

BEVEZETÉS A KRIPTOVALUTÁK VILÁGÁBA¹

Gábor Tamás – Kiss Gábor Dávid

Míg a 2010-es évek első felében a kriptopénzek túlnyomórészt csupán az informatika világában és azon belül is a programozásban jártas innovátorok érdeklődését keltették fel, addig a kriptovaluták térhódítása napjainkra megkerülhetetlen témává vált mind a kutatók, mind a tőkepiaci résztvevők és a szabályozó hatóságok körében.

Annak ellenére, hogy a média növekvő érdeklődéssel foglalkozik a digitális pénzek, azon belül a bitcoin napjainkban tapasztalt térhódításával és lehetséges buborékjelenségével, a legtöbb közgazdaságtanban és pénzügytechnikai kérdésekben jártas szakember továbbra is kevés ismerettel rendelkezik e sokak számára a jövő monetáris politikáját is akár átalakítani képes, izgalmas, belső értékkel nem rendelkező, informatikai kódok mögött rejtőzködő, rejtelmes valutáról.

Cikkünk során átfogó képet kívánunk adni a kriptovaluták működéséről. Bemutatjuk a blokklánc-technológián alapuló decentralizált applikációk jelentőségét, azon keresztül pedig a Bitcoin elszámolási rendszer működését, kiemelt figyelmet fordítva a bitcoin körül kialakult mániára.²

Az átfogó informatikai ismereteket igénylő, mögöttes technológiát csak olyan mértékig mutatjuk be az olvasónak, amennyi ahhoz szükséges, hogy a kriptovaluta-rendszerek pénzügyi-gazdasági beágyazottsága értelmet nyerjen.

Párhuzamot vonunk a kriptoeszközök árfolyam-emelkedése és néhány historikus árfolyambuborék között, majd szó lesz a valós belső értékkel nem rendelkező bitcoin értékeléséről, valamint használatának limitációjáról. Végezetül pedig a kriptoeszközökről mint új eszközcsoportról értekezünk, amelynek keretében a cikk utolsó fejezetében GARCH-, GJR-GARCH-, TARCH- és APARCH-modellek segítségével bizonyítjuk be, hogy a bitcoin amerikai dollárral szembeni árfolyama független minden más pénz- és tőkepiaci eszköz árfolyamától, ami akár alkalmassá is teheti a bitcoin portfólión belüli diverzifikációs célok alkalmazására.

Jel-kódok: O30, E49, E59, C22

Kulcsszavak: bitcoin, ethereum, kripto, blokklánc, decentralizált hálózat

1 A tanulmányban elhangzó megállapítások a szerzők saját véleményét és nézetét tükrözik. Azok semmi esetre sem interpretálhatók befektetési tanácsként.

A szerzők köszönetet mondanak Vidák Gábor kriptopiaci szakértőnek a tanulmány lektorálása során tett hasznos észrevételeiért.

2 A nagy-, illetve kisbetűvel írt Bitcoin és bitcoin közötti különbségről l. BÁNYI ZIÁD (2018) e számunkban megjelent cikkét: *A bitcoinről pénzügyi szempontból (Gazdaság és Pénzügy, 5. évf. 1. szám, 2–30. o.)*.

1. BEVEZETÉS

A kriptoeszközök piacáról talán a legkurrensebb és legpontosabb képet adó CoinMarketCap internetes portál adatbázisa szerint 1542 különböző kriptoeszközt jegyeztek a cikk megírása idején. E digitális eszközök túlnyomó részéről valószínűleg nem is hallott az olvasók többsége. Egy részük valutafunkciót tölt be, ezek a kriptovaluták (például: Bitcoin, Litecoin, Monero, Dash, ZCash), más részük infrastruktúrát szolgáltat a többi blokkláncalapon működő alkalmazás részére, ezek az úgynevezett „utility” kriptoeszközök (például az Ethereum, Filecoin), végül pedig az utolsó csoportba a szolgáltatásokat nyújtó kriptoeszközök sorolhatóak („application” kriptoeszközök, például Augur, ox, Steem). Habár nincs két teljesen egyforma „kripto”, egy dolog azonban közös bennük: a technológia. Mielőtt a kriptográfián alapuló valutákkal és azon belül is a bitcoinnal foglalkoznánk részletesen, szükséges a *decentralizált alkalmazások* működésének ismertetése. Ennek megértésén keresztül foghatjuk fel igazán a kriptopénzek mögött álló koncepciót.

Annak ellenére, hogy a közelmúlt híradásai főként a kriptoeszközök – elsősorban a bitcoin – árfolyammozgásaira fókuszáltak, a technológia eredendő célja nem pusztán valutafunkció (fizetési, illetőleg forgalmi eszköz) betöltése. Ennek szemléltetéséhez vegyük számba az eszközcsoportok funkcióit. A vállalati kötvény vállalatokat, a kormányzati kötvény kormányzati és állami szervezeteket, a jelzálogkötvény pedig ingatlantulajdonosokat szolgál. Ebben a tekintetben a kriptoeszközök valójában decentralizált alkalmazások futtatását teszik lehetővé.

A decentralizált applikációk teljesen újfajta megközelítést vezettek be az elektronikus szolgáltatások világába. Ezzel a merőben új megoldással létrehozhatunk, finanszírozhatunk és működtethetünk fentről lefelé megvalósuló decentralizált, azaz központi fél nélkül működő szolgáltatásokat. Mindez pedig radikálisan különbözik azoktól a standardoktól, amit az eddigiek során megismerhettünk.

Képzeld el a következőt: egy esőerdőben nőttünk fel, és valaki hoz nekünk egy kaktuszt, azt állítva, hogy az egy fa. Hogyan reagálnánk? Valószínűleg mosolyognánk, és megkérdőjeleznénk az állítást, hiszen mi értelme ennyi vizet tárolni a tömzsi, tüskés húsa alatt ott, ahol korlátlan vízkészlet áll rendelkezésre?

Minden bizonnyal hasonló lehet az emberek reakciója a decentralizált applikációk kapcsán.

1.1. A decentralizált alkalmazás

Decentralizált alkalmazás révén függetleníteni tudjuk a kínált szolgáltatást bármiféle központi – közvetítő – féltől, avagy szervertől.

2008 novembere volt minden idők legsúlyosabb pénzügyi válságának és bankpánikjának talán legkritikusabb időszaka. Ekkoriban, egy *Satoshi Nakamoto*³ (ál) nevet használó szerző publikált egy javaslatot⁴ a Cryptography levelezőlistán, amely egy forradalmian új megoldást mutatott be a központi elszámoló felek által működtetett fizetési rendszerekhez képest. Egy olyan rendszert dolgozott ki, ahol a fizetések lebonyolításához nincs szükség központi bankokra, klíringházakra avagy a PayPalhoz hasonló, online közvetítőkre.⁵ Ez volt minden idők legelső kriptográfát alkalmazó, decentralizált koncepciója, amelynek legfőbb célja a valós idejű fizetések lebonyolítása mellett a központi féltől független, megosztott nyilvántartási könyv létrehozása volt.

A mindösszesen kilenc oldalból álló publikáció nem meglepő módon a „Bitcoin” címet kapta. Satoshi arra kereste a választ, hogy miként hozható létre egy olyan hiteles elszámolási rendszer, amelyből a klasszikus tankönyvekben ismertetett központi felet – amely nyomon követi, teljesíti, elszámolja a pénzforgalmat, valamint számlát vezet szereplőknek – kiemeli. A legnagyobb kihívást az jelentette, hogy megoldást kellett találnia arra a problémára, hogy egy adott pénzegységet ne lehessen többször elkölteni. Az adat ugyanis nem kézzelfogható, azaz replikálható mindenféle korlátozás nélkül. Satoshi legnagyobb érdeme az volt, hogy a fenti kihívás áthidalásának a kidolgozása közben megoldást talált az úgynevezett *bizánci tábornokok problémájára* (*Byzantine generals problem*). Az elosztott rendszereknél ugyanis, mint amilyen a Bitcoin hálózata, az adathitelesítés és időkezelés kritikus a rendszer integritása és stabilitása szempontjából. A Bitcoin protokollja a közmegegyezés (*konszenzus*) kialakításának egyik legnagyobb kihívására ad megoldást: arra, hogy egy nem megbízható hálózaton miképpen lehetséges hiteles információt továbbítani.⁶

3 Személyét mind a mai napig találgatások övezik. Sokak szerint ez egy álnév, sőt vannak, akik szerint egy szűk csoport állhat a Bitcoin-protokoll alapjainak lefektetése mögött. A Satoshi szó annyit tesz japánul, mint „tisztán gondolkodó, gyors eszű, bölcs”. A „naka” közvetítőt, kapcsolatot vagy valaminek a belsejét jelenti, míg a „moto”-t eredetként vagy alapzatként fordíthatnánk. Ezek a kifejezések remekül leírják azt a személyt, aki mozgalmat indított egy jól kidolgozott algoritmus megírásával.

4 Bitcoin: A Peer-to-Peer Electronic Cash System – Satoshi Nakamoto, satoshin@gmx.com, www.bitcoin.org.

5 Satoshi nem titkolt szándéka e nyílt és decentralizált virtuális hálózat létrehozásával az volt, hogy tehermentesítse – esetleg kiváltsa? – a jelenlegi bankrendszerünket. A Bitcoin-protokoll első, o-díknak hivatkozott blokkjában a következő üzenetet rejtette el: „The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.” Ezzel a sorral a *The Times*ban 2009. január 3-án megjelent cikke utalt, amelyben a brit pénzügyminiszter kilátásba helyezett egy második bankmentő akciót. Mindebből arra lehet következtetni, hogy Satoshinak alapvetően a központi beavatkozással és a mentőakciók aszimmetrikus mivoltával volt problémája: azzal, hogy ha a bankrendszer jól működik, a tekintélyes profitot bezsebeli; turbulenciák esetén azonban az adófizetők pénzéből mentik meg. E problémák megoldására tervezte meg a Bitcoint (https://en.bitcoin.it/wiki/Genesis_block).

6 A bizánci tábornokok problémájáról. Bővebben a https://en.wikipedia.org/wiki/Byzantine_fault_tolerance cím alatt, illetőleg FODOR D. – SPEISER F. (2014): Autóipari beágyazott rendszerek című tanulmányában.

Az online elszámolási rendszerek működéséhez a gördülékeny adattovábbításon túl szükség van az adatok érvényesítésére, azaz *validálására*. Satoshi egy peer-to-peer – független és egyenrangú szereplők közötti – hálózatot képzelt el, amely teljesen nyitott, és mindenki számára hozzáférhető. Az utalást indító fél egyszerűen bejelenti tranzakciós szándékát a nyilvános hálózat minden szereplőjének, megjelölve többek között a küldeni kívánt összeget, valamint a saját és a címzett publikus címét. A tranzakciót a pénzügyi összeghez tartozó, egyedi kulcsával is ellátja, úgymond aláírja⁷ azt – bizonyítva rendelkezési jogát az adott pénzügyi összeg fölött. Már csak az szükséges, hogy ugyanazt az összeget egynél több alkalommal ne lehessen elkölteni. Napjaink központosított elszámolási rendszereinél ezt a funkciót egy központi szereplő tölti be. Mi történik azonban akkor, ha nincs egy előre deklarált központi fél? Satoshi forradalmi javaslata a tranzakciót hitelesítő felek megversenyeztetésében áll. Habár kétségtelen, hogy a tranzakció validálásához szükséges egy érvényesítést végrehajtó fél létezése, ebből azonban nem kell annak következnie, hogy e félnek mindig ugyanannak a szereplőnek kell lennie. Hasonlóan a piacgazdaságban megfigyelt versengéshez, itt is versenyeztetni kell a résztvevőket. Ehhez azonban szükség van még egy további komponensre. Egy olyan ösztönző eszközre, amely a tranzakciót hitelesítő felet jutalmazza. Ezt az eszközt nevezte Satoshi egész egyszerűen bitcoinnak. A hitelesítési folyamatban résztvevő szereplőket pedig – a hajdani aranyásók analógiájára – „bányászoknak”. Azzal pedig, hogy a forráskódot publikussá tette mindenki számára, a piacgazdasághoz hasonló szabad belépést biztosított.

De hogy is kell valójában elképzelni ezt a „versenyt”?

Satoshi erre is tett javaslatot. Képzeljünk el egy véletlenszerűen generált, hosszú számsort – ezt hashnek nevezik⁸ –, amely rendkívül nehezen fejthető meg. Annyira nehezen, hogy annak megfejtése érdekében több ezer szuperszámítógép erőforrását kell bevetni.

7 A tranzakció aláírása során úgynevezett Elliptic Curve Digital Signature Algorithm (ECDSA) típusú algoritmust használnak. Az ECDSA az aszimmetrikus titkosítási eljárások egy típusa, amely során az aláírás hitelességének ellenőrizhetősége rendkívül egyszerű, azonban annak feltörése rendkívül bonyolult és óriási számítási kapacitást igényelő feladat (bővebben: https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm).

8 A hash függvények (kiejtése: hes, magyarul hasítófüggvények) olyan informatikában használt eljárások, amelyekkel bármilyen hosszúságú adatot adott hosszúságra képezhetünk le. Az így kapott véges adat neve hash/hasító érték. Ezek az algoritmusok az 1980-as évek legvégén az elektronikus aláírás megjelenésével váltak szükségessé. Leggyakrabban használt és legközismertebb hash algoritmus az SHA (Secure Hash Algorithm) titkosítás (forrás: Wikipedia).

Az olvasónak bizonyára megfordulhat a kérdés a fejében, hogy miért van szükség erre a bonyolultnak tűnő és valódi költségekkel⁹ járó versenyre pusztán azért, hogy valaki a számsor megfejtésén keresztül hitelesíteni tudjon egy tranzakciót.

A tranzakció validálásáért, azaz a digitális időbélyegzővel való ellátásáért folytatott versenyt az egyéni – jutalmazási sémán keresztül – haszonszerzés vezérli. A munkabizonyíték-rendszer (*proof-of-work*)¹⁰ koncepció alapuló verseny teszi lehetővé a rendszerszintű stabilitást és az átutalások biztonságos könyvelését. E folyamat keretében a „bányászok” megvizsgálják minden egyes függőben lévő tranzakciót, kiiktatják a felhasználók azon törekvéseit, hogy kétszer költsék el ugyanazt az összeget, biztosítják az összes szabály betartását, valamint végrehajtják az érvényesíthető tranzakciókat – azaz a bitcoin esetében elvégzik az átutalásokat. Mindezt központi elszámoló fél nélkül teszik.

A proof-of-work koncepció működése kapcsán idézzük fel *Adam Smith* gondolatait: „*Ebédünket nem a mészáros, a sörfőző vagy a pék jóakarától várjuk, hanem attól, hogy ezek saját érdekeiket tartják szem előtt.*” A kriptobányász erőforrásait pusztán önös gazdasági érdekéből csoportosítja át a megfelelő hardware beszerzésére, mindazonáltal ezen egyéni érdek teszi lehetővé a rendszer egészének működését és stabilitását. A kriptovaluta – és a mögötte rejlő konszenzuson alapuló koncepció – ilyenformán nem más, mondhatni, mint a Bitcoin „láthatatlan keze”.

A bányászok az erőforrásaik biztosításáért cserébe kapott kriptopénz egy részét eladják keményvalutáért a nyílt piacon¹¹, hogy ebből fedezni tudják a hardverek működésével kapcsolatban felmerült költségeiket (elektromos áram, tárolás/ bérlet, hűtés). Ami ezen az összegben felül marad, nem más, mint a profit.

9 A kriptovaluta-bányászathoz igen korszerű és bonyolult számítási műveletek végrehajtására képes számítógépekre – erős processzorra és/vagy még erősebb videokártyákra (GPU-kra) van szükség. Az ilyen nagy kapacitású gépek jelentős áramfelvétellel működnek. Egy „bányász célra” összeállított konfiguráció belépési ára kb. ~600 000-800 000 Ft, áramfogyasztásának havi költsége pedig minimum 15 000-20 000 Ft.

A bitcoinbányászásra ma már célhardvert használnak. Az ún. ASIC típusú bányászgépek jelenlegi bekerülési ára 4-5000 dollárra is rúghat.

10 A bányászok azon versengenek, hogy kinek sikerül először a pénzügyi tranzakciókat tartalmazó adatblokkot megfejteni, és így azt a meglévő blokkláncba (Blockchain) beépíteni. Ehhez egy kellően nehéz matematikai problémát oldanak meg, amellyel igazolják a teljesítést és a jóhiszeműséget. Minél több bányász van a hálózaton, annál nehezebbé és időigényesebbé válik ennek a matematikai problémának a megfejtése. De ez mindig csak éppen annyira nehéz, hogy körülbelül átlagosan 10 percenként érkezhessen egy-egy megfejtés. Ez kettős célt szolgál: ezen keresztül meghatározódik, hogy ki kapja meg a megfejtésért járó jutalmat, másrészt pedig segíti kiszűrni azokat, akik meg akarják hamisítani a könyvelést.

11 A különböző kriptopénzek, valamint kriptopénzek és fiat valuták közötti adásvétel lebonyolítása érdekében speciális kriptotőzsdék jöttek létre. A <http://cryptocoincharts.info> szerint a cikk írásakor több mint 130 tőzsde működött, napi 26 milliárd USD forgalommal (a kriptopénzek egymás közötti forgalma is megjelenik ebben az összegben). Ezek közül talán a legnagyobbak és legismertebbek a Bitfinex, Bithumb, Poloniex, Bitstamp, Bitrex és a Coinbase GDAX.

Összefoglalva: tehát az a jutalomként funkcionáló eszköz, amelyet a központi elszámoló fél szükségességét helyettesíteni képes, egymással versengő tranzakciókat hitelesítő szereplők piactere hívott életre, nem más, mint az az eszköz, amely forgalomba kerülve, digitális pénzügyi értéket hordozó elektronikus fizetési eszközzé, azaz kriptovalutává válik.

1.1.1. *Decentralizált szolgáltatás: nem új a nap alatt?*

A decentralizált alkalmazás valójában a legtöbb esetben már létező szolgáltatás nyújtását és igénybevételét teszi lehetővé. Azonban mindezt központi üzemeltető/szolgáltató fél nélkül képes biztosítani.

A *Filecoin*¹², a *Storj* vagy éppen a *Sia* példának okáért lehetővé teszi, hogy peer-to-peer hálózat számítógépein tároljuk adatainkat központi szerver(ek) igénybevétele nélkül. Azok a felhasználók, akik nagy adatfájlokat biztonságos módon kívánnak tárolni a felhőben, nem a *Dropbox*-nak vagy éppen a *Box.com*-nak fizetnek majd tárolási díjat, hanem a peer-to-peer hálózat önkéntes szabad tárhellyel rendelkező „bányászainak”, akik szabad tárhelyük rendelkezésre bocsátásának jutalmaként *Filecoin*-t kapnak cserébe. A hálózat *tokene* – amely a *filecoin* nevet viseli – a tőzsdére vezetést követően szabadon eladható más kriptovalutáért vagy keményvalutáért cserébe.

Mindazonáltal sem a digitális adattárolási megoldások, sem az elektronikus fizetési rendszerek nem jelentenek újat. A forradalmi újítás abban áll, hogy a decentralizált platformok esetében nincs szükség központi vállalatra. Mindezt pedig a szerveződéseknek egy teljesen új formáját hívja életre.

A bitcoin riválisának tartott kriptoeszközről, az Ethereumról is ejtenünk kell pár szót, különösen az elmúlt időszakban tapasztalt, hihetetlennek tűnő, 10 000%-ot meghaladó árfolyam-emelkedés kapcsán. Az Ethereum egy olyan blokkláncon¹³ alapuló, decentralizált hálózat, amely más decentralizált alkalmazások számára teremt futtatási és működési környezetet. Éppen ezért szerepe és dominanciája kimagasló a kriptoeszközök világában. Az Ethereum-protokoll is – a Bitcoinhoz hasonlóan – ösztönzőrendszere révén von be számítási kapacitást a tranzakciók hitelesítésére. A bányászok az erőforrásaik rendelkezésre bocsátásáért pedig ethert kapnak cserébe. Az Ethereum rendkívüli újítása és vonzereje abban áll, hogy egy működési keretrendszert hozott létre a különféle decentralizált alkalmazások részére. Előre specifikált, programozott okos szerződések (*smart contract*) futtatását teszi lehetővé akként, hogy e szerződések teljesítését sem leállás, sem

12 A Filecoin projektet az első blockchain alapú felhő-adattárolási lehetőséget nyújtó kezdeményezések között jegyzik. A 2017 augusztusában lebonyolított nyilvános token (digitális zseton) kibocsátás (ICO, Initial Coin Offering) során alig egy óra alatt több mint 200 millió dollárt gyűjtöttek össze intézményes befektetőktől a koncepció finanszírozására.

13 A blokklánc definícióját lásd lejjebb, keretben.

cenzára, sem csalás vagy bármely harmadik fél által okozott manipuláció nem veszélyeztetni. E pont kapcsán azonban meg kell jegyeznünk, hogy a tranzakciók visszafordíthatatlanságának előnye egyben a hátránya, veszélye is. Ha ugyanis a programozó hibásan írja meg az Ethereum hálózatán futó programot, akkor annak lefutása óriási veszteséget eredményezhet – hiszen nincs lehetőség az átutalt pénzeszegek visszakönyvelésére!¹⁴

Napjaink decentralizált alkalmazásai a legtöbb tekintetben azonban nem tudnak versenybe szállni a mindennapjaink hagyományos megoldásaival. Ha összehasonlítjuk példának okáért a Bitcoint a PayPallal, vagy éppen a Filecoin szolgáltatását a Dropboxszal, könnyedén arra a következtetésre juthatunk, hogy a decentralizált szolgáltatások sokszor lassabbak, drágábbak, kevésbé skálázhatók, felhasználói élményben kevesebbet nyújtanak és volatilitásuk miatt jelentős bizonytalanságfaktort hordoznak magukban. Mindezek ellenére egy dologban teljesen új tulajdonsággal rendelkeznek: cenzúrarezisztensek.

A cenzúrarezisztencia azt jelenti, hogy a szolgáltatások mindenki számára korlátok nélkül bármikor elérhetők, az így lebonyolított tranzakciók pedig megállíthatatlanok és megmásíthatatlanok. Senki nem gátolhat meg bennünket abban, hogy bárkinek a címére bitcoint transzferáljunk. De épp úgy akadálymentesen futtathatunk le egy kódot (okos szerződést) az Ethereum hálózatán, avagy szabadon tárolhatunk adatot a Filecoin platformján. Mindaddig, ameddig rendelkezésünkre áll internetkapcsolat, és hajlandóak vagyunk a tranzakciós díjat megfizetni – természetesen az adott rendszer kriptovalutájában denominálva –, szabad akaratunk szerint cselekedhetünk, külső cenzúrától vagy bármilyen szabályozástól mentesen.

De vajon mely csoport(ok) számára fogadható el ez a trade-off¹⁵ jelenleg?

Azoknak, akik olyan régiókban élnek, ahol bizonyos szolgáltatások nem, vagy korlátozottan elérhetők, illetőleg akik a hatóságok vagy bármely harmadik fél látómezején kívül szeretnének maradni. Ebbe a körbe sorolhatók azok a fejlődő és feltörekvő országok, ahol a hiperinfláció miatt a belföldi deviza napról napra kevesebbet ér (pl. Venezuela), ahol a pénzügyi infrastruktúra és tőkeszabályozói rendszer kettőse nem teszi lehetővé a tőke szabad(abb), határon átívelő áramlását, avagy azok az érdekelték, akik a szürke- és a feketegazdaságban tevékenykednek.

Mindehhez azonban szükséges hozzátenni, hogy a technológiával kapcsolatban tapasztalt nehézségek a várakozások szerint idővel csökkenni fognak a protokoll

14 2016-ban a DAO (decentralized autonomous organization) projekt kapcsán történt egy hasonló incidens, melynek során több tíz millió dollár értékben 3,6 millió ethert tulajdonítottak el a rosszul átgondolt kód (szerződés) eredményeként (bővebben: <https://www.coindesk.com/understanding-dao-hack-journalists/>).

15 Megjegyezendő azonban, hogy azoknál, akik pusztán spekulációs céllal vásárolnak kriptopénzt, és nem a technológiában rejlő előnyöket kívánják kihasználni, nem beszélünk trade-offról.

folyamatos fejlesztésének köszönhetően, amely majd egyre szélesebb körben teszi lehetővé mindennapi használatukat.

Mi az a blockchain?

A blockchain (magyarul blokklánc) egy megosztott nyilvántartási könyv, lényegében egy tranzakciókat tartalmazó, decentralizált adatbázis, amely több száz, több ezer számítógépen van nyilvántartva. Az adatok blokkokra vannak tagolva, amelyeket egyedi azonosítóval: egy időbélyeggel és digitális aláírással is ellátnak. Az újabb blokkok úgy jönnek létre, hogy egy megelőző blokkhoz kriptografikus eljárással egy újabb blokkot kapcsolnak, amelyet a rendszerben lévő többi szereplő hitelesít. A hitelesítés után a láncban résztvevők adatbázisai megmásíthatatlan és visszavonhatatlan módon frissülnek

2. BITCOINMÁNIA

A *Fortune* magazin 2017. 12. 21-i számának vezércikkében szólaltatta meg a Nobel-díjas közgazdász, *Robert Shillert*, aki a 2007–2008-as amerikai másodlagos jelzálogpiaci válság kirobbanása előtt több alkalommal is felhívta a figyelmet az amerikai lakáspiac túlfűtöttségére. Ezúttal a bitcoin és kriptopénzek piacán tapasztalható áremelkedésről fejtette ki véleményét. Szerinte „úgy tűnik, újra itt a dotkombuborék vagy éppen az ingatlanpiaci lufi” (*Hackett–Wieczner, 2017*).

A professzor kijelentésénél azonban érdemes megállni egy pillanatra. Jelentős különbség van ugyanis az általa említett két pénzügyi válság között. Míg az utóbbi egy globalizálódó, több ezer milliárd dollár vagyontömeget elégető pénzügyi világválságot és gazdasági depressziót eredményezett, soha nem látott volumenű TBTF-intézményeket¹⁶ kiszegítő, állami mentőakciókat vonva magával, addig az ezredforduló során tapasztalt dotkombuboréknak jelentős technológiai hozadéka volt az utókor szempontjából. A technológiai szektorba felelőtlenül öntött dollármilliárdok tették például lehetővé, hogy országon belüli és országhatárokat átívelő száloptikás hálózatok épüljenek ki, vagy éppen bőséges erőforrást csatornázzanak a 3G mobiltechnológiai kutatások területére. De épp úgy hozzájárult az okostelefonok (Apple, Samsung), algoritmuson alapuló keresőmotorok (Google), az e-piacterek (Amazon), a social média felületek (Facebook, Twitter), vagy éppen a felhőalapú számítástechnikai megoldások (Dropbox) előfeltételeinek a megte-

¹⁶ Too big to fail, azaz túl nagy ahhoz, hogy bedőljön. A rendszerstabilitás szempontjából fontos intézményeket illetik ezzel a megnevezéssel. A pénzügyi szektorban okoz erkölcsi kockázatot az a jelenség, hogy a nagyra nőtt intézmények annak a szinte biztos tudatában alakítják üzleti stratégiájukat, hogy méretük miatt a kormányzat úgysem hagyja bedőlni őket, s a túlzott kockázatvállalás számláját végül is az adófizető állja.

remtéséhez – nem beszélve az olyan kardinális szabályozási kérdésekben bekövetkező változásokról, mint például a 2002-es amerikai Sarbanes–Oxley-törvény¹⁷. Hasonlóan az 1880–1890-es években megélt boom-bust gazdasági krízishez („Baring-válság”), amely egy egész országot behálózó vasúthálózatot hagyott hátra, a dotkomlufi felfúvódása és kipukkanása is jelentősen hozzájárult a gazdasági-technológiai szerkezetváltozáshoz.

További roppant nagy különbség a két gazdasági krízis között a tőkeáttétel mértéke volt. Míg a dotkomlufi felfúvódása mögött főként megtakarításait átrendező kis- és nagybefektetők portfólió-beruházásai (részvény) álltak, addig az ingatlanpiac radikális áremelkedését a hatalmas tőkeáttételből finanszírozott kereslet fűtötte.¹⁸ Az előbbi esetében a buborék kidurranása nem okozott rendszerkockázati problémákat, hiszen a bankrendszer pusztán marginális kitettséggel rendelkezett, az utóbbi esetében azonban a tőkeáttétel leépítése futótűzként terjedt végig először a pénzügyi rendszeren, majd magával húzta a reálgazdaságot is.

Shiller professzor azon kijelentése tehát, amellyel a kriptopiacon tapasztalható „irracionális túlbujánzást” a dotkom-, illetve az ingatlanlufihoz hasonlította, a fentiek fényében elhamarkodottnak és felszínesnek tűnhet.

Mindazonáltal kétségtelen, hogy mániáról beszélhetünk. A bitcoin árfolyama 2017-ben 1278%-ot, az etheré pedig 9473%-ot emelkedett.¹⁹ Az 1. ábra igen jól szemlélteti a bitcoinpiacon tapasztalható emelkedés nagyságát a múltbéli eszközár-buborékok tükrében. Jól kiolvasható belőle, hogy az elmúlt három esztendőben tapasztalt árnövekedés messzemenően túlszárnyalja a nagy történelmi ár-buborékok dinamikáját.

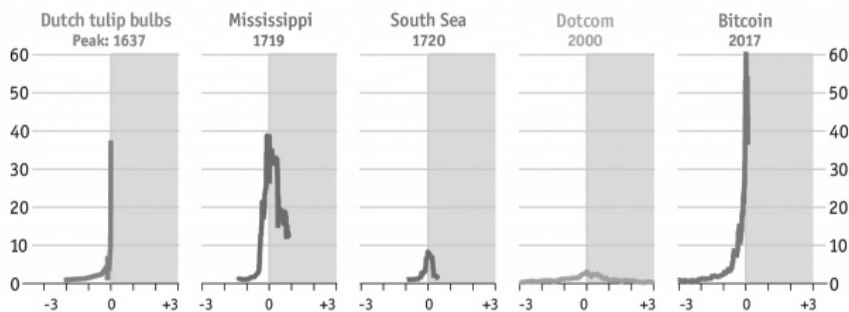
17 A 2002. évi Sarbanes–Oxley-törvényt az Egyesült Államok szövetségi szintű, értékpapírokra vonatkozó jogszabályait érintő legjelentősebb módosításnak tartják a New Deal óta. A törvény elfogadására vállalati pénzügyi botrányok sorozata nyomán került sor (többek között Enron, Arthur Andersen és WorldCom). A törvény legfontosabb rendelkezései: büntető és polgári jogi büntetések kiszabása az értékpapírszabályok megsértéséért, a könyvvizsgálói függetlenség/belső ellenőrzési munka külső szakértők általi ellenőrzésének szabályozása, a felső vezetői díjazások, a bennfentes kereskedés és a pénzügyi kimutatások részletesebb közzététele.

18 Mindezen felül természetesen a válság kialakulásához épp úgy hozzájárultak mikro- és makroszintű okok is, így a pénzügyi kvantok által újonnan létrehozott szintetikus, sokszorosan átcso-magolt „pénzügyi innovációk”, a rendkívül alacsony kamatkörnyezet és a végtelenül megengedő (accomodative) monetáris politika, valamint a nagyon sok minden felett szemet hunyó szabályozói keretrendszer is.

19 Az éven belüli maximális növekedés 2100%, valamint 11 400% volt. Mindezekhez képest is elképesztő emelkedést produkált a privát blokkláncon működő, bankközi tranzakációs rendszerek implementálásával foglalkozó cégeknek – Rippelnek – a kriptóárfolyama: 353 843%-ot tudott csúcspontjáig emelkedni 2017 decemberére! (Nem elírás! 353-szeresére emelkedett az árfolyam!)

1. ábra

Történelmi eszközár-buborékok összehasonlítása



Megjegyzés: Az ábra a tőzsdén jegyzett árak emelkedésének százalékos változását mutatja a buborék kidurranása előtti három évben (ahol nem állt rendelkezésre három év adatsora, ott rövidebb időszakot).

Forrás: Economist.com (Cryptocurrencies are in a tailspin, 2018. 01. 22)

A klasszikus közgazdasági szak- és tankönyvek által ismertetett eszközár-növekedési modellek ismeretében nehéz lenne nem buborékjelenségnek hívni a kriptopiacon tapasztalt növekedést. Mindez nem is csoda, hiszen az óvodáskorú lakosságtól egészen az idősebb korosztályig mind többen és többen foglalkoznak a bitcoinnal és a kriptovaluták világával – még ha csak közbeszéd szintjén is. A Google nemrégiben publikált jelentése szerint a „hogyan” kategóriában a „Hogyan lehet bitcoin vásárolni?” a második, a „Hogyan lehet bitcoin bányászni?” a hatodik helyet foglalta el a 2017-es keresési statisztikákban (*The Telegraph*, 2017).²⁰ E roppant nagy érdeklődés eredményeként a kriptotőzsdéken regisztráló, új felhasználók száma 2017 utolsó negyedében olyan mértékű emelkedést mutatott, amely a legtöbb tőzsde számára komoly technológiai és erőforrásbeli kihívást jelentett. A legnagyobb tőzsdék közül az USA-ban működő *Coinbase* (valamint vállalati felülete, a *GDAX*), a *Bittrex* és a *Kraken*, a luxemburgi *Bitstamp* és a kínai *Binance* 2017 utolsó két hónapja során napi szinten egyenként 100 000-es nagyságrendű új ügyfél-regisztrációt jelentett. A *Binance* CEO-ja 2018. január 4-én hivatalos közleményben jelentette be, hogy az új ügyfelek regisztrációjának a lehetőségét átmenetileg felfüggesztik²¹ a korábbi napon tapasztalt 250 000 új regisztrációt²² követően (*Cointelegraph*, 2018).

20 Érdekes még, hogy a „Mit jelent a bitcoin?” kérdés a „Mit jelent” kategóriában ötödik helyezést ért el.

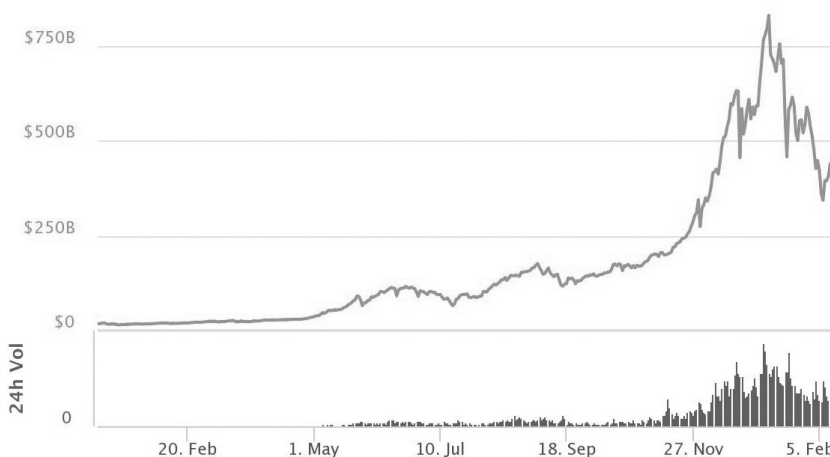
21 Más kriptotőzsdék is felfüggesztették az ügyfél-regisztrációt. Példának okáért a Bitfinex, Bitstamp és a Bittrex 2017. december és 2018. január közepe között nem fogadott új ügyfelet.

22 A napi több milliárd dolláros forgalom, magas profitrés, bőséges fizikai és emberi erőforrás ellenére a kriptotőzsdék legnagyobb kihívása abban áll, hogy a hatóságok által előírt KYC (Ismerd meg az ügyfeled) és AML (pénzmosás megelőzéséről szóló) szabályoknak megfeleljenek. Ehhez pedig arra van szükség, hogy minden új ügyfél regisztrálásakor a beadott dokumentumokat embereknek kell egyesével átnézniük és jóváhagyniuk.

A fenti ügyfél-regisztrációs adatokat figyelembe véve mindez azt jelenti, hogy havi szinten legalább 1-3 millióra tehető az ügyfélállomány növekményének a száma a nagyobb tőzsdék esetében. Ha pusztán azt feltételezzük, hogy csak minden harmadik ügyfél²³ helyezett el kis összegű befektetést – tegyük fel, 100 dollárt – ügyfélszámláján, amiből aztán valamilyen kriptovalutát vásárolt, akkor az azt jelentené, hogy napi szinten több mint 3 millió dollár tőke áramolhatott a kriptopiacokra. Hangsúlyozzuk: tőzsdénként. Ugyan hivatalos statisztikák jelenleg még nem léteznek a kriptotérbe áramló befektetésekről, de ha ezt az összeget felszorozzuk a néhány jelentősebb forgalmú, keményvaluta-befizetést támogató kriptotőzsdék számával, azt kapjuk, hogy 2017-es év utolsó hónapjaiban napi több tízmillió dollár új tőke áramlott a piacokra.

2. ábra

A kriptoeszközök piacának kapitalizációja, milliárd dollár (2017. 01–2018. 02)



Megjegyzés: A bitcoin teljes kriptopiacon belüli részaránya az év elején tapasztalható 90-95%-os szintről 2017 végére kb. egyharmadára zsugorodott.

Forrás: CoinMarketCap.com

A kriptopiac kapitalizációjának a 2. ábrán látható, exponenciális növekedési üteme igazolni látszik az új pénz beáramlásával kapcsolatos becslésünket. Mindezek fényében a 2017 utolsó negyedévében tapasztalt, soha nem látott mértékű áremelkedés aligha meglepő.

²³ Feltételezésünk szerint az újonnan regisztráló ügyfelek kétharmada először csak ismerkedik a platformmal.

Az árfolyam-emelkedés, azon belül is a bitcoin árának növekedése kapcsán azonban nem feledkezhetünk meg arról a tényről, hogy a Bitcoin 2009-ben elfogadott és lefektetett konszenzuson alapuló protokolljának értelmében a bitcoin kínálata folyamatosan – ámbár csökkenő mértékben – növekszik. 2017-ben körülbelül 4%-kal bővült a bitcoin teljes mennyisége. A jelenlegi feltételek mellett a körülbelül tízperces blokkidővel és blokkonkénti 12,5 bitcoin jutalommal számolva, naponta körülbelül 1800 új bitcoint bányásznak ki, amelynek egy részét minden bizonyosan keményvalutáért cserébe értékesítik a fenntartási és üzemeltetési költségek fedezése érdekében. Mindez a jelenlegi 8400 dolláros²⁴ árfolyammal számolva napi 15 120 000 dollár értékű új bitcoint jelent a forgalomban. Ahhoz, hogy az árfolyam-emelkedés fenntartható maradjon, legalább ekkora volumenű új tőke beáramlására van szükség a Bitcoin piacán.

A 2. ábra ugyanakkor nem csupán a Bitcoin kapitalizációját szemlélteti. A bitcoin teljes piacon belüli, év elején tapasztalt domináns aránya (95%) ugyanis az elmúlt esztendő leforgása alatt a teljes kapitalizáció harmadára csökkent. Ennek oka az alternatív kriptoeszközök piacának (*alt-coinok*) valutái iránt mutatkozó, növekvő érdeklődésben keresendő. Mindezt egyrészt azzal lehet magyarázni, hogy a sok számjegyű hozamokhoz szokott befektetők a bitcoinnak a 2017 nyarán tapasztalt, oldalazó mozgása láttán befektetések egy részét magasabb hozamú, éppen az érdeklődés középpontjába kerülő kriptovalutákba csoportosították át, másrészt pedig a piacot övező mánia következtében temérdek új pénz áramlott az alternatív kriptovalutákba.

Az alternatív kriptobefektések mellett említést érdemel még korunk legújabb közönségi finanszírozási formája, az ICO²⁵ is. A nyilvános kriptóérme-kibocsátás révén dollármilliárdokat költenek a befektetők sokszor csak pusztán koncepció szintjén létező, néhány oldalas, úgynevezett *white paper* keretében összefoglalt, sokszor még üzletinek sem nevezhető tervek finanszírozására. A CoinDesk 2017 utolsó negyedéves jelentése²⁶ szerint a befektetők három hónap leforgása alatt 3,23 milliárd dollárt öntöttek a piac eme rendkívül spekulatív jellegű szegmensébe,

24 Adatgyűjtés napja: 2018. 02. 11.

25 Az ICO az Initial Coin Offering vagy Initial Coin Offering angol kifejezés rövidítése. Legegyszerűbben úgy magyarázhatnánk, hogy ez a crowdfunding és a nyilvános tőzsdei kibocsátás (röviden: IPO) különleges ötvözete. A célja, hogy a kibocsátó a kriptovaluta kibocsátásával szerezzen tőkét projektjének, cégépítésének finanszírozásához. Hasonlít az IPO-hoz, ahol a kibocsátó részesedést (részvényt), haszonvárakozást kínál fel a forrásért cserébe. A crowdfundinghoz (a közösségi tőkeági finanszírozáshoz) hasonlóan pedig a befektetők visszakapják a pénzüket, amennyiben a nyilvános felhívás során a minimum bevonni kívánt összeg nem gyűlik össze. A nyilvános felhívásnak vagy kibocsátásnak ez a formája valójában egyfajta reakció a kockázati tőke és angyaltőke magatartására, arra, hogy a bitcoin startupok ezen forrásokhoz nagyon nehezen, nagyon hosszú idő alatt jutnak hozzá. Gyakran a tőkebevonás szigorú feltételeit a bitcoin- és blockchainprojektek nem is tudják teljesíteni. Tőzsdére pedig csak nagyon kevesek gondolhatnak (forrás: <http://fintechzone.hu>).

26 CoinDesk: State of Blockchain 2018, 2017-Q4 Report, <http://www.coindesk.com>.

arra számítva, hogy a digitális zseton (*token*) árfolyama a tőzsdére vezetést követően szárnyalásba kezd.

A kriptopiacokat övező hype-ot a fentiekén túl tovább fűtötte az a hír is az év vége felé, hogy a két meghatározó amerikai tőzsde, a CME és CBOE²⁷ bejelentette, hogy termékpalletájukra bevezetik a nagy érdeklődéssel várt bitcoin future terméket.²⁸ Ezen keresztül ugyanis megteremtődött a lehetősége annak, hogy azon intézményes befektetők is beléphessenek e már szabályozott keretek között működő, likvid, készpénz-elszámolású (*cash settlement*) piacra, akik korábban a szabályozói korlátozások miatt kiszorultak onnan. Bár a bitcoin future bevezetésével a szabályozott piacra áramló intézményes tőkének nincs közvetlen hatása a spotpiac árfolyamára, a forgalom és a piac mélységének növekedésével sokak szerint a forward árfolyam idővel simítani lesz képes az azonnali piacon tapasztalható, igen éles és szokatlanul nagy volatilitást. Mindez pedig azt jelentené, hogy a bitcoin közelebb kerülhetne ahhoz a ponthoz, hogy a pénzforgalmi és fizetési-eszköz-funkcióját hatékonyabban be tudja tölteni. Az ilyen és ehhez hasonló várakozások pedig nem meglepő módon további befektetőket ösztönöztek a bitcoin spotpiacára való belépésre.

A fentiek ellenére azonban tévhit lenne azt állítani, hogy az éven belüli, több ezer százalékos növekedés normális volna, és nem rejtene magában extrém kockázatot. Akár a bitcoin, akár más kriptovaluta piacán fektetünk be, tisztában kell lennünk a ténnyel, hogy azzal rendkívül nagy kockázatot vállalunk, és a befektetés sokkal inkább hasonlít egy szerencsejátékhoz, mint egy valós fundamentumokkal rendelkező eszközbefektetéshez. Mindazonáltal könnyen lehet, hogy az, aki szerencsés, sikerül eltalálnia a megfelelő beszállási pontot, és kellően prudens módon, portfóliójának csupán kis részét helyezi el a kriptopiacra, extrém nagy hozamot tud realizálni. Mondanunk sem kell, hogy a rossz pozíció megválasztása könnyen eredményezheti a teljes befektetés elvesztését.

Mánia tehát van. Részben a technológiába vetett, elvakult hit, részben pedig egy alapvető emberi jellemhiba, a kapzsiság miatt – attól tartanak, hogy kimaradnak a növekedésből (FOMO²⁹). Tagadhatatlan tény tehát, hogy buborékjelenséggel állunk szemben. A cikk megírása során pedig éppen e buborék deflálódása zajlik. A bitcoin legmagasabb – 2017 decemberi – árához képest közel 70%-ot veszített

27 A Chicago Mercantile Exchange (CME) a világ legnagyobb future tőzsdéje, míg a Chicago Board Options Exchange (CBOE) a legnagyobb amerikai opciós tőzsde. Mindkét intézmény 2017. decemberében vezette be készpénz-elszámolású bitcoin future termékét.

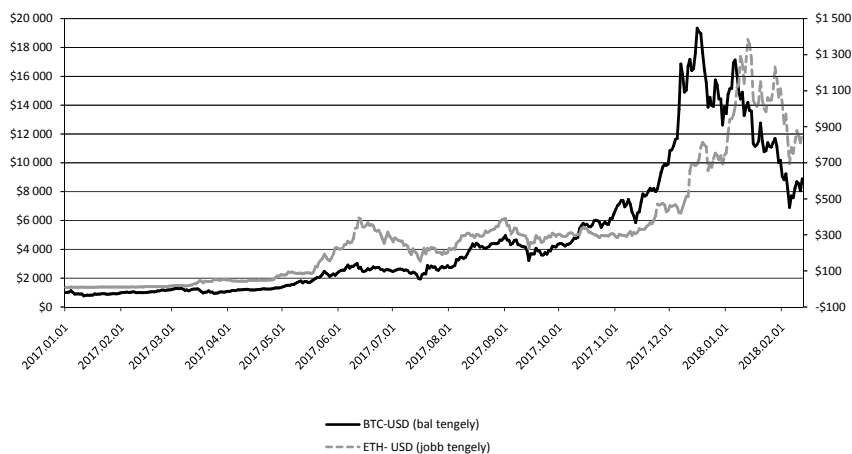
28 A CBO és CME után a Nasdaq is bejelentette: vizsgálja lehetőségét annak, hogy 2018 első félévében bevezessék a bitcoin futures-t.

29 Bár a FOMO (Fear of Missing Out), azaz a „félelem attól, hogy kimaradunk valamiből” egy új kifejezés, a jelenség maga nem az. Ez az érzelmi reakció mindig is létezett az emberiség történelme során. Pénzügyi buborékok idején pedig különösen jól jellemezte a befektetők gondolkodásmódját. Leginkább a kapzsisághoz és a mohósághoz áll közel.

értékéből (~19 800 USD) alig másfél hónap leforgása alatt, míg az ether, amely 2018 év elején még 10 nap alatt majdnem megduplázta árfolyamát (750 \$-ról 1400\$-ig emelkedve), alig 4 nap alatt 55%-ot zsugorodott (3. ábra).

3. ábra

A bitcoin és az ether árfolyamának alakulása (2017. 01. 01.–2018. 02. 12.)



Forrás: saját szerkesztés a Coindesk.com, EtherScan.com adatai alapján.

Becslésünk szerint a kriptovaluták mint kockázatos befektetési eszközök jelenleg az adaptáció korai fázisában lehetnek. Nehéz lenne megmondani, hogy mely eszközök tűnnek majd el, és melyek válnak eme technológia éllovasaivá hosszú távon. Azt sem lehet biztonsággal kijelenteni, hogy a bitcoin az utóbbi kategóriába sorolható-e, hiszen a szinte napról napra változó technológiai megoldások, valamint a meglévő eszközök protokolljában történő változások könnyen átírhatják a kriptopiac jelenlegi status quóját.

Egy dolog azonban bizonyosan kijelenthető: Robert Schiller állításának azon része, amely a kriptobuborékot a 2007–2008-as jelzálogpiaci válsághoz hasonlította, téves. Sokkal inkább hisszük – a dotkomválság analógiájára – azt, hogy egyszer majd visszatekintve, a kriptopiaci buborékot a bloklánc-technológián alapuló projektek szempontjából mérföldkőnek fogjuk tekinteni.

2.1. A Bitcoin értékelése

Minden pénzügyi buborék során kialakul egy (tév)hit az adott eszköz értékével kapcsolatban. Onnantól beszélünk lufiról, amikortól a keresleti és kínálati viszo-

nyok függvényében kialakult ár távolodni kezd az eszköz valós fundamentumai-ból³⁰ származtatható, belső értéktől.

A bitcoin és minden más kriptovaluta esetében azonban nem értelmezhető a belső érték. Ebből kifolyólag a buborékképződés is nehezen jelezhető előre. A következők során megvizsgáljuk, hogy melyek azok a tényezők, amelyek a bitcoin, illetőleg más kriptoeszközök értékét meghatározzák.

E kérdés megválaszolására már számos tudományos és kevésbé tudományos jellegű írás született, azonban konszenzusos módszertan az érték meghatározására továbbra sem létezik.

Egyesek szerint a kriptopénzek árfolyamát pusztán a keresleti-kínálati viszonyok alakítják, de születtek olyan jelegű írások is, amelyek a modern bitcoinbányász hardverek (ASIC; *AntMiner S9*) beszerzési árából, valamint a villamosenergia-árakból kiindulva a bányászás nehézségi fokának és a hálózat teljes számítási kapacitásának (amit gigahash/másodpercekben mérnek) függvényében adják meg az egy egységnyi bitcoin „előállításának” költségét. *Trubetskoy* (2017) kalkulációja szerint az USA átlagos villamosenergia-árával számolva, 1 bitcoin előállításának villamosenergia-költsége 1567\$ volt 2017 szeptemberében. A számítás azonban nem veszi figyelembe a célgépek egyszeri beszerzési költségét – amelyek piaci ára drasztikusan megnövekedett kereslet következtében 4-5000 dollárra emelkedett –, valamint a tárolással, karbantartással és sokszor hűtéssel járó további költségeket sem.

Létezik továbbá egy olyan elmélet is, amelynek keretében a bitcoin értékét a tranzakciók volumenéhez kötik. Azaz minél többen használják a bitcoint fizetési céllal, annál nagyobb értéket tulajdonítanak a bitcointnak.

A bitcoin értéke fundamentálisan nem megfogható, hiszen nincs mögötte egy ország gazdasági ereje és teljesítménye, nincs mögötte egy vállalat profittermelő képessége, valamint áruval vagy egyéb értékálló eszközzel sincs fedezve. Akik úgy hiszik, hogy a bitcoin hasonló a részvényhez, azaz venni kell belőle, majd később magasabb áron eladni, azok nem értik sem a bitcoin természetét, sem a vállalati részvények működését. Részvényvásárlással ugyanis társasági részesedést, tulajdonrészt szerezhetünk egy vállalatban, amelyen keresztül a közgyűlések révén szavazati jogot gyakorolhatunk, valamint az osztalékfizetés révén részesedünk a vállalat profitjából – a részesedéssel arányosan persze. Amennyiben az adott vállalat nyereséges, az árfolyam emelkedni fog, hiszen a kifizetendő osztalék volumen bearázódik a részvény árfolyamába.

30 Egy befektetési jóság fundamentális értékét az eszközt kibocsátó társaság, intézmény vagy ország gazdasági teljesítőképessége, profitabilitása/hitelképessége és az eszköz várható hozamának diszkontált értéke adja.

A bitcoin árát valójában nem egy mögöttes, fundamentális teljesítmény, belső érték adja, hanem a Bitcoin-hálózatot támogató közösség konszenzusa. A protokollt fejlesztők (*core developers*), a bányásztársaságok (*mining pool*), a kriptotőzsdék és az üzletileg érdekelt szereplők azon irányú egyetértése és hite, hogy a kriptográfiai eljárás révén előállított digitális kód – amely csak a digitális világban létezik – valódi értékkel rendelkezik. Értékét pedig a forradalmi újdonsága biztosítja: a lehetőség, hogy úgy lehet egymás között villámgyors és olcsó tranzakciókat lebonyolítani, azaz vagyont transferálni, hogy harmadik, közvetítő fél bevonására egyáltalán nincs szükség.

Ha belegondolunk, az arany árupénzfunkciója is egyfajta konszenzusként jött létre már évszázadokkal Krisztus előtt. Már *Arisztotelész* és *Platón* is értekezett a sárgán csillogó, ritka fémről. Úgy tartották, hogy az arannak a vízhez van köze – ami logikus is, hiszen a patakokban, vízfolyásokban találtak rá először –, és nem más, mint a víz és a napfény sűrű kombinációjának egyvelege. Tekintettel arra, hogy a Nap fényerejét a legtöbb vallás egy felettes, isteni erőhöz kötötte, az arannak különös jelentőséget tulajdonítottak. E hit következtében és annak a ténynek köszönhetően, hogy az arany képes volt betölteni az árupénz funkcióit (értékállóság, oszthatóság, egyneműség, szállíthatóság, elfogadottság), az arany és az abból készített érmék idővel fizetési eszközzé váltak.

Korunk digitalizálódó világában, amikor előbb-utóbb minden – technikai – eszköz képes lesz velünk és egymással is kommunikálni az interneten, miért lenne utópisztikus, ördögtől való gondolat az, hogy a mindennapjaink során használt pénz is teljesen digitálissá váljon? És ha ez bekövetkezne, miért ne lehetne a kriptovalutáknak szerepe e rendkívül nagy változást jelentő forradalomban?

E kérdések megválaszolására természetesen nem kívánunk próbát tenni. Pusztán gondolatébresztő kérdésként kívántuk feltenni a kedves olvasónak.

2.2. A Bitcoin korlátai

Satoshi Nakamoto egy olyan digitális pénzügyi rendszert képzelt el korunk legnagyobb globális pénzügyi válságának közepette, amely lehetővé teszi a rendkívül olcsó és gyors, valós időbeli pénzmozgatást. Cikkének időzítése vélhetően nem volt véletlen. Az egész világgazdaságon végigsöprő pénzügyi válság ugyanis rámutatott a monetáris politikák gyenge pontjaira, illetőleg az aszimmetrikus kulcsvalutarendszer hiányosságaira.

Koncepciójának egyik fő célja valójában az volt, hogy egy olyan digitális fizetési rendszert alkosson meg, amely független a monetáris politikáktól. Egyetlen hatóság sem képes ugyanis a bitcoin kínálatának szabályozására, újraelosztására, valamint a pénzforgalom befolyásolására, ilyenformán pedig az teljesen független

a világgazdasági és világpolitikai eseményektől. Bármennyire is izgalmasnak és forradalmian új megoldásnak tűnik a Bitcoin elszámolási rendszere, a felhasználóknak számos problémával és korlátozással kell szembesülniük napjainkban.

A Bitcoin-hálózat a 2017 második felében tapasztalt, nagyfokú érdeklődés következtében túlterheltté vált. Mindez költségesebb átutalásban és hosszabb tranzakcióidőben manifesztálódott.³¹ A 4. ábrán az átlagos tranzakcióidő alakulása látható 2017 eleje óta, ami jól szemlélteti a növekvő várakozási időt. 2018 januárja során számos alkalommal fordult elő, hogy több mint kétnapos átfutási idővel teljesült bitcointranzakció. Az eddigi leghosszabb tranzakciós idő 11 453 perc, azaz közel 8 napos volt, ez 2018. 01. 23-án került végrehajtásra. Jelenleg azoknál a megbízásoknál, ahol a magasabb tranzakciós díjat hajlandók megfizetni a bányászoknak, a teljesülési idő mediánja 13-15 perc. Egy trade-off figyelhető meg tehát a tranzakciós idő, valamint a tranzakciós díjak között. Akik vállalják a magasabb díjat, azoknak a hálózat az átutalást előbb fogja teljesíteni. Mindez pedig alapvetően ellenkezik azzal a koncepcióval, amit az alapító lefektetett: a villámgyors és olcsó digitális átutalás lehetőségével. Az 5. ábrán a hálózaton feladott tranzakciókat sorba állító memória pool (*mempool*) méretét láthatjuk, aminek következtében a korábbi néhány másodperc alatt teljesülő tranzakciók átlagideje akár órákra is elnyúlhat.

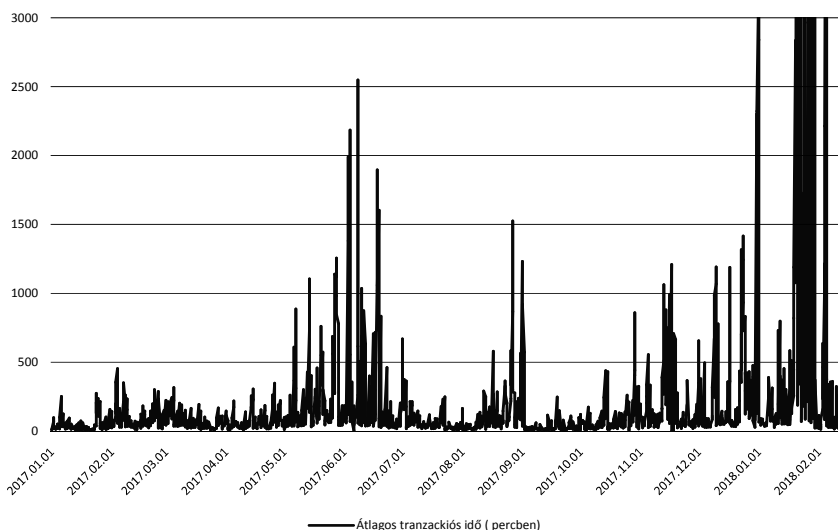
Számos próbálkozásnak lehattünk már szemtanúi a Bitcoin blokkméretének növelésére és blokkidejének csökkentésére, azonban mind a mai napig ezek csupán *hard-fork*³² eseménybe torkolltak, változatlanul hagyva az eredeti Bitcoin szabályrendszerét.

31 A bitcoin átutalásáért fizetendő tranzakciós költség 2017 előtt mindösszesen pár cent volt. 2017 második felében, a hálózat fokozódó terhelése következtében azonban egyre magasabb díjat – 1-5 \$ – kellett fizetni a bányászoknak a tranzakció validálásáért. 2017 decemberében volt két olyan nap is az ünnepek előtt, amikor – a vélhetőleg szándékos hálózati terhelés következtében – a tranzakciós díjak az egekbe szöktek: átlagosan 55\$-t kellett leróni akár egy 10\$ értékű bitcoinátutalásért is (volt, amikor extrém esetben 162\$-t is fizettek egy tranzakcióért!) Akik nem kívánták e magas díjat megfizetni, azoknak az utalási megbízása az úgynevezett memória poolba került. Ha szerencsénk volt, akkor az általuk megjelölt alacsonyabb díjon is teljesült a megbízás. Ha nem, akkor utalási megbízásukat visszautasították.

32 Tekintettel arra, hogy a bitcoin forráskódja nyilvános, bárki készíthet másolatot róla, amelyben kisebb vagy nagyobb módosításokat eszközölhet. E változtatások révén gyakorlatilag létrejön egy új blokklánc. Ezt hívják hard fork eseménynek. Ekkor a bányászok egy része egy másik blokkláncra és azon blokklánc tranzakcióinak hitelesítésére (bányászására) áll át. A folyamat során a bitcoinok teljesen biztonságban vannak. A legtöbb ilyen esemény ugyanis nem más, mint a Bitcoin-protokoll fejlesztése, frissítése. Létezik azonban olyan frissítés is, amelyik a bitcoin alapvető tulajdonságait befolyásolja, mint például a blokkméretet. Azzal, hogy két blokklánc jön létre, gyakorlatilag egy újabb digitális eszköz keletkezik. Ilyenkor a bitcointulajdonosok a privát kulcsuk segítségével hozzáférhetnek a kriptopénzükhöz mindkét blokkláncban. Ilyen esemény következett be a Bitcoin hálózatán 2017. augusztusában, mikor a blokkméret 8 Mbyte-ra történő módosításával létrejött a Bitcoin Cash. A nagyobb táborban, akik nem fogadták el ezt a változtatást, attól tartottak, hogy a blokkméret növelése hosszú távon a decentralizáltságot veszélyezteti – hiszen a nagyobb blokkmérettel lesznek olyan szereplők, akik kiszorulnak a piacról.

4. ábra

Átlagos tranzakciós idő a Bitcoin hálózaton, percekben



Megjegyzés: A 3000 perces meghaladó tranzakciós idők levágásra kerültek a könnyebb szemléltetés érdekében.

Forrás: saját szerkesztés a <http://blockchain.info> adatai alapján.

Bár nem célunk technikai jellegű részletekbe bocsátkozni, néhány szót azonban szükségesnek tartunk megemlíteni a Bitcoin protokolljával kapcsolatban. Az eredeti, 2009-ben lefektetett és azóta alapjaiban változatlan szabályrendszer szerint a blokkméret 1 Mbyte-ban került rögzítésre. Évekkel ezelőtt, 2010-ben az akkori hálózati infrastruktúra (sávszélesség) nem tette lehetővé a nagyobb blokkméret használatát; ezt felismerve Satoshi a stabilitás érdekében egy rendszerfrissítéssel vezette be az 1 Mbytes blokkméretet.

Historikus adatokból ismert, hogy egy átlagos bitcointranzakció mérete 495 byte. Azaz egy 1 000 000 bájtós blokkban körülbelül 2020 tranzakció elhelyezésére kerülhet sor. Tekintettel arra, hogy a Bitcoin protokollját akként határozták meg, hogy a hálózat bonyolultsági foka a teljes számítási kapacitás figyelembe vétele mellett úgy változzon, hogy egy blokk feldolgozási (kibányászási) ideje körülbelül 10 perc legyen, másodperceként mindösszesen 3,37 tranzakció lebonyolítására nyílik lehetőség. Ez a szám pedig meglepően alacsony érték a PayPal másodpercenkénti közel 500, a VISA-hálózat 1667 tranzakciójához képest.

A tranzakciós időnek a 4. ábrán látható, jelentős növekedését a bitcointranzakciók feltorlódása eredményezte (5. ábra). Az elmúlt két évben ugyanis a hálózat nagyobb szereplői (bányászok és a fejlesztők) nem jutottak konszenzusra a Bitcoin

szabályrendszerének fejlesztéséről, arról, hogy miképpen lehetne a hálózat kapacitását akként növelni, hogy az az alapokat – decentralizáltság, transzparencia, cenzúrazerezisztencia, manipulálhatatlanság – ne veszélyeztesse.³³ Mindez azonban szilárd bizonyítékul szolgál arra, hogy mennyire demokratikusan működik a rendszer – hiszen a kulcsfontosságú kérdésekben csak igen lassan és csak teljes konszenzus mellett döntenek.³⁴

5. ábra

A teljesítésre várakozó bitcointranzakciók aggregált mérete byte-ban



Forrás: saját szerkesztés a <http://blockchain.info> adatai alapján

Ahhoz hogy a bitcoin pénzként funkcionáljon, be kell töltenie a pénz funkcióit. Közvetítenie kell a cserét és mérnie az áru értékét (értékmérő funkció), elő kell segítenie az áruk és a hitelpénz mozgását (forgalmi és fizetési eszköz funkció), valamint lehetővé kell tennie a vagyon felhalmozását, azaz alkalmasnak kell lennie tartalékolásra.

A bitcoin árának rendkívül magas változékonysága (lásd 7. ábra) túlságosan nagy piaci kockázatot jelent a tranzakciós és befektetési célú bitcoin-felhalmozás tekintetében. Gondoljunk bele abba, hogy egy kereskedő hogyan tudná biztonságosan portékájának bitcoinban denominált árát meghatározni, ha a bitcoin árfolyama

33 A blokkméret növelését vagy változatlanul hagyását támogató két tábor között több mint két-éves, komoly szakmai vita zajlik, amit sokszor „scaling war”-ként említenek.

34 A kapacitás növelésére jelenleg két teljesen eltérő technikai megoldási javaslat létezik: a blokkméret emelése, valamint a másodsztintű (second layer) tranzakciók bevezetése. Ez utóbbi érdekében volt szükség a Segregated Witness (SegWit) bevezetésére 2017-ben, amelynek az előkészítése szintén éveket vett igénybe. A SegWittel „tömörebbé” vált a blokk struktúrája (egyfajta optimalizálás volt) azáltal, hogy nem minden aláírás kerül rögzítésre a blokkon belül. Ezzel pedig lehetőség nyílik a Lightning Network elindítására, amellyel tehermentesíteni lehet a Bitcoin-hálózatot a kisebb tranzakciók blokkláncon kívülrre való szervezésével (bővebben a SegWitről és a Lightning Networkről: <https://en.wikipedia.org/wiki/SegWit>; https://en.wikipedia.org/wiki/Lightning_Network).

akár napi 5-15%-os elmozdulásra is képes a világ első számú kulcsvalutájával, a dollárral szemben?

Egy valuta az árucserre közvetítésére csak akkor képes, ha értéke közel állandó, és elfogadottsága széleskörű. A termékek egymáshoz viszonyított árai ugyanis a valuta értékén keresztül határozódnak meg. Egy mindkét irányba hirtelen ármozgásokat produkáló eszköz pedig csak korlátozottan képes e közvetítő funkció betöltésére. Ráadásul a bitcoinkereskedők fizetőeszközként eléggé korlátozott mértékben fogadják el. 2017 során pedig nemhogy nőtt volna, hanem tovább csökkent a bitcoint elfogadó áruházak száma. Egy *James Faucette*, a Morgan Stanley elemzője által készített tanulmány szerint a top 500 online kereskedő közül 2016-ról 2017-re 5-ről 3-ra csökkent a bitcoint elfogadó szereplők száma.³⁵

Kérdéses, hogy e csökkenésre milyen mértékben van hatással a 2017-es évben tapasztalt, csillagászati hozamokat biztosító bitcoinárfolyam-felértékelődés. Ha ugyanis a bitcoin tranzackiós célokra történő felhasználása marginális a folyamatosan tapasztalt pozitív vagyonhatás következtében, a kereskedő sem lesz érdekelt új fizetési platform bevezetésében. Mindezek mellett még említést érdemel a növekvő tranzackiós díjak miatt az értékmérő funkció tekintetében kizáródó, alacsony összegű vásárlások köre, mint például egy kávé vagy üdítő bitcoinnal történő kifizetése. Hiszen abszurd lenne azt feltételezni, hogy bárki is hajlandó lenne a termék vagy szolgáltatás áránál magasabb tranzackiós díj megfizetésére.³⁶

Ha a pénz és az áru nem képes azonos időben gazdát cserélni, akkor a forgalmi-eszköz-funkció sérül. A Bitcoin esetében az elhúzódó átutalási idő pedig jelenleg e pénzfunkció ellenében hat. Amennyiben az évek óta előkészítés alatt álló, kapacitásnövelő frissítések kapcsán konszenzus jönne létre a felek között, és megvalósulna a Bitcoin protokolljának fejlesztése, az a teljesülési idő szingifinans lerövidülését (1-3 másodperc) eredményezné.³⁷ Mindez pedig a bitcoin forgalmi-eszköz-funkciójának megszilárdulását szavatolná.

A vagyon felhalmozódásának egyik formája a pénz tartalékolása. A pénznek alkalmasnak kell lennie arra, hogy a kincsképzés eszköze legyen. Ehhez ki kell elégíteni azt az állandó igényt, hogy értéke stabil, ne csökkenő legyen. A bitcoin dollárban denominált ára az elmúlt évek során egészen 2017 decemberéig folyamatos, 2017 utolsó negyedében parabolisztikus trendszerű növekedést produkált, újabb és újabb kis- és nagybefektetőket csábítva a piacra. Példának okáért, ha valaki 2010 nyarán 1000 dollárt fektetett volna bitcoinba (ami akkoriban ek-

35 <https://www.bloomberg.com/news/articles/2017-07-12/bitcoin-acceptance-among-retailers-is-low-and-getting-lower>.

36 A bitcoinban történő fizetés kapcsán pedig nem szabad megfeledkeznünk arról a tényről, hogy a vevő fizeti a tranzackiós díjat a bank- és hitelkártyás vásárlásokkal szemben.

37 Jelenleg a tesztelés alatt álló Lightning Networkön a tranzackiók teljesülési ideje csupán néhány másodperc.

vivalens lett volna azzal, hogy ezt a pénzt megjátssza a lóversenyen), 2017 végére 242 millió dolláros vagyon fölött diszponált volna (lásd a 8. *ábra* előtti megjegyzésünket). Mindez látszólag kielégíti a felhalmozási funkciót, hiszen a bitcoin értéke az időszakos korrekciókat leszámítva, folyamatosan nőtt az elmúlt évek alatt. Tavaly december óta azonban mind relatíve, mind abszolút értékben jelentős leértékelődést mutatott a bitcoin a főbb fiat valutákkal szemben, felerősítve a bitcoinszkeptikus véleményeket, valamint megkérdőjelezve a korábbi növekedő trend fenntarthatóságát.

A fentiek fényében úgy véljük, hogy a bitcoin jelenleg nem képes maradéktalanul betölteni a pénz funkcióját. Abban az esetben, ha a korábbiak során említett protokollt érintő fejlesztések teljesülnének, valamint a Bitcoin piacának feszessége, mélysége és rugalmassága (piaci likviditása) tovább javulna, úgy lehetőséget látnánk arra, hogy a pénzzé válási folyamatban a bitcoin egy újabb lépést tegyen. Mindezek mellett természetesen szükség lenne az árfolyam volatilitásának csökkenésére, amihez a nemrégiben elindított future bitcoinpiacok, valamint a folyamatosan emelkedő piacméret egyaránt kedvezően járul hozzá.

3. BITCOIN: AZ ÚJ ESZKÖZCSOPORT

Annak ellenére, hogy a Bitcoin piaci kapitalizációja nemrégiben már a 200 milliárd dollárt is meghaladta, a mai napig számos értelmezési és besorolási zavar övezi ezt a különös virtuális eszközt. Míg az amerikai határidős árutőzsdét felügyelő szerv, a CFTC áruként tekint a bitcoinra, addig az amerikai adóhatóság (IRS) tulajdonjogot megtestesítő eszközként tartja számon. Az amerikai értékpapír-felügyelet (SEC) bizonyos esetekben értékpapírként sorolja be, az Európai Központi Bank pedig konvertibilis decentralizált virtuális valutaként kezeli.

Maga a kriptovaluta kifejezés is bizonyos fokig félreértésre adhat okot, hiszen azt sugallhatja, hogy a kriptovaluták a tradicionális valuták egy alkategóriáját képezik. A valóságban azonban véleményünk szerint egy teljesen új eszközcsoporthról beszélhetünk. Ennélfogva a kriptográfián alapuló, nyitott, decentralizált virtuális valuták tekintetében célravezetőbb a kriptoeszköz elnevezés használata.

A tradicionális eszközcsoporthok megkülönböztetésére és kategorizálására már számtalan tanulmány született. Ezek közül *Robert Greer* (1997) munkáját emeljük ki, aki három fő közszósztaályt határozott meg: a tőkejavak, fogyasztható/átalakítható javak, valamint a vagyonszerzési eszközök (1. táblázat). Greer eszközcsoporth-kategorizálása az eszközök eltérő fundamentális gazdasági jellemzőin, valamint az eszközhozamok korrelációján alapszik.

1. táblázat**Tradicionális eszközcsoportok eszközosztályokba történő kategorizálása**

	Tőkejavak	Fogyasztható/ átalakítható javak	Vagyon- felhalmozási eszközök
	„Jövedelemáramlást biztosító jószág, amelynek a jelenértéke a jövőben várható hozamokból származtatható.”	„Megvásárolható, más eszközzé transzformálható. Gazdasági értékkel rendelkezik, azonban nem biztosít jövedelemáramlást.”	„Nem fogyasztható, jövedelemáram nem kapcsolódik hozzá, azonban értékkel rendelkezik, amely vagyonfelhalmozást tesz lehetővé.”
Részvény	X		
Kötvény	X		
Ingatlan	X		
Áru		X	
Nemesfém (arany)		X	X
Valuta			X
Műtárgy			X

Forrás: Rober J. Greer (1997): What is an Asset Class, Anyway?, The Journal of Portfolio Management

Burniske–White (2017) Greer megállapításaira építve, négy fő jellemzőt határozott meg a tradicionális eszközcsoportok egymástól való elkülönítésére:

- 1) Befektethetőség
- 2) Politikai-gazdasági jellemzők
- 3) Árfüggetlenség: hozamok korrelálatlansága
- 4) Kockázat-hozam profil

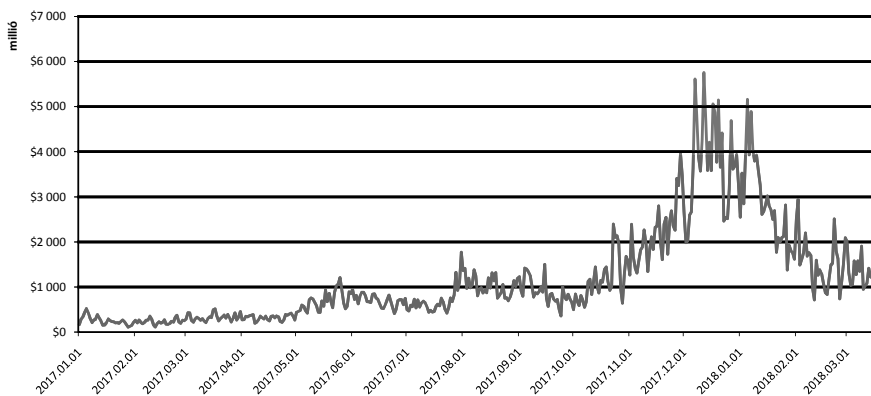
A befektethetőséget a piaci likviditás függvényében határozták meg. Másodszor, véleményük szerint egy jószág politikai-gazdasági profilját annak belső értéke, szabályozói környezete és használhatósága befolyásolja. Harmadszor, az árfüggetlenség alatt az eszköz piaci értékének a más eszközcsoport eszközeinek árától való függetlenségét értik, amit az eszközhozamok alacsony korrelációjából származtatnak. Végezetül pedig a kockázathozamprofil-eltérés mérésére az abszolút hozamok, valamint eszközárak volatilitásának mérését javasolták.

Különböző eszközcsoportba sorolható például a részvény és a kötvény, hiszen miután a befektethetőségi feltételt kielégítik, a másik három kategória szerint eltérnek egymástól. Míg a részvény egy határozatlan időre szóló követelést testesít meg, amelyet a vállalat jövőbeli profittermelő képessége biztosít, addig a kötvény csupán fix időszakra nyújt időközönkénti pénzáramot, amit a vállalat eszközértéke szavatol (politikai-gazdasági jellemző). Továbbá, a részvény- és kötvényárak alacsony kockázatú makrokörnyezetben ellentétes irányú mozgást írnak le: ha a kötvényárak emelkednek, a részvényárak lecsorognak (árfüggetlenség). Kockázat-hozam profil tekintetében is jelentős eltérést tapasztalni, hiszen a részvények alapvetően kockázatosabb és magasabb hozamú eszközök, míg a kötvények kevésbé volatilis, kisebb hozamtermelő képességgel rendelkező befektetési jóságok. A következőkben tekintsük át a bitcoin fent nevezett négy kategória szerinti jellemzőit.

A Bitcoin piacának likviditása a 2017-es év során jelentős bővülést mutatott. Míg 2014 és 2016 között körülbelül napi 10–150 millió dollár forgalom került lebonyolításra a bitcoin és a fiat valuták között, addig 2017 második felétől a forgalom fokozatosan megközelítette a 4 milliárd dolláros szintet (6. ábra). Ha csupán a BTC–USD-piacot vesszük figyelembe, amely a BTC–JPY-pár mellett a legnagyobb forgalmat adja, a bitcoin-dollár tranzakciók volumene napi szinten így is meghaladja az 1 milliárd dollárt. Egy ilyen mélységű és likviditású piac pedig akár több százmillió dolláros tranzakció lebonyolítására is alkalmas akként, hogy az szignifikáns árfolyamkilengést ne okozzon a bitcoin árfolyamában. Mindezek fényében tehát a Bitcoin illikviditásával és törékenységével kapcsolatban megfogalmazott, korábbi kritikák véleményünk szerint nem állják meg a helyüket, ennél fogva pedig a Bitcoin piaca kielégíti a fentebb említette befektethetőség kritériumát.

6. ábra

A Bitcoin átlagos napi tőzsdei forgalma 2017-ben, millió USD-ben



Forrás: Saját szerkesztés s <http://blockchain.info/> adatai alapján

A Bitcoin különlegessége és egyedisége nem csupán abban áll, hogy belső értéke nem létezik. Működési és szabályozási rendszere (*governance*) is jelentősen eltér a többi eszköztől. A Bitcoin a közösség konszenzusának, egyetértésének fényében létrejött protokoll szerint működik. E szabályrendszer tartalmazza a Bitcoin irányításával (*governance*), a letétek kezelésével (*custody*), a bitcoin „kibocsátásával” és disztribúciójával, a tranzakciók lebonyolításának menetével és végezetül a felügyeletével (*audit*) kapcsolatos minden információt, ami kötelező érvényű a hálózat minden szereplője számára. E szabályrendszer bármely elemének megváltoztatása csakis és kizárólag a Bitcoin-közösség közel teljes konszenzusa mellett valósulhat meg (ellenkező esetben a fentebb már említett *fork* esemény következik be).

Habár a felhasználás és használhatóság tekintetében a bitcoin hasonlónak tűnhet a tradicionális valutákhoz, vagy éppen az aranyhoz, a benne rejlő potenciál messze túlmutat az előzőkön. Az Ethereum hálózatának működése jó bizonyíték arra, hogy a blockklánc-technológián alapuló kriptoeszközök a pusztán adatrögzítésen és elszámoláson túl számos egyéb szolgáltatást nyújthatnak. A Bitcoin-protokoll – hasonlóan az Ethereumhoz – akár automatikusan futó szerződéseket kiszolgáló platformként is funkcionálhat majd, lehetővé téve, hogy a Bitcoin az eszközök egy igen széles csoportjának nyújtson digitális elszámolási szolgáltatást az ingatlanoktól a hitelek keresztül egészen az internetre csatlakozó eszközökig.

Mind ezek fényében úgy véljük, hogy a Bitcoin a politikai-gazdasági jellemzők tekintetében is különleges, hiszen nem létezik még egy olyan eszközcsoport, amelynek az esetében a fenti szabályelemek ilyen fokú koncentrációja megvalósulna.

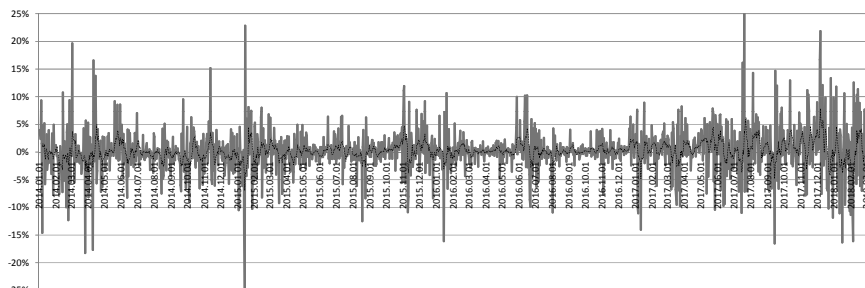
Az előzőekben bemutatott különbségek fényében a bitcoin ára kapcsán is azt várhatjuk, hogy az másképpen viselkedik, mint azt a klasszikus eszközcsoportok többségénél tapasztaltuk. Ennek mérésére leggyakrabban a korrelációs számítását alkalmazzák, amelyen keresztül a változók – jelen esetben a bitcoin és más eszközök – együttmozgását vagy annak a hiányát lehet számszerűsíteni. Amennyiben két eszköz ára tökéletes együttmozgást mutat, a korrelációs együttható $+1$ értéket, míg tökéletes ellentétes irányú mozgás esetén -1 értéket vesz fel. Ez utóbbi esetben egy két eszközből álló portfólió esetében tökéletesen kiküszöbölhető az eszközök egyedi kockázata. Mindebből az következik, hogy 0 vagy 0 -hoz közeli korrelációs együttható esetén az eszközárakra ható erők függetlenek egymástól. E külső gazdasági hatásoktól való függetlenség véleményünk szerint a Bitcoin egyedülállóságának a kulcsa. Cikkünk *4. fejezetében* a bitcoin árfüggetlenségével kapcsolatban megfogalmazott feltételezésünket dinamikus feltételes korreláció (DCC–GARCH) illesztésével támasztjuk alá. A mienkhez hasonló eredményre jutott *Burniske et al. (2017)* is, akik gördülő regressziós technikát alkalmazva mutatták be, hogy 2011–2017 között a bitcoin ármozgása képes volt függetlennek maradni a vizsgálatba bevont tőke és árupiaci eszközök áraitól. Egyebek mellett arra jutott, hogy a bitcoin az egyedüli olyan jószág, amely nem, vagy csak minimális korrelációt mutat a többi eszközcsoporttal.

Végezetül a bitcoin kockázat-hozam profiljának a bemutatása következik. Míg egy eszköz kockázatosságát az árának a volatilitása fejezi ki, addig a hozam tekintetében egyszerűen azt vizsgáljuk, hogy a befektetés értéke az árfolyamváltozás következtében miképpen módosul a vizsgált időintervallum alatt.

Habár a volatilitás számszerűsítésére leggyakrabban használt mutató a szórás és a variancia, a napi árfolyamváltozás is igen jól szemlélteti az eszközárak fluktuációját. A *7. ábráról*, amely a bitcoin napi záró árak változását mutatja, jól kiolvasható, hogy egy 10%-ot meghaladó árfolyamváltozás sem ritka a Bitcoin piacán. 2017. január 1-je óta egészen 2017. március 11-éig 122 napon fordult elő, hogy az árfolyamváltozás mértéke meghaladta az 5%-ot, és 30 napon, amikor a 10%-ot. Összességében a 2017 óta tartó periódusban az átlagos napi árfolyamváltozás 3,8%-ot mutat. Mondanunk sem kell, hogy például az S&P500 tőzsdeindex esetében 3,8%-os változás már igen heves árfolyamkilengésnek számítana. Mindez azonban a bitcoin piacán szó szerint mindennapos elmozdulásnak számít.

7. ábra

A Bitcoin napi árváltozása



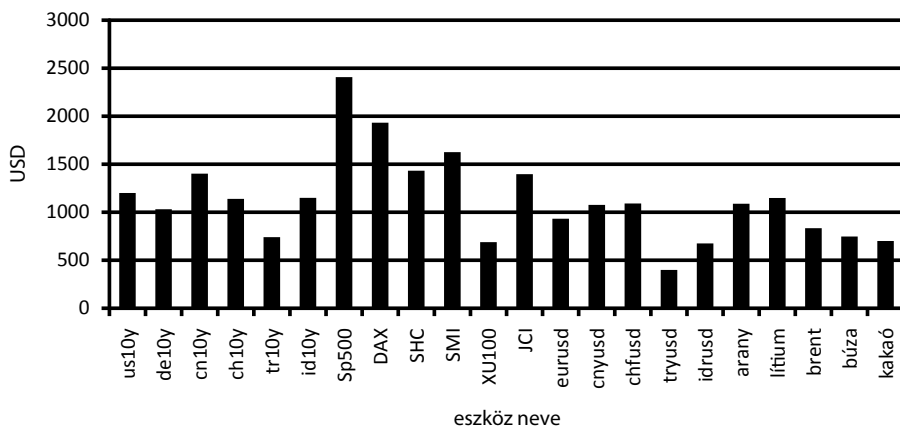
Megjegyzés: A Bitstamp tőzsde BTC–USD záró árai alapján

Forrás: saját szerkesztés a <https://www.quandl.com/> adatai alapján

A szaggatott vonal a napi árváltozások egyhetes mozgóátlagmódszer szerinti átlagát mutatja.

8. ábra

Egy feltételezett 1000 USD-s befektetés értéknövekedése 2010.07.23 és 2017.12.08. között



Forrás: saját szerkesztés

A 8. ábra azt szemlélteti, hogy egy, a mintavételezési periódus elején (2010. 07. 23-án) eszközölt 1000 dolláros befektetés értéke mennyivel változott volna, ha azt bitcoinba vagy a többi vizsgált eszközbe fektettük volna. Bitcoin esetében a végeredmény 242 702 012 dollár 2017. december 8-i zárás esetén, míg a többi befektetés eredményét a 8. ábra tartalmazza. Megállapítható, hogy a kötvénypiaci

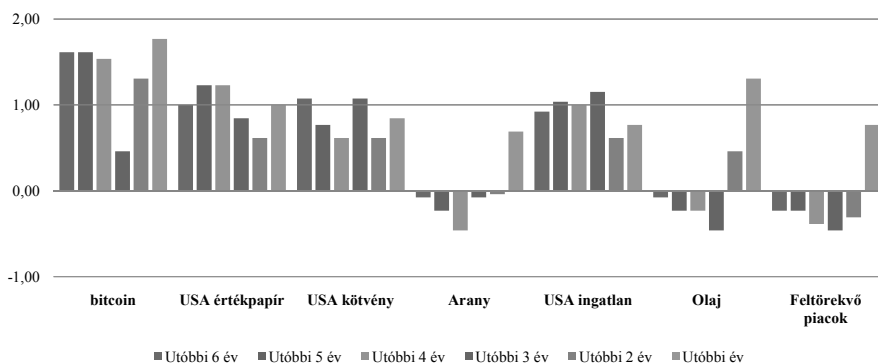
eszközök esetében a nulla közeli kamatláb politikája miatt nehezen realizálható hozam, míg a részvénypiacok (a török kivételével) kimagaslóan teljesítettek. Mindeközben sem devizákban sem nyersanyagokban nem volt elérhető érdemi nyereség. Bitcoinban tehát az árfolyam exponenciális emelkedése miatt egyszeri, rendkívül kimagasló hozamot lehetett elérni.

Mint az a modern portfólióelméletből következik, sem az eszközár-volatilitás, sem az eszköz hozamtermelő képessége nem jó útmutató a befektetési döntések meghozatalánál. Szükség van a hozamok volatilitással, azaz kockázattal történő kiigazítására. A szakirodalomban e célra leggyakrabban használt mutató a Sharp-mutató, amely megadja, hogy az egységnyi kockázatáért cserébe milyen extra hozamot nyújt a befektetésünk.

Burniske et al. (2017) több periódusra számolta ki 2011 és 2017 között a bitcoin, az amerikai értékpapírok, amerikai kötvények, az arany, az amerikai ingatlanok, az olaj, valamint a feltörekvő piacok valutáinak Sharp-mutatóját, amely szerint a legtöbb időtávon messze a legnagyobb megtérülést ígérő befektetési lehetőség volt a bitcoin (9. ábra).

9. ábra

A Sharp-mutató alakulása (2011–2017)



Forrás: Burniske et al. (2017)

Mind a bitcoin volatilitásának, mind pedig az abszolút hozamtermelő képességének ismeretében kijelenthető, hogy a kockázat-hozam profil tekintetében is egyedi jellemzőkkel bír a bitcoin.

Összefoglalva tehát, az a tény, hogy a Bitcoin kielégíti a befektethetőség feltételét, továbbá, hogy a politikai-gazdasági jellemzők, az árak együttmozgása, valamint kockázat-hozam profil tekintetében más, egyedülálló karakterisztikával rendelkezik, megerősíti azt a feltételezésünket, amely szerint a bitcoint és többi kriptoeszközt egyetlen, már létező eszközcsoport eszközeivel sem lehet egy kategóriába sorolni. Mindez pedig alátámasztja azt a tézisünket, hogy a kriptoeszközök megjelenésével egy új eszközcsoport van kialakulóban.

4. A BITCOIN ÉS MÁS ESZKÖZCSOPORT ESZKÖZEINEK ÖSSZEHASONLÍTÓ ELEMZÉSE

4.1. Adatok és módszertan

Munkánkban különböző pénz- és tőkepiaci heti záró árfolyamok³⁸ statisztikai jellemzőit hasonlítottuk össze a bitcoinnak az amerikai dollárral szembeni árfolyamával (BTC/USD) a 2010. július 23. és 2017. december 8. közötti intervallumon. Ennek során a 10 éves kötvény (US10Y, DE10Y, CN10Y, CH10Y), vezető részvény (S&P500, DAX, Shanghai Composite Index – SHC, Swiss Market Index – SMI), kulcsvaluták (EUR/USD, CNY/USD, CHF/USD) és a nyersanyagok piacára (olaj, arany, lítium, búza, kakaó) fókuszálunk.

Emellett megvizsgáltunk egzotikusabb eszközöket is, mint a török és indonéz részvénypiaci indexek (XU100, Jakarta Composite Index – JCI), 10 éves kötvények, illetve devizák árfolyamai. Miután a bitcoin esetében fontos szerepet kap majd a volatilitás elemzése, a vizsgálatba szintén beemeltük a VIX indexet is.

Munkánk során az egyes idősorok esetében előbb az alapstatisztikákat vetettük össze azok elvárható értékeivel a különböző eszközosztályok esetében, majd GARCH-, GJR–GARCH-, TARCH- és APARCH-modellek (1) közötti szelekció segítségével vizsgáljuk meg az eszközök volatilitását:

$$\begin{aligned} \text{GARCH: } \sigma_t^2 &= \omega + \sum_{i=1}^q \alpha_i \varepsilon_{t-i}^2 + \sum_{i=1}^p \beta_i \sigma_{t-i}^2, \\ \text{TARCH: } \sigma_t &= \omega + \sum_{i=1}^p \alpha_i |\varepsilon_{t-i}| + \sum_{i=1}^o \gamma_i S_{t-i}^- |\varepsilon_{t-i}| + \sum_{i=1}^q \beta_i \sigma_{t-i}, \\ \text{GJR-GARCH: } \sigma_t^2 &= \omega + \sum_{i=1}^p \alpha_i \varepsilon_{t-i}^2 + \sum_{i=1}^o \gamma_i S_{t-i}^- \varepsilon_{t-i}^2 + \sum_{i=1}^q \beta_i \sigma_{t-i}^2, \\ \text{APARCH: } \sigma_t^\delta &= \omega + \sum_{i=1}^p \alpha_i (|\varepsilon_{t-i}| - \gamma_i \varepsilon_{t-i})^\delta + \sum_{j=1}^q \beta_j \sigma_{t-j}^\delta, \end{aligned} \quad (1)$$

ahol σ_t a feltételes volatilitás, ε_{t-i}^2 az innovációtvagysokkot reprezentáló normális eloszlású hibabag, S_{t-i}^- a negatív értéket felvevő hibabag által jelentkező aszimmetriát reprezentáló dummy változó. A szelekció során a bayesiánus információs kritérium (BIC) minimumát keressük a homoszkedasztikus kimenettel rendelkező modellek között *Cappiello et al. (2006)* nyomán.

Végül dinamikus feltételes korrelációt (DCC–GARCH) illesztettünk a mintára (2), hogy felmérjük a bitcoinnal való együttmozgásukat.

$$\sigma_{it}^2 = \omega_i + \sum_{p=1}^{P_i} \alpha_{ip} e_{it-p}^2 + \sum_{q=1}^{Q_i} \beta_{iq} \sigma_{it-q}^2, \quad (2)$$

³⁸ Az adatok forrása: <http://stooq.com>.

A szükséges számításokat és modellillesztéseket Matlab 2014a szoftverrel, a *Kevin-Sheppard* által kifejlesztett MFE és UCSD toolboxok használatával végeztük el.

4.2. EREDMÉNYEK

Ideális esetben egy pénz- és tőkepiaci eszköz esetében elvárható, hogy nulla várható érték mellett aszimmetriát és 3-hoz közeli csúcosságot mutasson normális eloszlás, autokorreláció hiánya, homoszkedaszticitás és stacionaritás mellett (Kiss, 2017). Ezek az elvárások a gyakorlatban a logaritmikusan differenciáltak esetében jellemzően csak a várható értékre és a stacionaritásra szoktak teljesülni (2. táblázat). Mint látható, a kakaót és az EUR/USD-t leszámítva, egyik eszköz sem rendelkezik normális eloszlással (*Jarque-Bera* $p > 0,05$), miközben kiugróan magas csúcosságot (vastagfarkúságot) találhatunk a német és svájci 10 éves kötvényhozamok, a svájci tőzsdeindex, a svájci frank és az indonéz rúpia esetében. Emellett megjelenik az autokorreláció és a heteroszkedaszticitás is számos esetben.

Megállapítható tehát, hogy nincs egyik eszközkategória esetében sem olyan tipikus alap statisztikai tulajdonság, amely más kategóriákra ne lenne jellemző – leszámítva a svájci illetőségű eszközöket. Az ideális elvárásokhoz legközelebb a kakaó helyezkedik el, megfelelően valamennyi kritériumnak. A Bitcoin ellenben ugyanúgy aszimmetriát, vastagfarkúságot, nem normális eloszlást és autokorrelációt mutat, mint például a jüan.

2. táblázat

Különböző eszközök alapstatisztikái

Eszköz- átlag	Momentumok				Normális Eloszlás	Auto- korreláció	Hetero- szkedasz- ticitás	Unitroot	
	szó- rás	ferde- ség	csúcsos- ság	Jarque-B p	Ljung-B p	Arch-LM p	ADF p		
Kötvény	us10y	0,00	0,05	0,40	3,77	0,00	0,02	0,04	0,00
	de10y	-0,01	0,44	-0,26	35,96	0,00	0,00	0,11	0,00
	cn10y	0,00	0,02	-0,01	4,47	0,00	0,78	0,86	0,00
	ch10y	-0,01	0,41	-1,48	20,47	0,00	0,00	0,33	0,00
	tr10y	0,00	0,03	0,70	7,35	0,00	0,10	0,32	0,00
	id10y	0,00	0,03	0,14	4,50	0,00	0,25	0,33	0,00
Részvény	Sp500	0,00	0,02	-0,41	5,29	0,00	0,16	0,36	0,00
	DAX	0,00	0,03	-0,60	5,50	0,00	0,45	0,62	0,00
	SHC	0,00	0,03	-0,76	6,82	0,00	0,06	0,37	0,00
	SMI	0,00	0,02	-1,46	10,50	0,00	0,32	0,35	0,00
	XU100	0,00	0,03	-0,60	4,45	0,00	0,31	0,41	0,00
JCI	0,00	0,02	-0,47	6,81	0,00	0,03	0,18	0,00	

Eszköz- átlag		Momentumok				Normális	Auto-	Hetero-	Unitroot
		szórás	ferdeség	csúcsosság	Jarque-B p	Eloszlás	korreláció	szkedaszticitás	
						Ljung-B p	Arch-LM p	ADF p	
Deviza (USD)	BTC	0,03	0,16	0,89	8,09	0,00	0,00	0,07	0,00
	eur	0,00	0,01	-0,21	3,43	0,06	0,84	0,86	0,00
	cny	0,00	0,01	-0,55	6,65	0,00	0,00	0,00	0,00
	chf	0,00	0,02	1,79	30,70	0,00	0,07	0,16	0,00
	try	0,00	0,02	0,04	3,73	0,02	0,45	0,53	0,00
	idr	0,00	0,01	0,42	13,82	0,00	0,07	0,08	0,00
Nyersanyag	arany	0,00	0,02	-0,43	4,18	0,00	0,18	0,16	0,00
	lítium	0,00	0,03	-0,58	5,87	0,00	0,18	0,24	0,00
	brent	0,00	0,04	-0,24	4,86	0,00	0,20	0,33	0,00
	búza	0,00	0,04	0,42	4,36	0,00	0,16	0,23	0,00
	kakaó	0,00	0,03	0,02	3,22	0,71	0,26	0,29	0,00
	vix	0,00	0,15	0,54	5,72	0,00	0,00	0,00	0,00

Forrás: saját számítás, MFE toolbox

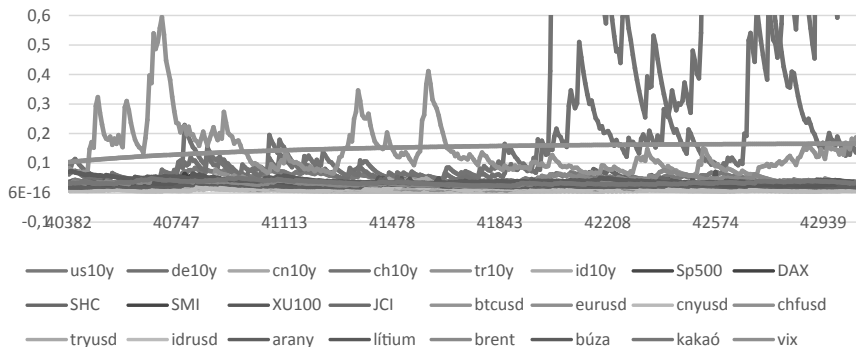
A következő lépésben Cappiello et al. (2006) nyomán megvizsgáltuk, hogy a bayesiánus információs kritérium (BIC) figyelembevételével mellett a GARCH-modellcsalád mely tagja és milyen p , α , q késleltetések mellett illeszthető úgy az idősorokra, hogy homoszkedasztikus kimenetet kapjunk (3. táblázat). Ebben az esetben már egyértelmű különbségeket találni az egyes eszköztípusok között: a 10 éves kötvényhozamok esetében szükség van a legkomolyabb APARCH-modellre, továbbá a svájci eszközök csak aszimmetrikus GARCH-modellekkel írhatóak le. Eközben a nyersanyagok esetében a legegyszerűbb GARCH(1,1)-es modell képes illusztrálni azt a folyamatot, amelynek során pusztán az előző heti volatilitás határozza meg a aktuális heti árfolyamot, 90% körüli súllyal. A részvény- és devizapiacokra ellenben az aszimmetrikus TAR(1,1,1) modellek voltak a jellemzőek, ahol jellemzően az árfolyam gyengülése vezetett a magasabb volatilitáshoz. Speciális helyzetben vagyunk a német és svájci kötvényhozamok esetében, ahol a hozam növekedése eredményezett magasabb volatilitást. Ugyanígy a devizák esetében a svájci frank és a bitcoin kapcsán lehetett hasonló eredményre jutni – az árfolyam erősödésével párhuzamosan nőtt a volatilitás is.

3. táblázat**A volatilitásmodellek jellemzői**

Eszköz	us10y	de10y	cn10y	ch10y	tr10y	id10y
konstans	0,00	0,00	0,00	0,00	0,00	0,00
alfa	0,00	0,13	0,13	0,08	0,12	0,17
gamma	0,11	-1,00		-1,00		
béta	0,95	0,84	0,60	0,75	0,83	0,76
nu		1,60		2,81		
modell	TARCH(1,1,1)	APARCH(1,1,1)	GARCH(1,1)	APARCH(1,1,1)	GARCH(1,1)	GARCH(1,1)
eszköz	Sp500	DAX	SHC	SMI	XU100	JCI
konstans	0,00	0,00	0,00	0,00	0,00	0,00
alfa	0,00	0,00	0,14	0,00	0,19	0,09
gamma	0,24	0,18		0,14		0,26
béta	0,83	0,86	0,86	0,84	0,11	0,66
nu						
modell	TARCH(1,1,1)	TARCH(1,1,1)	GARCH(1,1)	TARCH(1,1,1)	GARCH(1,1)	TARCH(1,1,1)
eszköz	bitusd	eurusd	cnyusd	chfusd	tryusd	idrusd
konstans	0,01	0,00	0,00	0,01	0,00	0,00
alfa	0,28	0,07	0,13	0,15	0,00	0,00
gamma	-0,18		0,00	-0,60	0,09	0,30
béta	0,81	0,92	0,83	0,84	0,90	0,84
nu				0,30		
modell	TARCH(1,1,1)	GARCH(1,1)	TARCH(1,1,1)	APARCH(1,1,1)	TARCH(1,1,1)	TARCH(1,1,1)
eszköz	arany	lítium	brent	búza	kakaó	vix
konstans	0,00	0,00	0,00	0,00	0,00	0,00
alfa	0,06	0,08	0,09	0,04	0,05	0,00
gamma						
béta	0,87	0,87	0,90	0,93	0,93	0,99
nu						
modell	GARCH(1,1)	GARCH(1,1)	GARCH(1,1)	GARCH(1,1)	GARCH(1,1)	GARCH(1,1)

Forrás: saját számítás, UCSD toolbox

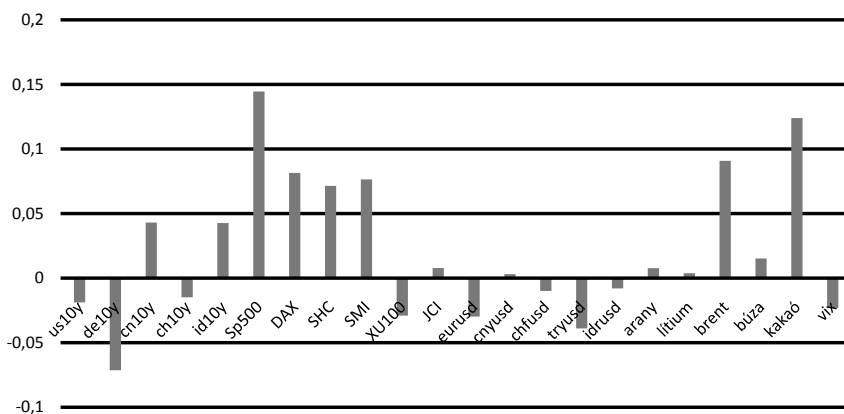
A német és svájci kötvényhozamok feltételes volatilitása kiugróan magas volt 2015 év elejét követően (*10. ábra*). Ezt leszámítva azonban egyedül a bitcoin esetében mérhető a piaci átlagot messze meghaladó mértékű volatilitás.

10. ábra**Feltételes volatilitás értékei**

Megjegyzés: a német és a svájci kötvényhozamok levágásra kerültek a könnyebb áttekinthetőség kedvéért.

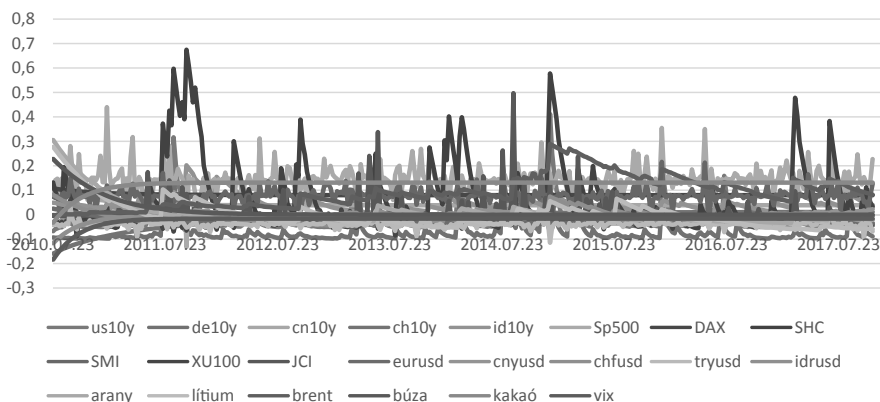
Forrás: saját számítás, UCSD toolbox

A Bitcoin esetében a szakirodalom hagyományosan a más eszközökkel való együttmozgás hiányát szokta kiemelni. A dinamikus feltételes korreláció átlagos értékeinek tükrében ez az állítás elfogadható (11. ábra).

11. ábra**Feltételes dinamikus korreláció (DCC-GARCH) átlagos értékei**

Forrás: saját számítás, UCSD toolbox

A korreláció időbeli alakulását szemlélve azonban szembetűnően előfordultak a múltban olyan esetek, amikor hol a kínai, hol az S&P500 vagy az indonéz tőzsdeindexekkel szemben mutatott rövid távon közepes együttmozgást (12. ábra).

12. ábra**Feltételes dinamikusan korreláció (DCC–GARCH) értékei**

Forrás: saját számítás, UCSD toolbox

5. ÖSSZEFOGLALÁS HELYETT

A 21. század második évtizedének utolsó éveiben járva, a digitalizáció és a bigdata korában, amikor a kávéfőzőnket vagy lassan bármelyik háztartási készülékünket okostelefonunkról távvezérelhetjük; amikor a tradicionális szolgáltatók a bankoktól az államigazgatáson keresztül egészen az oktatásig egyre gyakrabban kerülnek digitálisan kapcsolatba az ügyfelekkel, és életünk eseményeinek jelentős részét a különböző felhőszolgáltatásokon és szociális közösségi oldalakon keresztül digitalizáljuk és osztjuk meg egymással, a csupán az informatikai kódok mögött rejtőzködő pénz koncepciója egy szükséges következménye a digitalizálódó társadalmunknak.

Bár sokak előtt ismeretlen tény, de a 2007–2009-es globális pénzügyi és realgazdasági világválság borús és fájdalmas következményei, valamint a felelőtlenül működő és elégtelenül szabályozott bankrendszert megóvni hivatott mentőcsomagok fordulópontot hoztak a digitális pénzek világában. Noha a válság előtti években is léteztek már digitalizált pénzek, a közös bennük a központi elszámoló fél létezése volt.

Satoshi Nakamoto forradalmian új megoldási javaslata e központi félnek az egyenletből való kihagyása volt. Valójában már a korábbi évtizedek során is létező technológiákat ötvöztött igen innovatív módon. A blokklánc elosztott, decentralizált adatbázis-koncepciója valójában a peer-to-peer hálózat (P2P), a *nyilvános kulcsú*

infrastruktúrán (PKI) alapuló titkosítási rendszer, valamint a *kriptografikus hash* eljárás működésén alapszik.³⁹

A Satoshi által létrehozott bitcoin volt az első a kriptoeszközök sorában, amely valószínűsítő átalakulást indított meg az elszámolási rendszerek világában. Habár a bankok szempontjából a kriptovaluták feltűnése még nem jelent valódi kihívást napjainkban, idővel, ha a technológia adaptációja szélesebb körben elfogadottá válik, valamint a jelenlegi gyermekbetegségeken sikerül túljutnia, a kriptoeszközök csoportja megkerülhetetlen entitássá fog válni a pénzügyek világában.

A kriptovaluták piacának⁴⁰ mind az eszközök száma, mind az árak tekintetében tapasztalt, extrém gyors növekedése és drasztikus visszaesése, valamint a pénzügyi rendszert érintő kihívása arra ösztönzi a pénzügyi szereplőket és szabályozó hatóságokat, hogy közelebbről vizsgálják e forradalmian új piac működését. Fennállhat annak a veszélye, hogy azok az intézmények, amelyek figyelmen kívül hagyják e technológia térhódítását, hosszú távon kimaradnak a versenyből.

Nem kétséges, hogy a kriptovaluta mint új eszközcsoport, jelenleg az életgörbe kezdeti szakaszán jár, így véleményünk szerint egyetlen olvasó sem késett el ahhoz, hogy a blokklánc-technológia nyújtotta lehetőségeket megismerje és időben kiaknázza. Osztjuk azt a véleményt, hogy ezen új innovatív, elosztott főkönyvi technológia (*distributed ledger technology*⁴¹) az általa nyújtott infrastruktúrával és folyamatokkal egyszerűbbé és hatékonyabbá teheti a pénzügyek világát, valamint a már meglévő technológiákkal együtt pénzügyi szolgáltatások új generációjának alapját képezi majd. Itt persze nem lehet megállni, hiszen a blokklánc nyújtotta lehetőségek kiaknázásával eme innovatív technológia a biztosítási piactól kezdve a földhivatali nyilvántartáson át az egészségügyi szektorral bezárólag megannyi területen hozhat komoly változásokat.

Végzőként a Nobel-díjas keynesiánus közgazdász, *Paul Krugman* 1998-ban megjelent szavait idézzük: „*Körülbelül úgy 2005-re mindenki számára nyilvánvalóvá válik majd, hogy az internetnek nem lesz nagyobb hatása a gazdaságra, mint egy faxgépnak*”⁴² (*The Red Herring*, 1998). Nyilvánvaló, hogy Krugman nagyot tévedett e rendkívül elhamarkodott kijelentésével. Véleményünk szerint pedig napjaink

39 Az első P2P-hálózat a Napster fájlmegosztó szolgáltatásán keresztül vált ismertté 1999 júniusában. A PKI, amely lehetővé teszi a tranzakciók titkosítását két egymással bizalmatlan fél között, és amely például bevezette az tranzakciók időbélyegzését, már az 1990-es évek óta ismert technológia. (A legegyszerűbb PKI-implementációkkal szinte bizonyosan találkoztunk már mindannyian: ezek egyike az SSL-titkosítás). Végezetül a kriptografikus hash (pl. az ECC, Elliptic Curve Cryptography) már 1985 óta létező hitelesítési eljárás, azonban csupán az évezredforduló során kezdték szélesebb körben felhasználni, például a mobiltelefonok biztonságtechnikai tervezése során.

40 Napjainkban már több mint 1500 kriptoeszközt regisztrálnak.

41 Az elosztott főkönyvi technológia a blokklánc-technológia szinonimája.

42 <http://www.digitaljournal.com/article/346996>.

blokklánc-technológiája legalább akkora lehetőséget és kihívást ígér a jövő számára, mint az 1990-es években megjelenő internet. Éppen ezért is azt javasoljuk: mindenki legyen résen!

HIVATKOZÁSOK

- BURNISKE C. – WHITE A. (2017): Bitcoin: Rising the bell for a new asset class. *Research White Paper*, ARK Invest Research & Coinbase Inc.
- CAPPIELLO, L. – ENGLE, R. F. – SHEPPARD, K. (2006): Asymmetric Dynamics in the Correlations of Global Equity and Bond Returns. *Journal of Financial Econometrics* 4, 537–572. o., CoinDesk: State of Blockchain 2018, 2017-Q4 Report, <http://www.coindesk.com>.
- Cointelegraph* (2018): Exponential Growth: Cryptocurrency Exchanges Are Adding 100,000+ Users Per Day, 2018.01.07, <https://cointelegraph.com/news/exponential-growth-cryptocurrency-exchanges-are-adding-100000-users-per-day>.
- HACKETT, R. – WIECZNER, J. (2017): How High Can Bitcoin's Price Go in 2018? *Fortune*, 2017.12.21, <http://fortune.com/2017/12/21/bitcoin-price-value-prediction-bubble/>.
- FODOR D. – SPEISER F. (2014): *Autóipari beágyazott rendszerek*. TÁMOP-4.1.2.A/1-11/1-2011-0042, Veszprém, Pannon Egyetem.
- GREER, R. J. (1997): What is an Asset Class, Anyway? *Journal of Portfolio Management* 23, 86–91., <http://dx.doi.org/10.3905/jpm.23.2.86>.
- KISS, G. D. (2017): *Volatilitás, extrém elmozdulások és tőkepiaci fertőzések*. Szeged, JATEPress.
- TRUBETSKOY, G. (2017): Electricity Cost of 1 Bitcoin (Sep 2017)., <https://grisha.org/blog/2017/09/28/electricity-cost-of-1-bitcoin/>.
- The Telegraph* (2017): Bitcoin mania: Google's top searches in 2017 dominated by digital currency craze. 2017.12.13, <http://www.telegraph.co.uk/technology/2017/12/13/bitcoin-mania-googles-top-searches-2017-dominated-digital-currency>.