Bitcoin: digitális szemfényvesztés, vagy a jövő valutája?*

Bugár Gyöngyi – Somogyvári Márta

A bitcoin az elmúlt tíz év egyik legérdekesebb pénzügyi innovációjának nevezhető. Az esszében arra keressük a választ, hogy miért nem terjedt el fizetőeszközként, hogyan vált ehelyett kockázatos befektetési formává. Megvizsgáljuk a bitcoin-technológia működési mechanizmusát, és bemutatjuk a bitcoin népszerűségét megalapozó ideológiai hátteret. Következtetéseink szerint a bitcoin a mostani formájában nem alkalmas arra, hogy általánosan elfogadott fizetőeszközzé váljon.

Journal of Economic Literature (JEL) kódok: E42, G10, O31

Kulcsszavak: bitcoin, kriptovaluta, blockchain, libertariánus gazdaságpolitika

1. Bevezetés

Az utóbbi évtized talán egyik legérdekesebb pénzügyi innovációja a bitcoin és más kriptovaluták megjelenése. Ez a fizetőeszköznek szánt befektetési forma ma már mindenki számára elérhető, akár az interneten, akár a Budapesten is megtalálható bitcoin ATM-eken keresztül. Azonban sem az egyszerű felhasználók, de még a pénzügyi szakemberek jó része sincs tisztában a bitcoint megalapozó ideológiával, e kriptovaluta működési mechanizmusával és a benne rejlő kockázatokkal. Célunk az, hogy bemutassuk azt az elméleti problémát (double spending), amelynek megoldására Nakamoto kidolgozta a bitcoin alapjául szolgáló blockchain-rendszert, és felvázoljuk a bitcoin működési mechanizmusát, mai szerepét. Rá kívánunk világítani arra az ideológiai háttérre is, ami a bitcoin népszerűségét biztosítja, és fenntartja a bitcoin-közösséget. E területek áttekintésével szeretnénk megválaszolni a címben felvetett kérdést, és kitekinteni a bitcoin jövőbeli felhasználási lehetőségeire. Ezután bemutatjuk a bitcoin technológiai hátthereként szolgáló fehér könyvet, a kriptovalutá-

* A jelen kiadványban megjelenő írások a szerzők nézeteit tartalmazzák, ami nem feltétlenül egyezik a Magyar Nemzeti Bank hivatalos álláspontjával.

Bugár Gyöngyi egyetemi docens a Pécsi Tudományegyetem Közgazdaságtudományi Kara Kvantitatív Menedzsment Intézetében. E-mail: bugar.gyongyi@ktk.pte.hu
Somogyvári Márta egyetemi docens a Pécsi Tudományegyetem Közgazdaságtudományi Kara Kvantitatív Menedzsment Intézetében. E-mail: somogyvari.marta@ktk.pte.hu

A kutatást az Innovációs és Technológiai Minisztérium Felsőoktatási Intézményi Kiválósági Programja finanszírozta, a Pécsi Tudományegyetem *4.* tématerületi programja – *A hazai vállalatok szerepének növelése a nemzet újraiparosításában* – keretében.

A magyar nyelvű kézirat első változata 2019. szeptember 14-én érkezett szerkesztőségünkbe.

DOI: http://doi.org/10.25201/HSZ.19.1.132153

kat megalapozó ideológiát, és rámutatunk a bitcoin jelentőségére. A *3. fejezetben* ismertetjük a bitcoint megalapozó blockchain-technológiát és működési mechanizmusát. A *4. fejezetben* megvizsgáljuk, hogy fizetőeszközként, illetve befektetési lehetőségként milyen szerepet játszik a gazdaságban. Az *5. fejezetben* rámutatunk elterjedésének korlátaira, ami egyrészt a technológiából, másrészt a szabályozási környezetből adódik. Végül összegezzük a bitcoin jövőjével kapcsolatos meglátásainkat.

2. A bitcoin-rendszer kialakítása, a bitcoin szerepe és jelentősége

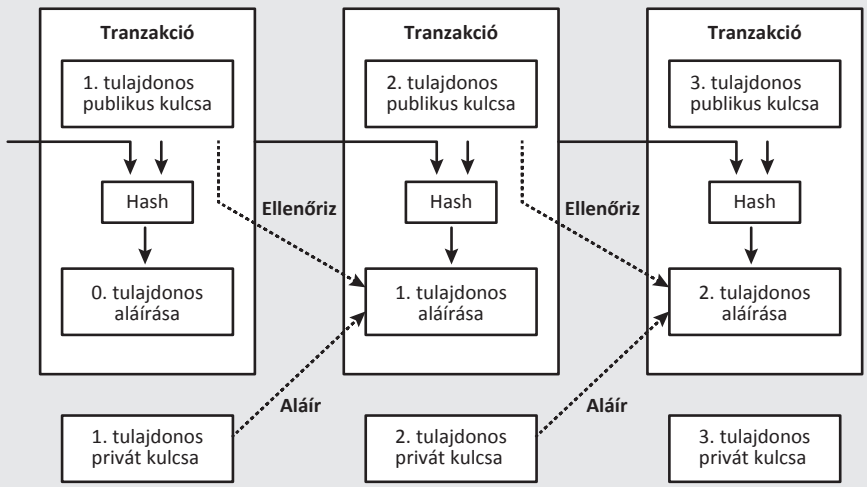
2.1. A bitcoin fehér könyve: a rendszer kialakítása

Satoshi Nakamoto 2008. október 31-én publikálta egy új, innovatív fizetési rendszerre vonatkozó elképzelését egy kriptográfiával foglalkozó levelezőlistán. A filantrópiai küldetéstudat által vezérelt szerző kilencoldalas tanulmányában – a legutóbbi pénzügyi világválság legkeményebb évében – egy bankoktól mentes, központi (közvetítő) szereplő nélküli, független és egyenrangú szereplők közötti online fizetési hálózatot ír le (*Nakamoto 2008*), amely lényegében mindenki számára hozzáférhető. A bitcoin-rendszer minden idők legelső, kriptográfiát alkalmazó, decentralizált fizetési koncepciójának tekinthető (*Gábor – Kiss 2018*).

A Nakamoto által elképzelt és megvalósított, nyílt forráskódú rendszer nem bizalmon, hanem digitális aláírásokon alapul. A nyílt forráskód révén a rendszer publikus, abba bárki szabadon beléphet, és bármikor ki is léphet belőle. A szerző a hálózatban előállított *bitcoint* úgy definiálta, mint *digitális aláírások láncolatát*. Egy tranzakció során az elektronikus érmét tulajdonosa úgy ruházza át a következő tulajdonosra, hogy privát kulcsa segítségével digitálisan aláírja az előző tranzakcióból származó hash-t[1], valamint a következő tulajdonos publikus kulcsát, és ezt az érmét reprezentáló aláírás-sorozat végéhez csatolja. A hash-függvények (magyarul hasítófüggvények) olyan informatikában használt eljárások (tulajdonképpen rejtjelezési algoritmusok), amelyekkel bármilyen hosszúságú adatot adott hosszúságúra képezhetünk le. Az így kapott véges adat neve hash (hasító érték). A hash tulajdonképpen egy, az eredeti üzenetet azonosító ellenőrzőkód, egyfajta digitális ujjlenyomat[2]. A kedvezményezett a hitelesség megerősítése céljából ellenőrizheti a digitális aláírásokat. A fentiekben leírt tranzakciók sorozatát az *1. ábrán* szemléltetjük.

[1] A hash jelentése szó szerinti fordításban: hasadék, darálék, darált hús.
[2] Schaffer József: *A Bitcoin ismertetője*. Elektronikus feljegyzés, 2014. január 7. http://plastik.hu/2014/01/07/a-bitcoin-ismertetoje/. Letöltés ideje: 2019. augusztus 14.

1. ábra
A bitcoin átruházására szolgáló tranzakciók láncolata



Forrás: Nakamoto (*2008:2*) *alapján szerkesztve*

A rendszer működése szempontjából fontos kihívás annak megakadályozása, hogy egy már elköltött összeget újra el lehessen költeni. Ennek a problémának a megoldására *Nakamoto* (*2008*) a tranzakciók nyilvánosságra hozatalát és a hálózat szereplőinek konszenzusán alapuló tranzakcióhitelesítést javasolt. Ezzel ki tudja küszöbölni azt a központi szereplőt, amely az elszámolást végzi, és garantálja a tranzakciók hitelességét.

A tranzakciók nyilvánosságra hozatala egy megosztott nyilvántartási könyv (osztott főkönyv) segítségével történik, amely lényegében a tranzakciókat tartalmazó adatbázis, és bármely szereplő számára elérhető. Ebben az adatok (az egyes tranzakciók) blokkokba vannak rendezve, a hitelesített blokkok pedig láncot alkotnak (blockchain, magyarul blokklánc). A hálózat egyes csomópontjai versenyeznek abban, hogy ki tudja először a soron következő pénzügyi tranzakciókat tartalmazó adatblokkot megfejteni, és a hitelesítést igazoló digitális időbélyegzővel ellátni. Ez egy kellően nehéz matematikai algoritmus alkalmazására épülő kódfejtést jelent (proof-of-work). Ezzel válik igazolhatóvá, hogy egy adott tranzakció résztvevője a tranzakcióban szereplő összeget korábban még nem próbálta elkölteni.

A tranzakciók hitelesítéséért versengő szereplőket *Nakamoto* (*2008*) bányászoknak nevezi. A bányászokat az motiválja, hogy a blokkok megfejtéséért bitcoint kapnak cserébe. Alapjában véve így keletkezik a pénz a rendszerben, azaz a blokkokat dekódoló tranzakcióhitelesítők végzik a pénzteremtést.

A hálózat működtetésének lépéseit *Nakamoto* (*2008:3*) a következőképpen írja le:

1) Az új tranzakciók elterjesztése az összes csomópont számára;

2) Minden egyes csomópont egy blokkba gyűjti az új tranzakciókat;

3) Az egyes csomópontok dolgozni kezdenek a blokk megfejtésén;

4) Amint egy csomópont sikeresen megfejti a blokkot, továbbítja azt a többi csomópontnak;

5) A csomópontok csak akkor fogadják el a blokkot, ha minden általa tartalmazott tranzakciót érvényesnek találnak, és nem derül fény arra, hogy egy pénzösszeget újra el akartak költeni;

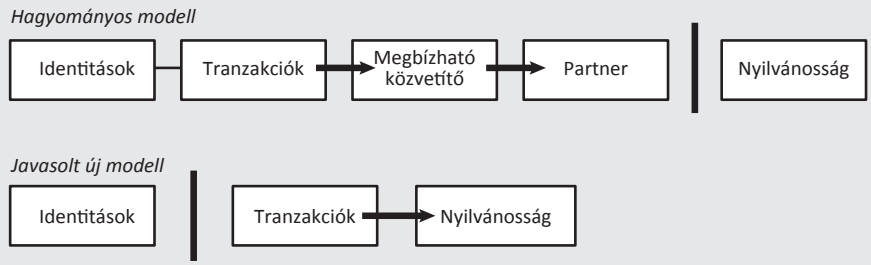
6) A csomópontok úgy fejezik ki a blokk elfogadását, hogy dolgozni kezdenek a lánc következő blokkján azáltal, hogy elkezdik alkalmazni az azt megelőző, elfogadott blokk hash-értékét.

A rendszer biztonságos működését az egyes csomópontok többségi konszenzusán alapuló hitelesítési folyamat garantálja. A csomópontok mindig a leghosszabb láncot fogadják el korrektnek, és ennek kiterjesztésén dolgoznak folyamatosan. Ha két csomópont egyidejűleg a következő blokk eltérő változatát osztja meg a többi csomóponttal, akkor bizonyos csomópontokhoz az egyik, míg másokhoz a másik változat érkezhet be először. Ebben az esetben az elsőként beérkező blokkon dolgoznak tovább, de lementik a másikat is arra az esetre, ha az azt tartalmazó blokklánc hosszabbá válna. Az mindig a soron következő blokk megfejtésével válik nyilvánvalóvá, hogy melyik blokkot kell elvetni, azaz melyik ágon kell továbbhaladni. (Ebből adódik, hogy azok a tranzakciók, amelyek egy rövidebb blokkváltozatban szerepelnek, nem teljesülnek, így azokat újra kell indítani.)

Nakamoto (*2008*) a rendszer biztonsága szempontjából rámutatott a rendszerben meglévő ösztönzőrendszer fontosságára. Minden blokk első tranzakciója speciális tranzakció, amely egy új, a blokk megfejtőjének tulajdonába kerülő virtuális pénzt (bitcoint) teremt. Ez motiválja a csomópontokat a rendszer támogatására, és ugyanakkor biztosítja a virtuális pénzegységek forgalomba kerülését. Egy blokk megfejtéséért járó „juttatás" tulajdonképpen a kódfejtésre használt számítógép-erőforrások (CPU-kapacitások) és a ráfordított elektromos energia megtérülését szolgálja. Ez a rendszerbe beépített ösztönző *Nakamoto* (*2008*) meggyőződése alapján segíti azt, hogy a rendszer szereplői kövessék a szabályokat. Ha megjelenik a hálózatban egy kapzsi „támadó", aki több CPU-kapacitást birtokol, mint a becsületes csomópontok együttesen, akkor választhat, hogy erre támaszkodva – a rendszer szereplőinek megtévesztésével – visszaszerzi az addigi befizetéseit, vagy erőforrásait arra használja, hogy új pénzt teremtsen. *Nakamoto* (*2008*) szerint ebben az esetben fel kell ismer-

nie, hogy jövedelmezőbb számára, ha betartja a „játékszabályokat", amelyek abban támogatják, hogy így több új bitcoinhoz juthat, mint a többi szereplő együttesen.

2. ábra
A hagyományos pénzügyi közvetítői rendszer és a bitcoin titoktartási modelljének összehasonlítása



Forrás: Nakamoto (*2008:6*) *alapján szerkesztve*

Nakamoto (*2008*) fizetési rendszere a tranzakciók nyilvánosságra kerülése tekintetében is eltér a hagyományos banki titoktartási modelltől. A hagyományos banki modell a résztvevő felek, valamint a megbízható harmadik fél (közvetítő bank) számára korlátozott hozzáférést biztosít az információkhoz, a nyilvánosságot pedig egy tűzfallal teljesen kizárja az információáramlás folyamatából. A tranzakciók nyilvánossá tételének szükségessége kizárja az előző modellt, de a személyes adatok védelme, sőt az anonimitás – az információáramlás más ponton történő megszakításával – fenntartható. A publikus kulcsok ugyanis nem névre szólók. Az arra vonatkozó információ, hogy valaki küld egy másik személynek (identitásnak) egy összeget, nyilvánosan elérhető anélkül, hogy a tranzakció résztvevői azonosíthatók lennének. Ez hasonlít a tőzsdék által követett titoktartási elvekhez, ami abban áll, hogy nyilvánosságra hozzák az egyedi tranzakciók méretét és idejét, a bennük részt vevő felek azonban nem ismertek. A két modell közti különbséget a *2. ábrán* szemléltetjük.

2.2. A bitcoint megalapozó filozófiák

Nakamoto bitcoint megalapozó tanulmánya látszólag egy, az online átutalási rendszerek technikai problémáival foglalkozó tanulmány, amely ki akarja küszöbölni a bankokat és a pénzügyi intézményeket az átutalási folyamatból. A bitcoin és a kriptopénzek elterjedése azonban nem a technológiának, hanem a technológia által képviselt ideológiának köszönhető. Ennek az ideológiának két fontos eleme a mindenfajta állami szabályozás, így a központi bankok és a monetáris szabályozás megkérdőjelezése, illetve a digitális létforma elsőbbségét hirdető cyber-libertarianizmus.

Az USA ultrakonzervatív köreinek felfogása szerint az állam autoriter (*Levin 2009*), s mindenféle állami beavatkozás, így például a szociális transzferek, így az alanyi jogon járó egészségbiztosítás is, az egyéni szabadság megsértését jelentik. A bitcoin-közösségben ezek a gondolatok újra meg újra felvetődnek, s innen adódik a bitcoin mozgalmi jellege is, amivel újabb meg újabb bitcoin-hívőket tudnak elérni. Eszerint minden kormányzás elvetendő, csak a piaci erők jók, amelyekkel meg lehet akadályozni a hatalom koncentrációját, ami, ha az állam, a kormányzat rendelkezik vele, akkor túlzott hatalmi fókuszhoz vezethet. Kritizálják a monetáris politika vitelét, valamint összeesküvés-elméletekre hivatkozva a Fed és a központi bankok tevékenységét is (*Rothbard 2002, Mullins 1992*). E szélsőséges nézetek szerint (lásd *Golumbia 2016*) az infláció és a defláció nem gazdasági okokra vezethető vissza, hanem a központi bankok tevékenységének eredménye. Ez a gondolatkör alapozza meg az inflációtól mentes pénz megteremtésének igényét a bitcoin algoritmusában.

A cyber-libertarianizmus a digitális létforma elsődlegességét hangoztatja, s ez nemcsak a bitcoin hívei, hanem sokszor a digitális világ szereplői számára is az egyetlen elfogadható világnézet. Ennek egyik megnyilvánulása az internet abszolút szabadságának védelmezése. A valódi és egyedül fontos szakértelem a cyber-libertariánusok számára a digitális technológiákra vonatkozik, s mivel minden visszavezethető IT-folyamatokra és IT-algoritmusokra, ha valaki ezekhez nem ért, akkor nincs joga véleményt mondania (*Golumbia 2016*). Így a bitcoinnal kapcsolatos minden olyan kritikai észrevétel, amely gazdasági, társadalmi vonatkozásokat emel ki, diszkvalifikálódik a bitcoin hívei előtt.

2.3. A bitcoin jelentősége a kriptovaluták között

2.3.1. A kriptovaluták típusai

A kriptovaluták két fő csoportját a saját blockchainnel rendelkező digitális pénzek (digital coin) és a már meglevő blockchainre épített tokenek alkotják. Az első csoportot is két részre szokták osztani, ide tartozik a bitcoin, amely ki tudta használni a piacra először belépő szereplők innovációs előnyét, és máig a legjelentősebb kriptovaluta, illetve azok az alternatív kriptovaluták, az altcoinok, amelyek vagy a bitcoin leszármazottai, vagy teljesen új blockchain-algoritmusra épülnek.

Hogyan jöhetnek létre új kriptovaluták a bitcoinból? A bitcoin nyílt forráskódú, osztott főkönyvű, vagyis blockchain-szoftverre épül, ami azt jelenti, hogy lehetőség van a szoftver kódjának megváltoztatására. Amennyiben ezzel a változtatással nem ért egyet az adott blockchain közössége, akkor akár véglegesen kettéválhat a blockchain (ezt nevezik „fork”-nak). Az új kódra épülő blockchain – ami azelőtt a bitcoin része volt, ezután önálló, a bitcointól független életet él. A kód megváltoztatásának az egyik célja az, hogy új tulajdonságokkal ruházzák fel a szoftvert, így jött létre a tranz-

akciók sebességének megnövelésére alkalmas litecoin. Arra is lehetőség van, hogy alapvető változtatásokat hajtsanak végre a kódon, megnövelve például a blokkok méretét 1MB-ról 8MB-ra, ez vezetett a bitcoin cash kialakulásához. Találunk olyan altcoinokat is, amelyek nem a bitcoin leszármazottai, hanem teljesen új blockchainre épülnek, mint az Omni, az Ether vagy a Ripple.

A kriptovaluták második csoportját az ún. tokenek alkotják. A tokenek nem rendelkeznek külön blockchainnel, hanem olyan platformokat használnak (ilyen a saját altcoinra, az Etherre épülő Ethereum), amelyek lehetővé teszik, hogy a platformok saját blockchain-architektúrájára épülő applikációkkal (DApp) hozzanak létre másodlagos, digitális „kriptopénz-helyettesítő" eszközöket. Ez a folyamat sokkal egyszerűbb, mint a saját blockchain kialakítása. A forgalomba hozáshoz meghirdetik az ún. ICO-t (Initial Coin Offering) egy White paper (fehér könyv) formájában. A tokenek jelképezhetnek valamilyen szolgáltatást, amelyhez a projekt indulása vagy sikeressége esetén hozzá lehet férni, vagyis a token kibocsátása ilyenkor a közösségi finanszírozás új formájaként fogható fel, de gyakran ezeket is befektetési céllal vásárolják.

Jellemzően azok a tokenek népszerűek, és azok árfolyama éri el a kibocsátáskori értékük sokszorosát, amelyek a blockchain-technológia továbbfejlesztését tűzik ki célul. Az IOTA[3] célja egy új filozófiára épülve a tranzakciók lebonyolításának felgyorsítása, az NXt a kriptovaluták elleni támadásokat szeretné kivédeni egy új hitelesítési módszerrel. A cryptocompare.com weboldalon felsorolt 1 394 token több mint 90 százaléka a kibocsátáskori értékét rövid idő alatt elveszti, néhány hónap múlva már csak töredékét éri. Az Ázsiában, elsősorban Koreában és Kínában népszerű, Ponzi-sémára épülő, havi 9–18 százalék kamatot ígérő PLUS Token összeomlása 2019 júniusában egyes becslések szerint 3,5 milliárd dollár értékű kárt okozott a befektetőknek (*Emsley 2019*).

2.3.2. A legfontosabb kriptovaluták piaci kapitalizációja

A coinmarketcap.com 2019. augusztus 24-én csaknem 2 500 kriptovalutát tartott számon. Nap mint nap generálnak újabb és újabb kriptovalutákat, és a legtöbb viszonylag rövid életű. A bitcoin a legnagyobb kriptovaluta, a piaci dominanciája csaknem 70 százalékos, ami árfolyamtól függően egy 180 milliárd dollár körüli piaci kapitalizációt jelent. A bitcoint követő második legnagyobb kriptovaluta, az Ethereum 20 milliárd dolláros, a Ripple, ami egy centralizált, egy cég kezében összpontosuló blockchain a bankközi átutalások meggyorsítására, 11 milliárd dolláros piaci kapitalizációval rendelkezik. Vajon mit jelent egy kriptovaluta esetében az USD-ben kifejezett piaci kapitalizáció? Definíció szerint a forgalomban levő kriptovaluták (coinok vagy tokenek) száma megszorozva a piaci árral. Ez a számítási módszer lemá-

[3] A IOTA szakít a blockchainnel és a hitelesítést gráfok segítségével végzi (DAG: irányított körmentes gráf). Nincs szükség bányászatra, így az egyes tranzakciók energiafelhasználása elenyésző, a rendszer sokkal gyorsabb és skálázhatóbb, mint a blockchain. Popov, S.: *The Tangle*. 2018. April 30, Version 1.4.3. https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

solja az értékpapírok piaci kapitalizációjának definícióját. Miután az egyes valuták esetében alkalmazott mutatószámok (átváltási árfolyam, vásárlóerő, infláció stb.) nem alkalmazhatók a kriptovalutákra, már önmagában ennek az indikátornak az alkalmazása is megkérdőjelezi a kriptovaluták pénzjellegét.

3. A bitcoin technológiai háttere

3.1. Blockchain (osztott főkönyv)-technológia

A blockchain a bitcoin legfőbb technológiai újítása.[4] Egy megosztott, nyilvános főkönyvként működik, amely rögzíti az összes bitcoin-tranzakciót. Ez biztosítja a rendszer összes szereplője számára a nyilvánosságot és a transzparenciát. A blokklánc tulajdonképpen egy folyamatosan növekvő, a tranzakciókat tartalmazó adatblokkokból álló lista, amelyben az egyes blokkokat a hamisítást és módosítást kizáró módon kötik össze.

A digitálisan rögzített adatblokkokat egy lineáris láncban tárolják. A tranzakciókat tartalmazó adatblokkokat egy hash-függvény segítségével titkosítják (kriptográfiailag kódolják) és időbélyegzővel látják el. Amikor egy bányász új blokkot hoz létre, akkor ez tartalmazza az előző blokk hash-ét, így a blokkok – a legelsőként létrehozott, ún. genezis-blokktól kezdődően és a legújabb blokkig bezáróan − egy időben rendezett láncot alkotnak. Ez a folyamat újra meg újra ismétlődik, ezáltal növekszik a hálózat.

A blokklánc minden egyes blokkja tartalmaz adatokat (ilyenek például a bitcoin-tranzakciókra vonatkozó adatok), blokkfejlécet, blokkazonosítót és Merkle-fát.

- A blokkfejléc az adott blokkra vonatkozó metaadatokból[5] áll. Ezek a következők: (a) a blokkot időben megelőző blokk hash-értéke, amely az előző blokk azonosítására szolgál; (b) a blokkot megfejtő bányász azonosítására szolgáló adatok; (c) a blokkban foglalt tranzakciókat összegző adatstruktúra, amely Merkle-fa-gyökérként ismert.

- A blokkazonosító lényegében az a hash-érték, amely az adott blokk egyértelmű azonosítására szolgál.

- A Merkle-fa a blokk tranzakcióinak összefoglalására hivatott. A „fa" kifejezés a számítástechnikában egy elágazó adatszerkezet leírására használatos. A Merkle-fákat általában fejjel lefelé ábrázoljuk, azaz „gyökerük" van az ábra tetején, míg „leveleik" a diagram alján. A Merkle-fa szerepe, hogy a blokkban szereplő tranzakciókból egy átfogó digitális ujjlenyomatot hozzon létre, és így hatékony eljárást biztosítson

[4] Az alfejezet megírásában két forrásra támaszkodtunk: a Blockchain Technologies honlapján közzétett információkra (https://www.blockchain-technologies.com) és Andreas M. Antonopoulos „Mastering Bitcoin" nyílt kiadású könyvének „Bitcoin fejlesztőknek" címmel, elektronikusan hozzáférhető fordítására (https://bitcoinbook.info/wp-content/translations/hu/book.pdf).

[5] A metaadat (angolul metadata) az adatra vonatkozó adat.

annak ellenőrzésére, hogy egy adott tranzakció valóban szerepel-e a blokkban. A Merkle-fa csomópontpárok rekurzív hash-elésével épül fel egészen addig, amíg már csak egy hash, az úgynevezett gyökér vagy Merkle-gyökér marad.

A bitcoin-blokklánc technológiájának legfontosabb jellemzői az alábbiak:

- Konszenzus: arra utal, hogy a hálózat valamennyi anonim részvevője egyetért a hálózat szabályainak követésében, azaz elfogadja, hogy a blokklánc-környezetben „csak egy igazság létezik". Ehhez a résztvevők 51 százalékának egyetértése szükséges. Ebből adódik, hogy megfelelő számítási kapacitással, amennyiben a csomópontok 51 százalékát egy szereplő uralja, meghekkelhető a blokchain.
- Megosztott adatfeldolgozás: azt fejezi ki, hogy nincs központi csomópont az adatok feldolgozására és elosztására, minden csomópont függetlenül feldolgozhatja és továbbíthatja a hálózat számára a már hitelesített adatokat.
- Információtárolási képesség: azt jelenti, hogy a technológia alkalmas a tranzakciók adatainak és a hozzájuk kapcsolódó információknak a rögzítésére és megőrzésére.
- Tranzakciók eredetének azonosíthatósága: arra utal, hogy minden tranzakció és ahhoz fűződő aktivitás rögzítésre kerül, így teljes mértékben nyomon követhető.
- Megmásíthatatlanság: azt fejezi ki, hogy a hálózat egyetlen résztvevője sem módosíthat egy már rögzített tranzakciót. A hibás rekord nem törölhető, és mindig látható, ha egyszer rögzítették. A hiba kijavítása a hibás tranzakciót ellentételező, új tranzakció indításával lehetséges.
- Nyilvános hozzáférhetőség: azt jelenti, hogy a rendszer valamennyi szereplője korlátozás nélkül kapcsolódhat a hálózathoz, és elérheti a blokkláncban tárolt adatokat.

3.2. SHA–256 algoritmus

Az SHA, a Secure Hash Algorithm (magyarul biztonságos hasító algoritmus) kifejezés rövidítése. Az eljárás a kriptográfiában (titkosításban) használt legelterjedtebb hasító algoritmusok egyike. Az SHA az Egyesült Államok Nemzeti Szabvány- és Technológiai Hivatala (NIST: National Institute of Standards and Technology) által kibocsátott szabványos eljárások összefoglaló elnevezése, amelyek egyike a bitcoin esetében alkalmazott SHA–256 algoritmus. Bár a hasítófüggvények a számítástechnikában már az 1950-es évek elején megjelentek, csak az 1980-as évek legvégén – az elektronikus aláírás megjelenésével – terjedtek el igazán (*Buttyán – Vajda 2012*).

Az SHA első változatát (SHA 1) 1993-ban fejlesztették az Egyesült Államok rádiótechnikai jelhírszerzéssel foglalkozó szervezetének (NSA: National Security Agency) felügyelete alatt. Ez 160 bit hosszúságú üzenetkivonatot képez, amelyet ezt követően a digitális aláírás algoritmusban használhatunk. A bitcoin esetében alkalmazott

SHA–256 hasonló elvek alapján működik, azonban lényegesen nagyobb adatmennyiséget képes kezelni. A bemenete (a továbbítandó üzenet) $2^{64} – 1$ bit hosszúságú lehet, amelyet a feldolgozás során 512 bites blokkokra osztanak. Az output mérete (a kapott hash/hasító érték) összességében 256 bit hosszúságú és 8 darab 32 bites blokk alkotja[6]. Az SHA–256 elnevezés tehát az algoritmus alkalmazása során az outputként kapott hash-érték bitben megadott méretére utal.

3.3. Proof-of-work

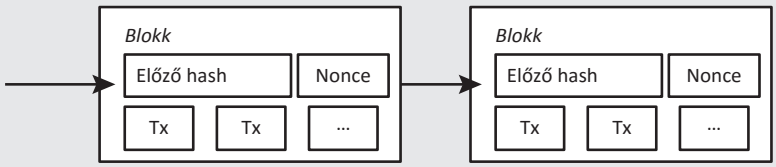
A proof-of-work (magyarul munkabizonyíték) olyan számérték, amelynek előállítása jelentős számítási kapacitást igényel. A bitcoin esetében a bányászok az SHA-algoritmust használják arra, hogy olyan hash-értéket találjanak, amely megfelel a hálózat egészére vonatkozó nehézségi szintnek (*Antonopoulos 2016*).

A proof-of-work végrehajtása a bitcoin esetében lényegében egy fent említett érték keresését foglalja magában, amelyre alkalmazva az SHA–256 algoritmust, olyan hasító értéket kapunk, amely meghatározott számú zéró bittel kezdődik. Az algoritmus lépésszáma – az előírt zéró bitek számának függvényében – exponenciális, a megoldás helyessége azonban egyetlen hash végrehajtásával ellenőrizhető (*Nakamoto 2008*). Ez konkrétan úgy zajlik, hogy a megfelelő blokk megfejtése során a bányász az előző hash mögé ír egy értéket (nonce), majd ezt egészen addig növeli, ameddig az adott blokk így keletkező hash-értéke el nem éri az elvárt zéró bitek számát (a folyamat működését a *3. ábra* illusztrálja). Amennyiben a megfejtés sikeres, az így létrejövő új blokk csak a fenti munka újbóli elvégzésével változtatható meg. Ha időközben újabb blokkok lépnek be a láncba, akkor egy adott blokk megváltoztatása egyúttal a blokkot követő minden újabb blokk megfejtését is megköveteli.

Fontosnak tartjuk megemlíteni, hogy a kriptovaluták esetében a blokklánc-hálózat működtetésében a proof-of-work mellett az – utóbbi időben egyre népszerűbb – ún. proof-of-stake eljárás is használatos. Ebben az esetben a következő blokk előállítója a véletlen és a vagyoni helyzet vagy életkor (stake: magyarul részesedés) kombinációján alapuló kiválasztás eredménye.[7] Ennek az az előnye, hogy felgyorsítja a rendszer működését, és kiküszöböli azt a veszteséget, amely azokat a bányászokat éri, akik ugyan elkezdik a számításokat, de más megelőzi őket, és így nem kapnak bitcoint. Ezzel szemben a proof-of-work alapú kriptovaluták esetében, mint amilyen a bitcoin is, az új blokk előállítása bányászaton, azaz egy számításigényes algoritmus sikeres végrehajtásán alapul.

[6] A fentiekhez lásd bővebben: *Kathi* (*2009*).
[7] https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

3. ábra
A proof-of-work működésének szemléltetése



Forrás: Nakamoto (2008:3) alapján szerkesztve

3.4. A rendszer szereplői, működtetése

A blockchaint működtető rendszer alapvető szereplői a csomópontok (node), amelyek lehetnek bányászok (miner) és felhasználók (user). Erre nagyon sok közvetítő is ráépül, ami lehetővé teszi, hogy a számítástechnikai tudással és technikai háttérrel nem rendelkezők is hozzáférjenek a kriptovalutákhoz. A működés során ahhoz, hogy egy felhasználó bitcoin-tranzakciót tudjon indítani és fogadni, szüksége van egy elektronikus pénztárcára (wallet), ami általában egy ingyenesen letölthető alkalmazás. A tranzakció hitelesítése az ezzel foglalkozó bányászok számítógépén történik, majd az így létrejött új blokkot az egész hálózatnak el kell fogadnia, és az hozzáfűződik az utolsó blokkhoz, megnövelve a teljes blockchain méretét. Ahhoz, hogy valaki részt vegyen a hálózatban, nem szükséges a teljes blockchaint a számítógépén tárolnia. A nemcsak a bitcoinhoz, de más kriptovalutákhoz történő hozzáféréssel rendelkezők száma 2019 első negyedévében mintegy 36 millió felhasználó volt (*Tassev 2019*). Ezzel szemben azoknak a számítógépeknek a száma (full node), amelyek tárolják a teljes bitcoin-blockchaint 9 000 körül volt 2019 augusztusában, és az utóbbi két évben folyamatosan csökkent.[8] Ez a csökkenés érthető, hiszen semmilyen anyagi előnyt nem jelent a teljes bitcoin-blockchain futtatása, miközben a blokkok száma folyamatosan növekszik. A teljes, a generikus blokkot is tartalmazó blockchain mérete 2019 első negyedévére elérte a 226 GB-ot. A teljes csomópontot üzemeltetők jórészt már nem azok az idealisták, akik lázadnak a kormányok és központi bankok által irányított monetáris rendszer ellen, hanem a bányászok és a befektetők. A hitelesítés folyamata, amelyet a bányászok végeznek el, a blockchain méretének növekedésével egyre nagyobb számítási kapacitást és specializált hardvert és szoftvert igényel. Ennek hatására megindult egy koncentrációs folyamat. A legnagyobb szereplő a piacon a kínai BitMain cég, amely, amellett, hogy a legnagyobb specializált hardvergyártó és szoftverfejlesztő, a bitcoin-bányászat több mint 20 százalékát bonyolítja le. 2019 elejére a nagy energiaigényű bányászat jó része, mintegy 70 százaléka Kínában összpontosult, azokra a területekre, ahol a kiépített

[8] https://bitnodes.earn.com/dashboard/?days=730

villamosenergia-termelő kapacitások kihasználatlansága miatt alacsonyak az energiaárak (*Tuwiner 2019*). Az 1 bitcoin kibányászásához szükséges energia- és egyéb költségek 2019-ben Kínában 507 és 4 562 dollár között mozogtak, a villamosenergia árától függően.[9] Ez a helyzet a jövőben alapvetően meg fog változni, miután Kína a kriptovaluta-tőzsdék felszámolása után a bányászatot is nemkívánatos tevékenységként listázta, s minden bizonnyal be fogja tiltani (*Brenda – Alun 2019*).

A kriptovaluták köré ma már egész iparág épült olyan szolgáltatókból, amelyek lehetővé teszik a kriptovaluta vásárlását „valódi" nemzeti fizetőeszköz ellenében, illetve a kereskedést a kriptovalutával a kriptovaluta-tőzsdéken, platformokat nyújtanak a tokenek kibocsátásához és a különböző applikációk kifejlesztéséhez, kézben tartják a befektetők számláit, elemzik az egyes kriptovaluták árfolyamát.

A kriptovaluták regionális elterjedését tekintve az észak-amerikai régióban összpontosul a piaci szereplők 27 százaléka, itt zajlik a tranzakciók 18 százaléka, itt található a pénztárcák 39 százaléka. A második legjelentősebb szereplő Európa, de jelentős növekedés várható Ázsia csendes-óceáni régiójában, különösen Japánban.[10]

4. A bitcoin szerepe és jelentősége a gazdaságban

4.1. A bitcoin mint fizetőeszköz

A bitcoin több mint egy évtizedes fennállása alatt nem az eredetileg neki szánt szerepet töltötte be. A bitcoinnal való fizetés ugyanis nem vált mindennapi gyakorlattá, fizetőeszközként történő elfogadása inkább kuriózumnak számít. Ez nyilvánvalóan a szélsőséges árfolyamingadozásának köszönhető. Teljesen érthető, ha a kereskedők nem hajlandók (sőt nem is tudják) kifejezni egy olyan valutában a termékük értékét, amelynek árfolyama nem stabil.

Említésre érdemes még ebben az összefüggésben, hogy a bitcoin-tranzakciók átfutási ideje más fizetési módokéval (Paypal, hitelkártyák) szemben magas. Ez a rendszer túlterheltsége esetén nagymértékben megnövelheti a tranzakciós díjakat. Ez jelenleg azért fontos szempont, mert a bitcoinnal történő fizetés során – a bank- és hitelkártyás vásárlásokkal szemben – a vevő fizeti a tranzakciós díjat (*Gábor – Kiss 2018*). Ilyen feltételek mellett nem tűnik valószínűnek a közeljövőben annak elterjedése, hogy bitcoinért vásároljunk kisebb értékű cikket (például könyvet vagy kávét).

A bitcoin besorolását a mai napig számos bizonytalanság övezi. Az amerikai határidős árutőzsdét felügyelő szerv (CFTC[11]) áruként határozza meg, az amerikai adóhatóság (IRS[12]) pedig tulajdonjogot megtestesítő eszközként tekint rá. Az amerikai

[9] http://www.chinacryptonews.com/industry/chart-bitcoin-mining-cost-china-cheapest/
[10] https://www.fortunebusinessinsights.com/industry-reports/cryptocurrency-market-100149
[11] Commodity Futures Trading Commission
[12] Internal Revenue Service

értékpapír-felügyelet (SEC[13]) bizonyos esetekben értékpapírként sorolja be (*Chohan 2017*), az Európai Központi Bank pedig konvertibilis decentralizált virtuális valutaként kezeli (*Gábor – Kiss* 2018, *Bánfi 2018*).

Gábor és Kiss (*2018*) kriptovalutákról írt tanulmányukban hangsúlyozzák a kriptovaluta kifejezés félrevezető mivoltát, miszerint ez azt sugallhatja, hogy azok a tradicionális valuták egy alkategóriáját képezik. Véleményük szerint – amellyel abszolút egyetérthetünk – egy teljesen egyedi, új eszközcsoportról van szó.

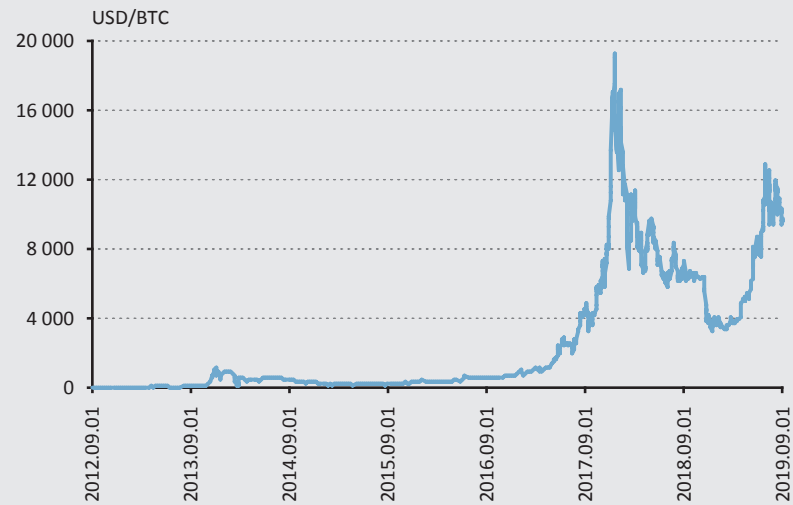
4.2. A bitcoin mint befektetés

Mivel a bitcoin a pénz funkcióját csak korlátozottan képes betölteni,[14] érdemes megvizsgálni, milyen lehetőséget tartogat számunkra, ha befektetési eszközként tekintünk rá. A bitcoin-árfolyam alakulásának vizsgálatához a Yahoo Finance oldalról letöltöttük a dollárban kifejezett napi záró árfolyamait a 2012. szeptember 1. és a 2019. szeptember 1. közötti, hétéves periódusra. Az árfolyam változását a *4. ábra* mutatja.

A vizsgált időszakban a bitcoin napi árfolyama közel 10 dolláros értékről 9 578 dollárra nőtt, azaz nagyjából 960-szorosára emelkedett. Nem szabad azonban megfeledkezni arról, hogy ez a rendkívülinek számító növekedés kiugróan magas volatilitással, azaz rendkívül nagy kockázattal párosult. Az ábrán jól látható, hogy a bitcoin árfolyamának növekedése 2017-ben vett igazán komoly lendületet, amikor a kezdeti kb. 1 000 dolláros értékről 19 340 dolláros ár fölé emelkedett (ami nagyjából 1 900 százalékos (!) éves hozamnak felel meg).[15] Ezt követően az árfolyam erőteljes zuhanásba kezdett, amit a bitcoin-szkeptikusok úgy interpretáltak, hogy „kipukkadt a lufi" (*András 2019*), azonban az árfolyam a 3 000 dollár körüli mélypontot követően ismét emelkedésbe kezdett, és újra 10 000 dollár fölötti értéket ért el.

[13] Securities and Exchange Commission
[14] Ennek a kérdésnek a kifejtésével a tanulmányban nem foglalkozunk. A témához kapcsolódóan *Bánfi* (*2018*) írását érdemes elolvasni.
[15] Valójában a bitcoin eddigi története során a legmagasabb árfolyamértéket, amely 20 089 USD/BTC volt, 2017. december 17-én érte el (https://coinmarketcap.com/currencies/bitcoin/historical-data/).

4. ábra
A bitcoin napi árfolyamának alakulása 2012. szeptember 1. és 2019. szeptember 1. között



Forrás: A Yahoo Finance adatbázisa alapján szerkesztve[16]

A bitcoin befektetési szempontból történő megítélése jövedelmezőségi és kockázati profiljának együttes elemzésén alapulhat. Ebből a célból a rendelkezésre álló napi árfolyamokból először napi hozamokat számítottunk, majd az egyes évekre vonatkozó napi átlaghozamok felhasználásával – a hétéves periódus minden egyes évére vonatkozóan – meghatároztuk az éves effektív hozamot. Kockázati mértékként a hozamok szórását alkalmaztuk. Ebben az esetben először a hozamok idősorának felhasználásával az egyes évekre vonatkozóan napi szórást számoltunk, majd a kapott napi szórás értékeket éves értékekké konvertáltuk. Eredményeinket az *1. táblázatban* foglaljuk össze. A táblázat utolsó sorában a kockázat egységére eső hozamot is feltüntettük.

[16] https://finance.yahoo.com/quote/BTC-USD/history?p=BTC-USD

1. táblázat
A bitcoin éves effektív átlaghozamának és kockázatának alakulása 2012. szeptember 1. és 2019. augusztus 31. között

Periódus	2012/9/1 – 2013/8/31	2013/9/1 – 2014/8/31	2014/9/1 – 2015/8/31	2015/9/1 – 2016/8/31	2016/9/1 – 2017/8/31	2017/9/1 – 2018/8/31	2018/9/1 – 2019/8/31
Éves hozam (%)	2 294,27	11 741,89	–37,82	197,23	968,28	130,23	75,13
Hozam szórása (%)	102,95	390,02	71,53	57,61	71,19	97,9	73,54
Hozam/Kockázat	22,29	30,11	–0,53	3,42	13,60	1,33	1,02

Forrás: A Yahoo Finance adatbázisa alapján számítva

Az *1. táblázatból* kiolvasható, hogy mind a hozamokban, mind a hozzájuk kapcsolódó kockázat értékeiben tükröződik az a szélsőséges ingadozás, amely az árfolyamváltozás profilja alapján már kirajzolódni látszott. Az éves átlaghozam –38 százalék és 11 742 százalék között mozog (az utóbbi érték, amely tulajdonképpen napi 1,3 százalékos átlaghozamnak felel meg, nem elírás!). A hozam szórásával mért éves kockázat ugyanakkor 58 és 390 százalék között mozog. Összehasonlításképpen: ez utóbbi mutató az S&P 500 részvényindex esetében általában évi 10 és 20 százalék közé tehető (lásd *Misik 2018:70*). Az egységnyi kockázatra eső hozam, amely a Sharpe-mutatóhoz hasonlóan a befektetési teljesítmény egyfajta mérőszámának tekinthető,[17] szintén elég széles skálán mozog. Nevezetesen vizsgálatunkban –0,5 és 30 közötti értékeket vesz fel.[18] Míg az előbbi az árfolyamcsökkenési tendenciából következő veszteségre mutat, addig az utóbbi egyedülállóan magas érték a szélsőségesen nagy éves átlaghozam hatását fejezi ki. Ez utóbbit még a hozzá kapcsolódó, rendkívül magas kockázat sem tudta „közömbösíteni" (lásd az *1. táblázat 3. oszlopában* szereplő értékeket).

A fentiek alapján úgy tűnik, hogy a bitcoin sokkal inkább tekinthető a spekuláció, mint egy megalapozott, kiegyensúlyozott hozamot biztosító befektetési stratégia eszközének. A bitcoinba történő befektetés pozitív sajátosságának tudható be azonban, hogy hozama nem korrelál más eszközök (részvények, kötvények, árupiaci termékek, arany) hozamával. Ez a számos szerző által kimutatott tulajdonsága (lásd például *Brière et al. 2015* és *Misik 2018*) a bitcoint alkalmassá teszi arra, hogy egy befektetési portfólióban más eszközök árfolyamcsökkenésének negatív hatását kompenzálja. Egyes tanulmányok rámutattak egy további kedvező sajátosságára is, nevezetesen arra, hogy növelni képes a befektetési portfólió hatékonyságát (*Chen – Pandey 2014*; *Eisl et al. 2015*; *Misik 2018*). Ezen azt kell érteni, hogy a bitcoin portfólióba történő bevonásával – az általunk is kimutatott magas egységnyi kockázatra eső hozama

[17] Pontosabban ez a mutató lehetővé teszi különféle, eltérő jövedelmezőséggel és kockázattal rendelkező befektetések teljesítményének összehasonlítását.
[18] Említésre érdemes, hogy *Misik* (*2018*) elemzésében ez a mutató az S&P 500 részvényindex esetében 1,68-nak bizonyult. A bitcoinra vonatkozóan az általa vizsgált periódusban ugyanakkor 13,07 nagyságú egységnyi kockázatra eső hozam értéket kapott.

következtében – elérhető, hogy az így kapott befektetéskombináció adott kockázati szinthez tartozó hozama növekedjen.

5. A bitcoin elterjedésének korlátai

5.1. Technológiai és energetikai korlátok

A kriptovaluták jövőbeli felhasználását alapvetően korlátozza az Ethereum megalkotója, Buterin által megfogalmazott trilemma: a kriptovaluták esetében nem teljesülhet egyszerre az a hármas követelmény, hogy skálázhatók, decentralizáltak és biztonságosak. A skálázhatóságot megakadályozza a proof-of-work rendszer, ami limitálja a percenkénti tranzakciók számát. A biztonságot ugyan a decentralizáció biztosítaná, de a blokkméret növekedése és az egyre bonyolultabb számítási feladatok megoldása óhatatlanul elősegíti a bányászat, és ahogy az adatok mutatják, a kereskedelem centralizációját is (*Roubini 2018*).

A bitcoin-technológia létrehozásának legfőbb célja a tranzakciók biztonságának növelése volt oly módon, hogy ne kelljen megbízni egy pénzügyi közvetítőben, mint például a bankokban, mert maga a rendszer felépítése védi ki a csalásokat. Ezt a nyílt forráskód és a teljes blockchain visszaellenőrizhetősége biztosítja. A kezdeti időszakban ez talán így is volt, de mióta nem csak a cyber-libertariánusok és programozók szűk köre használja a kriptovalutákat, azóta ez az ellenőrzési lehetőség a 36 millió felhasználó számára illuzórikus. Nem egy – a társadalom, illetve a kormányzat által ellenőrzött – bankban kell megbízni a felhasználóknak, hanem a sokszor a legalitás határán mozgó, és ahogy a csődök és botrányok mutatják, akár pillanatok alatt eltűnő kriptovaluta-kereskedőkben, token-kibocsátókban és DApp-fejlesztőkben. Az Ethereum-platformon futó kódokban például 1 000 soronként 100 hiba található (*Gerard 2017:96*). A kriptovaluták fejlesztése centralizált, maga a „kód a törvény" (*Roubini 2018*), de ez a kód bármikor megváltoztatható, és ebbe az egyszerű felhasználóknak nincs beleszólásuk. Maga a blockchain-rendszer sem védett a támadásoktól, és ha a rendszer 51 százaléka egy kézben összpontosul, akkor lehetőség nyílik arra, hogy visszamenőleg megváltoztassák a blokkokat (*Farivar 2014*).

A bitcoin-tranzakciók végrehajthatósága és gyorsasága attól függ, hogy van-e elég bányász, aki hitelesíti azokat. A bányászat pedig csak akkor éri meg, ha a költségei nem haladják meg a bitcoin adott piaci értékét. A bitcoin bányászatához felhasznált éves átlagos energia 61 TWh[19], ami a teljes magyar éves villamosenergia-felhasználás 130 százaléka (*MAVIR 2019*). A bitcoinnak a magas energiafelhasználáson kívül nincs semmilyen kapcsolata a valóságos gazdasági eseményekkel, hacsak nem vezeti be egy ország a bitcoint nemzeti valutaként és általános fizetőeszközként. Miután erre igen kevés az esély, ezért a bitcoin-bányászat során felhasznált villamosenergia

[19] https://cbeci.org/

elvesztegetett energia, ami a társadalom és a jövő generációi számára kifejezetten károkat okoz. A bitcoin-infrastruktúrához szükséges hardver előállítása, az épületek felépítése, az energiaellátás kiépítése és a bányászat magas energiafelhasználása ugyanis még akkor is nagyon nagy környezeti terheléssel jár, ha a villamosenergiát megújuló forrásokból állítják elő. Nincsen olyan villamosenergia-termelés, ami ne károsítaná a környezetet, ne használna föl környezeti erőforrásokat és ne járulna hozzá a biodiverzitás csökkenéséhez.

5.2. A szabályozási környezet kihívásai

A kriptovaluták szabályozási környezete szinte országonként eltér, s a teljes tiltástól az engedélyezésig terjed. A világ két legnépesebb országa, Kína és India teljesen betiltotta a kriptovaluták használatát. A kínai kormány elkezdte a kriptovalutákat kiszolgáló infrastruktúra és ipar felszámolását is, aminek utolsó lépéseként környezetvédelmi okokra hivatkozva a kriptovaluták bányászatát is a nem kívánatos tevékenységek közé sorolta. Emellett a kínai központi bank saját kriptovaluta (CBDC – Central Bank Digital Currency) kibocsátását tervezi, ami nem egy decentralizált, peer-to-peer technológián alapuló digitális fizetőeszközt jelent, hanem a készpénz teljes kivonását és ezzel a pénzügyi tranzakciók, illetve a a lakosság összes tranzakciója ellenőrzésének a lehetőségét (*Bloomberg 2018*).

A teljes tiltással szemben találjuk azokat az országokat, ahol engedéllyel lehet kriptotőzsdéket üzemeltetni, ilyen például Japán, Dél-Korea vagy Luxemburg. Svájc különleges helyet foglal el, a Zug kantonban található Cripto Valley-ben adókedvezményekkel és egyéb támogatásokkal segítik a kriptovalutával, illetve blockchain-technológiával dolgozó start-upokat, amelyek 3000 embert foglalkoztatnak, és a legnagyobb 50 vállalatnak mintegy 44 milliárd dollár a piaci kapitalizációja (*CVVC 2018*).

A kriptovaluták kereskedelmében legnagyobb szerepet játszó USA és EU szabályozása még kiforratlan, visszatükrözi a bitcoin felhasználásának bizonytalanságait.

Az EU szabályozásának[20] a középpontjában a pénzmosás megakadályozása áll, illetve előírja a kriptotőzsdék és kriptovalutával kapcsolatos szolgáltatások regisztrálását az adott országban. A pénzmosás lehetősége ugyan magától értetődőnek tűnik a kriptovaluták esetében, de a gyakorlatban egyelőre ez a kockázat alacsony, ahogy azt a brit kincstár kockázatértékelése is bemutatja (*HM Treasury 2015*). Az árfolyam változékonysága és bizonytalan likviditása miatt egyelőre nem éri meg pénzmosásra használni a kriptovalutákat. A bitcoin-tranzakciók anonimitása is csak látszólagos. A publikus főkönyvben kitörölhetetlenül megmarad minden tranzakció, s ugyanígy nyomot hagy az interneten is. A szabályzó hatóságok számára azonban nagy kihívás a pénzmosás elméleti lehetősége. A pénzmosás elleni harc klasszikusan a központi-

[20] *5th Anti-Money Laundering Directive* (*2018/1080/COD*)

lag ellenőrzött pénzintézetek ügyfélazonosítására épül. A kriptovaluták pénzmosási kockázatának csökkentése érdekében azonban új elveket és technológiai megoldásokat kell kidolgozni (*Campbell-Verduyn 2018*).

Magyarországon az EU-s direktívák implementálásán felül egyelőre nincs speciális szabályozás a kriptovalutákra. A Pénzügyminisztérium álláspontja szerint a bitcoin nem pénz (*Fintechzone 2018*), míg a Magyar Nemzeti Bank (MNB) felhívja a figyelmet a „fizetésre használható virtuális eszközök" magas kockázatára (*MNB 2018*).

6. Van-e a bitcoinnak jövője?

A bitcoinnal kapcsolatos vitákban gyakran felmerül az a tétel, miszerint a bitcoinnak nincs belső értéke (*Brown 2019*), a kriptovaluta valójában „puszta levegőre" épül. A bitcoin valóban nem használható fel semmilyen más célra, mint például az arany vagy egyéb kincsképző eszköz. A bitcoin ugyanis tiszta információ, és ebben a tekintetben betöltheti annak az abszolút pénznek a szerepét, ami nem kötődik semmilyen fizikai megtestesüléshez (*Simmel 1900*). Azonban ahhoz, hogy egy információ valóban pénz legyen, szükség van arra, hogy azt egy közösség elfogadja. Vagyis a pénzt nem a belső értéke teszi pénzzé, hanem az, ahogy a gazdasági szereplők értéket tulajdonítanak neki, ami így felfogható nem belső, hanem külső értéknek.

Mi az, ami a bitcoin-felhasználókat arra ösztönzi, hogy bitcoint, illetve más kriptovalutákat vásároljanak? Ez elsősorban a bitcoint körülvevő infrastruktúra, a ráépülő másodlagos szolgáltatások, amelyek lehetővé teszik bárki számára, hogy beszálljon, a bitcoinnal és kriptovalutákkal kapcsolatos hírek a médiában, a szabályozás bizonytalansága és a profitkilátások. A bitcoin ma elsősorban a rövid távú spekuláció eszköze, olyan befektetési eszköz, ami mögött a meglehetősen magas energia- és erőforrás-felhasználáson kívül semmilyen konkrét gazdasági folyamat és teljesítmény nincs. A bitcoint vásárlók számára egyetlen dolog fontos, az a hit, hogy a közeli vagy távolabbi jövőben lesznek olyanok, akiknek el tudják adni a kriptovalutájukat. Miután a bitcoin felhasználói nem köthetők egy-egy adott gazdasági közösséghez vagy országhoz, ezért az a potenciális felhasználóréteg, amelyik a jövőben fenntartja a kriptovalutákat, az internet-használók köréből kikerülve akár több milliárdra tehető.

A bitcoin vagy bármelyik decentralizált kriptovaluta általános fizetőeszközként részben a már idézett technológiai és biztonsági problémák miatt sem terjedhet el. Nehéz elképzelni továbbá egy olyan kormányt, amely feladja a pénzkibocsátás és ezzel együtt a monetáris szabályozás lehetőségét. Egy-egy vállalat számára pedig a bitcoin elfogadása óriási kockázattal jár, hiszen az árfolyam volatilitása akár percek alatt felőrölheti a vállalat által alkalmazott árrést.

Nem hanyagolható el a bitcoin hatása a pénzügyi eszközök fejlődésére (*Kerényi – Molnár 2017*). A blokklánc-technológia bizonyos esetekben alkalmas lehet pénzügyi, gazdasági vagy akár társadalmi folyamatok nyomon követésére, a bitcoin által propagált digitális pénz eszméje pedig olyan új pénzügyi innovációkat generálhat, mint a Facebook által bevezetni kívánt, ám eddig meglehetősen nagy ellenállásba ütköző Libra, vagy a Wal-Mart által szabadalomra benyújtott dollár alapú digitális fizetőeszköz.

A bitcoin nem töltötte be azt a szerepet, amelyet Nakamoto szánt neki. Ennek az az oka, hogy az általa kifejlesztett szoftver-architektúra valójában technikai megoldást kínál fel bizonyos problémákra, de nem veszi figyelembe a pénzügyi tranzakciók mögötti gazdasági folyamatokat. A címben felvetett kérdésre válaszolva leszögezhetjük, hogy a bitcoin a mostani formájában nem alkalmas arra, hogy általánosan elfogadott fizetőeszközzé váljon. A blockchain-technológiába beépített biztonsági rendszer lelassítja a tranzakciók átfutási idejét, s így nem veheti fel a versenyt az elterjedt pénzügy-technológiai megoldásokkal. A bitcoin-iparág szolgáltató cégei (a tőzsdék, pénztárca-szolgáltatók) a legalitás határán mozognak, bármelyik pillanatban eltűnhetnek, vagy állami beavatkozással megszüntethetik őket. A legtöbb országban nincs megfelelő szabályozás a tevékenységüket illetően, így a felhasználók, illetve befektetők semmilyen védelemre nem számíthatnak. A bitcoin több mint egy évtizedes története azt mutatja, hogy bár széleskörű elterjedése nem történt meg, de egy szűk piaci szegmensben kockázatos befektetési eszközként fennmaradhat.

Felhasznált irodalom

András Bence (2019): *Hát nem arról volt szó, hogy összeomlik a bitcoin? Portfolio.hu – Online gazdasági újság*, augusztus 5. https://www.portfolio.hu/prof/20190805/hat-nem-arrol-volt-szo-hogy-osszeomlik-a-bitcoin-333275. Letöltés ideje: 2019. augusztus 5.

Antonopoulos, A.M. (2016): *Mastering Bitcoin* (ford. Bitcoin fejlesztőknek). https://bitcoinbook.info/wp-content/translations/hu/book.pdf. Letöltés ideje: 2019. július 14.

Bánfi Ziád (2018): *A bitcoinról pénzelméleti szempontból*. Gazdaság és Pénzügy, 5(1): 2–30.

Bloomberg (2018): *China's Plan to Sideline Bitcoin*. https://www.bloomberg.com/news/articles/2018-12-13/china-s-plan-to-sideline-bitcoin. Letöltés ideje: 2019. augusztus 5.

Brenda, G. – Alun, J. (2019): *China wants to ban bitcoin mining*. https://www.reuters.com/article/us-china-cryptocurrency/china-wants-to-ban-bitcoin-mining-idUSKCN1RL0C4. Letöltés ideje: 2019. augusztus 5.

Brière, M. – Oosterlinck, K. – Szafarz, A. (2015): *Virtual currency, tangible return: Portfolio diversification with bitcoin*. Journal of Asset Management, 16(6): 365–373. https://doi.org/10.1057/jam.2015.5

Brown, C. (2019): *Bitcoin Has No Intrinsic Value — and That's Great*. (n.d.). https://medium.com/coinmonks/bitcoin-has-no-intrinsic-value-and-thats-great-e6994adbfe0f. Letöltés ideje: 2019. augusztus 5.

Buttyán Levente – Vajda István (2012): *Kriptográfia és alkalmazásai*. Typotex.

Campbell-Verduyn, M. (2018): *Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance.* Crime, Law and Social Change, 69(2): 283–305. https://doi.org/10.1007/s10611-017-9756-5

Chen, W.Y. – Pandey, V. K. (2014): *The value of bitcoin in enhancing the efficiency of an investor's portfolio*. Journal of Financial Planning, 27(9): 44–52.

Chohan, U. W. (2017): *Assessing the Differences in Bitcoin & Other Cryptocurrency Legality across National Jurisdictions*. School of Business and Economics, University of New South Wales, Canberra Discussion Paper. https://doi.org/10.2139/ssrn.3042248

CVVC (2018): *The Crypto Valley's Top 50 Technology Partner. The Blockchain Industry in Switzerland & Liechtenstein analyzed and visualized.* https://www.coinpro.ch/wp-content/uploads/2019/07/CVVC-Top50-H1-2019.pdf. Letöltve: 2020. február 3.

Eisl, A. – Gasser, S. – Weinmayer, K. (2015): *Caveat emptor: Does bitcoin improve portfolio diversification?* SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2408997

Emsley, J. (2019): *Alleged Bitcoin Ponzi scheme Plus Token could be liquidating billions of dollars in stolen crypto, says VC*. https://cryptoslate.com/alleged-bitcoin-ponzi-scheme-plus-token-could-be-liquidating-billions-of-dollars-in-stolen-crypto-says-vc/. Letöltés ideje: 2019. augusztus 24.

Farivar, C. (2014): *Bitcoin pool GHash.io commits to 40% hashrate limit after its 51% breach*. Ars Technica, 16 July.

Fintechzone (2018): *A Pénzügyminisztérium válasza a kriptovaluták szabályozásával kapcsolatban*. https://fintechzone.hu/a-penzugyminiszterium-valasza-a-kriptovalutak-szabalyozasaval-kapcsolatban/. Letöltés ideje: 2019. augusztus 24.

Gábor Tamás – Kiss Gábor Dávid (2018): *Bevezetés a kriptovaluták világába*. Gazdaság és Pénzügy, 5(1): 31–65.

Gerard, D. (2017): *Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum & Smart Contracts*. CreateSpace Independent Publishing Platform.

Golumbia, D. (2016): *The Politics of Bitcoin Software as Right-Wing Extremism*. University of Minnesota Press.

HM Treasury (2015): *UK national risk assessment of money laundering and terrorist financing*. Her Majesty's Treasury and Home Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf. Letöltés ideje: 2020. január 12.

Kathi Ferenc (2009): *Hash függvények*. Szakdolgozat, Debreceni Egyetem Informatikai Kar. https://dea.lib.unideb.hu/dea/bitstream/handle/2437/90313/Szakdolgozat_KathiFerenc.pdf;jsessionid=B66004CEDC6B420308BC16C17D65FFA1?sequence=1. Letöltés ideje: 2019. december 12.

Kerényi Ádám – Molnár Júlia (2017): *A FinTech-jelenség hatása – Radikális változás zajlik a pénzügyi szektorban?* Hitelintézeti Szemle, 16(3): 32–50. http://doi.org/10.25201/HSZ.16.3.3250

Levin, M.R. (2009): *Liberty and Tyranny: A Conservative Manifesto*. New York: Simon and Schuster.

MAVIR (2019): *A teljes bruttó energiafelhasználás megoszlása*. http://www.mavir.hu/documents/10258/229275463/Előzetes+Termelésmegoszlás++2018+MavirHonlapra+-HU+20190131.pdf. Letöltés ideje: 2019. július 12.

Misik Sándor (2018): *A bitcoin a portfólióelmélet tükrében*. *Gazdaság és Pénzügy*, *5*(1), 66–73.

MNB (2018): *Az MNB kockázatosnak tartja a fizetésre használható virtuális eszközöket, például a Bitcoint*. Sajtóközlemény, Magyar Nemzeti Bank. https://www.mnb.hu/archivum/Felugyelet/root/fooldal/topmenu/sajto/sajtokozlemenyek/bitcoin_kozl. Letöltés ideje: 2019. július 12.

Mullins, E.C. (1992): *The World Order: Our Secret Rulers*. Published by Ezra Pound Institute of Civilization, Staunton, VA.

Nakamoto, S. (2008): *Bitcoin: A Peer-to-Peer Electronic Cash System*. White paper. 1–9. https://bitcoin.org/bitcoin.pdf. Letöltés ideje: 2019. április 15.

Roubini, N. (2018): *Crypto is the Mother of All Scams and (Now Busted) Bubbles. While Blockchain Is The Most Over-Hyped Technology Ever, No Better than a Spreadsheet/Database*. https://www.banking.senate.gov/imo/media/doc/Roubini%20Testimony%2010-11-18.pdf. Letöltés ideje: 2019. július 12.

Rothbard, M. (2002): *A History of Money and Banking in the United States: The Colonial Era to World War II*. Auburn, Ala.: Mises Institute.

Simmel, G. (1900): *Philosophie des Geldes*. Leipzig: Duncker&Humboldt Verlag.

Tassev, L. (2019): *The Number of Cryptocurrency Wallet Users Keeps Rising*. https://news.bitcoin.com/the-number-of-cryptocurrency-wallet-users-keeps-rising/. Letöltés ideje: 2019. augusztus 14.

Tuwiner, J. (2019): *Bitcoin Mining in China*. https://www.buybitcoinworldwide.com/mining/china/. Letöltés ideje: 2019. augusztus 14.