2013-2014-ben. Azonban egy, a Bitcoin szabályrendszerében talált sérülékenység[120] kihasználásának esett áldozatul, és 2014. február 24-én egyetlen pillanat alatt bezárt. Kb. 850 000 BTC tűnt el (mint később kiderült, már 2011 óta folyamatosan), amely akkori árfolyamon mintegy 450 millió USD-nek felet meg. Bár a Mt. Gox vezérigazgatóját, *Mark Karpelés*-t[121] 2015-ben letartóztatták, ez nem nyújtott vigaszt mindazoknak, akiknek a Mt. Gox tőzsdén bitcoinban tárolt pénze teljes egészében odaveszett.

Egy másik, a közelmúltban megesett visszaélés volt a BTC-e kripto tőzsde esete, amelynek tulajdonosát, az orosz *Alexander Vinnik*-et idén nyáron pénzmosás gyanújával

[112] Lásd: https://www.reuters.com/article/us-china-finance-digital/chinas-virtual-coin-fundraising-ban-just-the-start-of-tighter-regulations-yicai-idUSKCN1BG05S

[113] https://bankinnovation.net/2017/09/regulations-controls-and-non-security-tokens-the-chinese-ico-ban-in-context/

[114] A szervezetet Christoph Jentzsch és Simon Jentzsch találta ki, a program kódot Christoph Jentzsch fejlesztette.

[115] https://www.coindesk.com/coindesks-influential-people-blockchain-2016/

[116] Csak példák az ismertebb és nagyobb tőzsdékre: Bitfinex, bitFlyer, Bitstamp, Bittrex, C-CEX, Cex.io, Coinbase, Gatecoin, Gemini, HitBTC, Kraken, Livecoin, OKCoin, Poloniex, QuadrigaCX, Quoine, YoBit, és akkor még a Kína által, az ICO betiltása miatt ideiglenesen bezárt tőzsdéket nem is említettük.

[117] Itt azonban *„megdől"* az az elv, hogy nem kell megbízható harmadik fél, mert aki ilyen kriptotőzsdén nyit egy *„pénztárcát"*, az nyilván megbízik ebben a tőzsdében (holott nem mindig kellene, lásd a Mt. Gox esetet).

[118] https://coinmarketcap.com/exchanges/volume/24-hour/

[119] https://en.wikipedia.org/wiki/Mt._Gox

[120] Ez volt az ún. tranzakció képlékenység (transaction malleability), amely azokat a tranzakciókat érintette, amelyek még nem kerültek *„lekönyvelésre"* egy adott, sikeresen lezárt blokkban.

[121] https://en.wikipedia.org/wiki/Mark_Karpel%C3%A8s

6. ábra
Kriptotőzsde nyitó oldala
Forrás: poloniex.com

tartóztatták le.[122] A terhére rótt összeg nem kevesebb, mint 4 milliárd USD volt, amellyel a gyanú szerint az ún. *„darkweb"*-en működő illegális kereskedelem ügyleteinek tranzakcióit intézte, illetve ezeket a pénzeket mosta tisztára.[123] Elemzők ráadásul összefüggést találtak a Mt. Gox eset és a BTC-e esete között.[124] No comment.

Rendszerhibák

A blockchain-en alapuló alkalmazások, megoldások még nem teljesen kiforrottak. Ugyanakkor, ahogy a fentiekből is látszik, rengeteg pénz van mögöttük, így nem csoda, ha szerencselovagok, tolvajok, hackerek, alvilági csoportok is *„érdeklődnek"*, hogyan lehetne kiaknázni a rendszer gyengeségeit. Maga a matematikai alap fix, és jól körülírt. Az informatikai megvalósításba természetesen csúszhat – véletlen vagy szándékos – hiba, sőt, a használat során sokszor kiderülnek hiányosságok, és/vagy olyan problémák, hogy egy-egy rendszer bizonyos mértékű terhelést már nem képes változtatás, optimalizálás nélkül elviselni. De hogyan lehet rávenni egy elosztott rendszer minden üzemeltetőjét, a csomópontokat (node-okat), ha bányászathoz szükséges számítástechnikai kapacitás legalább 51%-ának birtokosait, hogy most pedig át kell állni egy újabb fejlesztés üzembe állítására, frissítésre (upgrade-elni kell)? Ez a publikus blockchain rendszerek egyik fő hiányossága, és sokszor nem megy simán a dolog.

Először is, a tapasztalatok alapján ellenőrizni kell, hogy a hiba tényleg fennáll-e. Ha igen, minél gyorsabban valamit ki kell találni, mert ha a hiba olyan jellegű, mint pl. a Mt. Gox esetén volt, rengeteg kriptopénz tűnhet el a semmibe, vagy vándorolhat tolvajok pénztárcájába. Ha megvan, hogy mi a hiba, meg kell állapodnia a közösségnek, hogy hogyan is kell azt kijavítani. Itt általában sok vita keletkezik, többféle megoldási javaslat is születik, amelyek versengenek egymással.[125] Ha végül megvan az intézkedés, a hiba kijavítása, akkor rá kell venni minden felhasználót, de minimálisan a csomópontok üzemeltetőit arra, hogy a rendszerüket frissítsék. Ez sem megy egyszerűen, erre is különböző megoldásokat találtak ki.[126] Ezek a megoldások azonban nem mindig járnak sikerrel, 2017. augusztus 1-jén pár versengő megoldás közül az egyik[127] a Bitcoin blockchain-en oda vezetett, hogy egy új kriptovaluta alakult ki, amely a Bitcoin Cash nevet kapta (kódja BCC, vagy BCH – még a rövidítése sem egyértelmű).[128] Mindenesetre az árfolyama nem elhanyagolható, a cikk írásának idején 0,076 BTC (kb. 453 USD), piaci kapitalizációja pedig közel 1,2 millió BTC (kb. 7,5 milliárd USD).[129]

Volatilitás és kockázat

Mivel a blockchain-en alapuló megoldások – itt elsősorban a fizető eszközökre (kriptopénz, token) gondolunk – mögött semmilyen gazdasági teljesítmény nem mutatható ki, csak a spekuláció, valamint a bányászat által generált óriási villany-

[122] https://www.washingtontimes.com/news/2017/oct/8/alexander-vinnik-bitcoin-crime-suspect-at-center-o/

[123] https://www.deepdotweb.com/2017/07/28/greek-law-enforcement-arrest-btc-e-founder-laundering-billions-bitcoin/

[124] https://www.coindesk.com/coindesk-explainer-btc-e-arrest-mt-gox-connection-big-news/

[125] Ilyen eset volt a 2017. augusztus 1-jével bevezetett javítás, amely több versengő megoldás alkalmazása lett – lásd: https://www.btcforkmonitor.info/

[126] Ilyen pl. az ún. *„hard fork"*, azaz a kényszerű upgrade, illetve pl. a felhasználók által indított *„soft fork"* (UASF – User Activated Soft Fork), amikor is fokozatosan próbálják meg rávenni a node-okat a frissítésre.

[127] A BitcoinABC.

[128] Azóta még két, a Bitcoin rendszerből leágaztatott valutáról eshet szó. Az egyik az október végén bevezetett Bitcoin Gold (BTG), a másik egy, 2017. november 1-jén bevezetett hibajavítás (SegWit2x) elterjesztésétől, és így sikerétől függően az ún. BTC1 lesz.

[129] https://coinmarketcap.com/currencies/bitcoin-cash/, ill. https://www.cryptocompare.com/coins/bch/overview/BTC

számla[130], adódik a kérdés, hogy mi vezérli a piacot, mitől nő vagy csökken ezen kriptovaluták árfolyama? Természetesen nyilván van gazdasági teljesítmény e mögött, de ahogy fentebb már említettük, az alvilág és a pénzmosodák is jelentős részt visznek ebből a *„teljesítményből"*. Azonban egyikre sem az a jellemző, hogy szívesen nyilatkoznának a részt vevők az általuk eladott/vásárolt áruk értékéről, vagy bármely egyéb jellemzőjéről[131].

Azaz nincs tetten érhető gazdasági értelemben vett fundamentum, úgyhogy a piacok fundamentális elemzése semmiféle eredményt nem hoz. Nincs még olyan cég, amely mérlegfőösszegét pl. bitcoinban adná meg, bitcoinban vezetné a könyveit és az általa előállított/forgalmazott árukat, és/vagy szolgáltatásokat bitcoinban fixált áron nyújtaná. Természetesen vannak, akiknél lehet bitcoinban vásárolni, de az áru értéke akkor is valamilyen fizikai világban létező pénznemben (fiat-ban) fixált, a bitcoin-os, vagy bármilyen már kriptovalutás fizetés csak a fiat és a kriptovaluta aktuális árfolyamának átszámítása után lehetséges. Ugyanakkor, szabályozás hiányában, hiába is várnánk, hogy bármely állam illetékes hatóságai elfogadnának egy olyan mérleget, vagy eredmény kimutatást, időszaki beszámolót, amelyet pl. bitcoinban vagy Ether-ben vezettek.

Kimutatható gazdasági teljesítmény, GDP-hez való hozzájárulás hiányában tehát csak a másik elemzési módszer kínálkozik a kriptotőzsdéken forgó kriptopénzek árfolyamának megjósolására, múltbeli viselkedésük magyarázatára, ez pedig a technikai elemzés. Erről pedig tudjuk, hogy kizárólag az emberek szubjektumán, a befektetők pszichológiáján alapuló jóslás. Nem véletlen tehát, hogy egy-egy hír a kriptovaluták világában igen nagy mozgásokat tud elindítani a kriptotőzsdéken. Az előző fejezetben említett, 2017. augusztus 1-jével bevezetett *„javítás"* a Bitcoin rendszeren, már a bevezetés előtt két héttel óriási pánikot okozott, és az addig 3500 USD körül mozgó bitcoin árfolyam napok alatt leesett 1900 USD-re, sőt az alá is, igen nagy volumen mellett. Amikor viszont kiderült, hogy a szoftver javításának nem lett semmilyen, előre nem várt hatása, a bitcoin árfolyama szárnyalni kezdett, és hamar túllépte a 4000 USD-t. Most, a cikk írásának időpontjában, tehát mindössze két hónappal a vázolt esemény után a bitcoin árfolyama már 6300 USD felett van (a jelen cikk írásának kezdetén, pár nappal ezelőtt még „csak" 5700 USD volt). Ekkora volatilitás egyrészt óriási és hirtelen meggazdagodáshoz is vezethet, másrészt óriási bukásokhoz is. Bár mindenki a meggazdagodásra vágyik, és ha ez megvan, nem akadékoskodik, kérdezősködik, hogy hogyan történhetett ez, de bukás esetén – mint azt kifejtettük korábban pár eset kapcsán –, hiába is fordulna bárkihez a befektető. Hiszen ez a rendszer ilyen, és nincsen mögötte, pl. egy betétbiztosítási, vagy befektető védelmi alap, amely jótállna bármilyen káresemény kapcsán.

Buborék, pilótajáték, tulipánhagyma láz

Be kell látni tehát, hogy ma a blockchain, a kriptopénzek és az ICO tokenek világában az eredeti tőkefelhalmozás, az aranyláz kora zajlik. Van olyan vélemény, hogy ez a 2000-es évek *„dotcom"* válságához hasonlóan kipukkad, mert nincs mögötte semmi. Sőt, vannak olyan vélemények, amelyek pilótajátékhoz, vagy multi-level-marketing (MLM) módszerekhez hasonlítják a blockchain világát. A kérdés csak az, hogy mennyien hisznek benne? Elegen vannak-e a hívők ahhoz, hogy meghaladják azt a kritikus tömeget, amely túllendíti ezt a világot azon, hogy buborékként kipukkadjon. A szerző véleménye jelen tudása alapján az, hogy ez már túl van a kritikus tömegen, pont a fent leírtak miatt.[132] Ezért nem lehet ölbe tett kézzel ülni, és várni, hogy vége legyen ennek az *„őrületnek"*. Ha vége is lesz az aranyláznak, a blockchain akkor is gyökeresen megváltoztatja azt a világot, amelyet ma ismerünk.

Mindemellett megjegyzendő, hogy születtek olyan cikkek is, amelyek ezt a 400 évvel ezelőtti, hollandiai tulipánhagyma lázhoz hasonlítják[133]. Akkoriban a tulipánhagymák miatt alakult ki az első tőzsde, amely azonban 1637 februárjában napok alatt omlott össze, maga alá temetve egy egész gazdaságot. Igaz, ott tényleg nem volt a gazdasági teljesítménynek még a szikrája sem, és nem is kecsegtetett azzal, hogy valaha is óriási hasznot lehet húzni a kifejlett tulipánok eladásából. Ott csak a határidős és opciós ügyletek, a spekuláció számított. Jelen esetben azonban annyi, olyan sokféle és olyan mértékű innováció megvalósulását támogatja valamilyen módon a kriptovilág, hogy ezek közül bármelynek lehet esélye a startup fázisból való növekedésre[134]. Az is igaz, hogy maga a blockchain világa is sok új innovációt tartalmaz, amely további technológiai fejlesztéseket indukálhat.

Ki van mögötte?

Természetes módon felvetődik a kérdés, hogy különösen a publikus blockchain-ek mögött, van-e valaki, vagy valakik,

[130] A bitcoin bányászat által fogyasztott áram megegyezik kb. Dánia éves áramfogyasztásával.

[131] Ilyen – eBay-hez, Amazonhoz, Aliexpress-hez hasonló – internetes piacterek százával léteznek, ahol gyakorlatilag csak illegális árukkal kereskednek. A legnagyobb ezek közül az AlphaBay volt egészen addig, amíg az üzemeltetőjét idén nyáron holtan nem találták saját lakásában. Azonban ennek a helyét hamar átvették az egyéb illegális piacterek. Lásd: https://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/. Ezeknek a webhelyeknek az elérése egyébként külön hálózatot igényel, amely szintén a peer-to-peer kommunikáción alapuló, de titkosított adatátvitelen alapszik.

[132] Hozzáteendő, hogy a cikk írása és lektorálása közt (pár nap) eltelt időben ez a *„buborék"* jelentősen felfújódott, igaz, csak a bitcoinra vonatkozóan, a többi altkoinnál ilyet nem találunk. De a bitcoinnál ismét láz tartja élénken a piacot (igen erős *„bull market"* van), hiszen a cikk írásának kezdetén még 1 BTC=5700 USD volt, később már a szerző hivatkozott 6300 USD-s árfolyamra is, a cikk lektorálás utáni lezárásakor (2017. 11. 05.) pedig már az árfolyam több mint 7400 USD. Azaz időközben közel 30%-ot erősödött a BTC. Minden valószínűség szerint ez után valamilyen visszakorrigálás következik majd. A szerző is kíváncsi, hogy a jelen cikk megjelenésekor milyen árfolyamot jegyeznek majd a kriptotőzsdék.

[133] Lásd pl: https://www.cnbc.com/2017/07/20/bitcoin-bubble-dwarfs-tulip-mania-from-400-years-ago-elliott-wave.html, http://hvg.hu/gazdasag/20090608_tulipanmania_penzugyi_valsag_krach

[134] Azaz elérjen a kérdőjel (question mark) fázisból a felívelő (star) fázist, később pedig a pénztermelő (cash cow) fázist.

rejlik-e mögöttük valami hátsó szándék, vagy tényleg egy központ nélküli, konszenzuson alapuló új dolog, amely önmagától működik? Az ICO-knál már láttuk, hogy azok startup cégek finanszírozását szolgálják, ott természetes módon maguk a startup-ok alapítói vannak a megoldások mögött. Az, hogy ők kik, lehet-e róluk többet tudni, mint azt, hogy pár fényképes rövid életrajzzal bemutatkoznak az adott startup honlapján, nem tudhatjuk.

A kérdés inkább az, hogy pl. a Bitcoin, vagy az Ethereum, és ennek megoldásai mögött kik vannak, és egyáltalán milyen hatásuk lehet a rendszer működésére? Esetleg valamilyen központi hatalom van mögötte, valamely kormány, aki ily módon akar szuperhatalommá válni, vagy ezt a státuszát erősíteni?

Az Ethereum esetében az alapítók, a már korábban említett *Vitalik Buterin* és fejlesztő társai, valamint más szakemberek Svájcban bejegyezték az Ethereum Alapítványt.[135] Ennek az alapítványnak azonban a további fejlesztésekre nincs sokkal nagyobb hatása, mint bárki másnak, aki időt és energiát szán egy fejlesztésre. Az Ethereum Virtual Machine működésére, amely maga a rendszer, semmi hatása nincs, hiszen a rendszer elosztott. Igaz azonban, hogy amennyiben ezen alapítvány égisze alatt jön ki egy új fejlesztés, abban a résztvevők jobban fognak hinni, mint ha bárki megjelenne *„a semmiből"*, hogy ő jelentőset fejlesztett az Ethereum rendszeren, és ezt a fejlesztést most mindenki legyen szíves használatba venni. De ne feledjük, hogy a publikus blockchain megoldások szinte mindegyike nyílt forráskódú szoftvereken alapszik, azokhoz bárki hozzáférhet, és akár ellenőrizheti, hogy nincs-e bennük valami hiba[136].

A Bitcoin rendszer esetében már bonyolultabba kérdés. Mivel a Bitcoin megálmodója, *Satoshi Nakamoto* személye azóta sem azonosított, és van pár fejlesztő, aki a Bitcoin Core[137] nevű rendszert, azaz az ún. referencia rendszert fejleszti[138], sokan úgy gondolják, hogy ez a pár ember az, akitől a rendszer működése függ. Azonban a referencia rendszer is csak egy a sok megvalósítás közül, a lényeg az, hogy a szabályrendszert, a protokollt kövesse egy megvalósítás. Tehát leginkább az a kérdés, hogy van-e valaki, vagy valakik, akik erőszakos módon meg tudják változtatni a szabályrendszert. Erre viszont tudjuk a választ a korábbiakból, hogy ez csak a bányászatnál, a hash-eléshez felhasznált számítástechnikai kapacitás (hashpower) 51 %-os, egy kézben történő birtoklása esetén lehetséges, és ha mégis, annak leginkább az adott blockhain kettéválása (fork) lenne a következménye, mint az, hogy valaki ráerőszakolja a saját egyéni szabályait egy ilyen rendszerre.[139] Tehát a Bitcoin rendszer, mint publikus blockchain működése szempontjából teljesen mindegy, hogy kicsoda *Satoshi Nakamoto*. A rendszer mára elérte azt a kritikus tömeget, hogy csak konszenzusos alapon lehet a szabályait úgy megváltoztatni, hogy a lánc (azaz a blockchain) több részre válása elkerülhető legyen.

[135] https://www.ethereum.org/foundation

[136] Az Ethereum esetén egy ilyen, sajnos túl későn feltárt hiba vezetett a *„The DAO"* hacking-hez, lásd az erről szóló fejezetet.

[137] https://bitcoincore.org/en/about/

[138] https://bitcoincore.org/en/team/

[139] Erről korábban, az 51 %-os támadás leírásakor már ejtettünk szót.

Mit csinálnak a nagyvállalatok?

Az információtechnológiai óriásvállalatok közül az IBM volt az első, amelyik meglátta a lehetőséget a blockchain technológiában[140], és ma a legfejlettebb, erre alapuló megoldással rendelkezik. De ugyanúgy a Microsoft[141] is *„beszállt"*, valamint az SAP[142] és az Oracle[143] is rendelkezik már blockchain alapú megoldásokkal. Jellemző azonban, hogy ezek a cégek nem magába a blockchain rendszerbe invesztálnak, hanem saját technológiai megoldásokat adnak el, jellemzően privát blockchain-t alkalmazó felhasználóknak. Természetesen vannak olyan vállalatok, amelyek erre a technológiára jöttek létre, ehhez adnak el eszközöket, szoftvereket, komplett megoldásokat (pl. R3, 21, Coinbase, Bitmain, Ledgerwallet, Trezor)[144]. A szektor igen látványos fejlődésére jellemző, hogy egyre másra alakulnak (nem csak ICO-ra alapuló), blockchain technológiát kínáló vállalatok[145].

Államok, akik „be akarnak szállni"

Több állam is úgy érezte, hogy valamit kezdenie kell a blockchain technológiával. Van, aki tiltotta (fentebb többször esett szó Kínáról, de az USA-ban – ahol már szabályozott a kriptovaluták világa – szintén vannak tiltó rendelkezések[146]), és vannak, akik élenjárók szeretnének lenni. Észtország bejelentette, hogy bevezetné saját kriptovalutáját, az Estcoint[147]. Ezt a kísérletet azonban az Európai Központi Bank visszautasította[148], mondván, hogy az EU-ban már van egy hivatalos fizető eszköz, ez pedig az Euro. Oroszország is fontolgatja a Rubel mellett blockchain-en alapuló fizető eszköz, *„kripto-rubel"* bevezetését,[149] de kis államok is megpróbálnak az élre törni, pl. az off-shore cégek egyik fő bejegyzési helyéről ismert Vanuatu is jelezte, hogy kriptopénzt kíván bevezetni, igaz, egyelőre arra, amennyiben valaki a vanuatui adóparadicsom állampolgára kíván lenni, és ezért kriptopénzzel kíván fizetni.[150]

Más oldalról viszont nem csak fizetőeszközként tekintenek az egyes államok a blockchain-en alapuló megoldásokra. Van, aki blockchain stratégiát dolgozott ki, pl. ilyen az Egyesült Arab Emirátusok egyik tagja, Dubai[151], mások, köztük

[140] https://www.ibm.com/blockchain/

[141] https://azure.microsoft.com/hu-hu/solutions/blockchain/

[142] https://www.sap.com/products/leonardo/blockchain.html

[143] https://www.oracle.com/cloud/blockchain/index.html

[144] http://www.cbronline.com/news/verticals/fintech/top-10-biggest-blockchain-players/

[145] https://investingnews.com/daily/tech-investing/blockchain-investing/blockchain-technology-stocks/

[146] Virtual currency law in the United States – https://en.wikipedia.org/wiki/Virtual_currency_law_in_the_United_States

[147] https://www.cnbc.com/2017/08/23/estonia-cryptocurrency-called-estcoin.html

[148] https://www.reuters.com/article/us-ecb-bitcoin-estonia/ecbs-draghi-rejects-estonias-virtual-currency-idea-idUSKCN1BI2BI

[149] https://www.rt.com/business/400728-blockchain-russia-ruble-cryptocurrency/

[150] https://news.bitcoin.com/vanuatu-becomes-first-nation-to-accept-bitcoin-as-citizenship-payment/

[151] http://www.smartdubai.ae/dubai_blockchain.php

Brazília[152], ill. Svédország[153] is bejelentette, hogy blockchain technológián kívánja közzétenni a földhivatali regisztrációs adatokat, illetve a továbbiakban így regisztrálni földtulajdonokat, ezzel is lehetővé téve mindenki számára, hogy azok hitelességét ellenőrizze.

Szabályozni, vagy sem?

A publikus blockchain-en alapuló – elsősorban fizetési – megoldások megbízható harmadik fél nélkül működnek, azaz kikerülik a bankrendszert. Az okos szerződések esetén a polgári jogot érvényesítő ügyvédeket, illetve a bírói rendszert hagyja ki a konszenzuson alapuló, elosztott rendszer. Sőt, a konszenzus jellege miatt egy adott állam jogrendszerét is megkerülik, hiszen az okos szerződést a világon lévő összes csomópont (node) ellenőrzi, hajtja végre, és ez a végrehajtás teljesen független attól, hogy az okos szerződésben foglaltak pl. adott állam területén jogellenesek. Mindemellett, amint fentebb többször is szó esett róla, az alvilág is intenzíven használja a kriptopénzeket, és nyilvánvaló, hogy ezzel a vonatkozó jogrendet kerüli ki, azaz függetleníti magát az egyes államok központi hatalmától.

Ebben a helyzetben eléggé nehéz megmondani, hogy hogyan és miként lehet szabályozni, valamint egy ilyen szabályozás időbeli, térbeli és személyi hatálya kikre terjed ki, és egyáltalán egy szabályozós szankció rendszere hogyan tartatható be?

Ha csak a kriptopénzek világát vesszük, már az is kérdéses szabályozási szempontból, hogy ez egyáltalán micsoda, áru, pénz, vagy valami új? A pénz jogi definíciója híján a közgazdasági definícióból szoktak kiindulni, azonban eddig nem sikerült sehol dűlőre jutni a tekintetben, hogy a kriptopénzek teljesítik-e azokat a követelményeket, amelyeket a közgazdaságtan a pénzzel szemben támaszt. Így a kriptovaluták jelen tudásunk szerint pénznek nem tekinthetők. Az áruként (vagy szolgáltatásként) való definiálás hasonló okokból szintén akadályokba ütközik.

Így a jelen társadalmát szabályozó jogrendszerekbe a kriptovaluták szabályozása igen nehézkesen fér be, és ezek a szabályok is sokszor megkérdőjelezhetők.[154] Ha belegondolunk azonban, hogy a jog általánosan élethelyzeteket szabályoz, látnunk kell, hogy ez itt egy teljesen új élethelyzet, tehát nem is biztos, hogy mindenáron a jelen jogi terminológiák közül kell választani akkor, amikor a szabályozásról esik szó. Volt már ilyenre korábban is példa, hiszen az pl. elektronikus aláírás technológiájának és elterjedésének megjelenése előtt olyan élethelyzet nem volt, amelyre ezt lehetett volna alkalmazni. Hiszen az elektronikus aláírás csak nevében *„aláírás"*, gyakorlatilag egy, csak elektronikusan létező számsorozat, amely mind az aláírót, mind az aláírt dokumentum (adathalmaz) azonosítására és az aláírt adathalmaz sértetlenségének (időnként aláírási idejének) igazolására szolgál. Így az elektronikus aláírás, mindamellett, hogy nem aláírás, egyszersmind több is, mint aláírás, mivel pl. a hagyományosan aláírt szerződések esetében a szerződés betű szerint pontos adattartalma nem mindig volt ellenőrizhető, csakúgy, mint kétség esetén a tényleges aláíró személye (ezért is vannak írásszakértők).

A blockchain-en alapuló megoldásoknál is valami hasonló a helyzet, azaz pl. a kriptopénzek fogalma teljesen új kell legyen, különböznie kell a pénz, de az áru fogalmától is. Az, hogy szabályozás szükséges, a fentiek alapján nem lehet kérdéses, tekintve a jelen nemzetközi trendeket is. Továbbra is a hogyan és miként a kérdés. Ha viszont a szabályozás alapjául ezt a teljesen új élethelyzetet vesszük alapul, remélhetőleg a szabályozó megszabadul egy nagy halom sztereotípiától, és képes lesz sui generis szabályozásra.

Konklúzió

A szerző megítélése szerint a blockchain mint innováció csak az utolsó csepp volt egy olyan innováció halmazban, amely mára már egy önfenntartó ökoszisztémát alkot. Ez az önfenntartó ökoszisztéma viszont jó táptalajként, és finanszírozási alapként szolgálhat további innovációknak, és lehet, hogy pár év múlva már nem az információ sűrűségről, hanem az innováció sűrűségről fognak szólni a hírek.

A fentiek alapján azonban további meggyőzés nélkül is látszik, hogy valamit lépni kell. De mit és merre, ezt még senki sem tudja. Egymásnak ellentmondó vélemények, nyilatkozatok látnak napvilágot, miközben a háttérben egy új, gazdasági, társadalmi, sőt politikai elit kialakulása rajzolódik ki. Mindez globálisan, határokon, nemzeteken átívelően. De a blockchain forradalmát hasznossá is lehet tenni. Ahhoz, hogy kiderüljön, hogy az államigazgatásnak, a politikai és gazdasági szabályozóknak, az egyes állami szereplőknek mit kell tenniük ehhez, még nem világos. Sem nálunk, se sehol a világon. Ami viszont látszik az az, hogy – mint minden anarchiának – a nagy szabadság, az állami főhatalom hiánya egyben negatívuma is. Hiszen, ha egyrészt nincs főhatalom, amelyet igénybe muszáj venni akkor, ha pl. adózni kell, ugyanúgy nincs, aki megvédje a szereplőket, igazságot szolgáltasson, jogbiztonságot adjon akkor, ha egyes szereplők vitába keverednek, netán meglopják őket. Lehet, hogy egyszer ezek a rendszerek *„tökéletesek"* lesznek, teljesen autonóm módon fognak viselkedni és szabályozni életünket, de ha bármi probléma adódik, kit lehet ezért felelőssé tenni?[155] Mindezekért nálunk, Magyarországon is komolyan kell venni a blockchain filozófiáját, mind a gazdasági és politikai szereplőknek, mind a szabályozóknak, mind a közigazgatásnak.

[152] Blockchain Land Registry Tech Gets Test in Brazil – https://www.coindesk.com/blockchain-land-registry-tech-gets-test-brazil/

[153] Sweden Officially Started Using Blockchain to Register Land and Properties – https://cointelegraph.com/news/sweden-officially-started-using-blockchain-to-register-land-and-properties

[154] Korábban már hivatkoztuk, hogy egyedül az USA-ban és Kínában van szabályozva a kérdéskör.

[155] Russian President Putin Praises and Bashes Cryptocurrencies – https://www.cryptocoinsnews.com/russian-president-putin-praises-bashes-cryptocurrencies/ – Idézet a cikkből: *„Putin went on to explain that cryptocurrencies "are issued by an unlimited number of anonymous sources". In any event of "system malfunctions" or volatility, no-one would be held liable, Russian president Putin added in his critique."*