MIRE JÓ, ÉS MIRE NEM JÓ A BLOCKCHAIN?

Sík Zoltán Nándor[1]

Abstract

A cikkben a blockchain technológia alkalmazásának érveit és ellenérveit taglalja a szerző, elsősorban az adott blockchain rendszer szereplői szerinti felosztás szemszögéből. Mindemellett kitér az állami szerepkörökre, a blockchain technológia bevezetésével megoldható társadalmi problémákra, valamint a blockchain-en alapuló rendszerek által generált társadalmi problémákra, illetve ezek kormányzati kezelési módjaira, ezek hiányára, problémáira.

What is the good of blockchain for, and what it isn't good for?

In this article, the author discusses the pros and cons of using blockchain technology, primarily categorising the possible using the blockchain regarding the stakeholders, and actors. Also addresses the role of the state, the social problems that can be solved by using blockchain technology, the social problems generated, the ways of handling them by the government, the lack of handling and the problems caused by the blockchain itself.

1. Internet és dotkom

A blockchain (magyarul a blokklánc) az utóbbi pár év legfelkapottabb informatika kifejezése, mivel jelentőségét ahhoz hasonlítják, mint amikor az Internet megjelent (pontosabban, amikor az Internetet 1991-ben megnyitották mindenki számára). Az Internet korszakalkotó, *„világmegváltó"* jelentőségét lehet ugyan vitatni, de tény, hogy a mai fiatal generáció nem tud meglenni nélküle, egyszerűen el sem tudják képzelni, hogy hogy működött a világ Internet és okostelefonok nélkül. Így nem is nem véletlenül hívják őket Youtube generációnak, vagy *„C"* generációnak (a creation, curation, connection, community szavak kezdőbetűjéről elnevezve).[2]

Mindemellett megjegyzendő, hogy a 2000-es évek elején az ún. dotkom (*„.com"*) válság egyik kiváltó okaként is az Internetet teszik felelőssé, de ha visszatekintünk, azon cégek némelyike, amely érintett volt a dotkom válságban, ma nyertesként a világ óriás cégei közé tartozik (pl. az Apple, az Amazon, vagy a Facebook).[3] Nézzük meg ezeknek a cégeknek a piaci kapitalizációját a dotkom válság, más néven dotkom lufi idején, amikor *„fel voltak pumpálva"*, és nézzük meg ma, amikor nagyságrendekkel többet érnek, mint a 2000-es évek elején.

2. Blockchain

A blockchain[4] is hasonló utat kezd bejárni, mint anno az Internet, korszakalkotó, világmegváltó kifejezésekkel illetik. Az első blockchain alapokon nyugvó megoldás, 2009-es indulással a Bitcoin fizetési rendszer[5] volt, ami gyakorlatilag, és kis túlzással speciális elektronikus pénzként (e-money) is felfogható. Mivel magát a blockchain-t is ez a rendszer vezette be, ezért, ezen specialitása miatt nem is e-money-nak, hanem cryptocurrency-nek (kriptopénznek) nevezik. A Bitcoin rendszer után a következő jelentős az Ethereum rendszer bevezetése volt, amely már nem is annyira a fizetési eszközre, nem a tranzakciókra fókuszált, hanem a blockchain által biztosított informatikai előnyökre, beleértve az u.n. smart contract-okat (okosszerződéseket), illetve ez alapján az u.n.

[1] A szerző jogi szakokleveles villamosmérnök, MBA és politikai szakértői diplomával, valamint tőzsde szakvizsgával és brókervizsgával rendelkezik. Informatikai kormánybiztos 2000-2002-ig, a Nemzeti Hírközlési és Informatikai Tanács alelnöke 2015-2019-ig. Jelenleg a Magyar Államkincstár és a Kormányzati Informatikai Fejlesztési Ügynökség elnöki tanácsadója, információbiztonsági és blockchain szakértő.

[2] Pl. Introducing Gen C: the Youtube Generation: https://www.thinkwithgoogle.com/consumer-insights/introducing-gen-c-the-youtube-generation/ (lekérdezés ideje: 2019. 07. 30.)

[3] 4 Chart That Show This Tech Boom Is No Dot-Com Bubble: https://www.thecapitalideas.com/articles/4-charts-show-tech-boom-not-bubble (lekérdezés ideje: 2019. 07. 30.)

[4] Pontosabban a blokchain-re, mint új információtechnológiai működési módra alapozódó megoldások.

[5] Ez a rendszer *Satoshi Nakamoto* ötlete, aki ilyen néven nem létezik (egyesek szerint a név több embert takar).

tokenizációt. Az Ethereum rendszert magát ezért is nevezik Ethereum Virtual Machine-nak (EVM). Mára pedig gombamód szaporodnak a fizetési mind a cryptocurrency-k, ill. közkeletűbben coin-ok (érmék), mind a tokenek. Miután azonban a token-ek is értéket képviselnek, sokan ezeket is egy kalap alá veszik a cryptocurrency-kkel.

A smart contract-ok mindemellett sok egyéb, sarkalatos funkciót tesznek lehetővé a blockchain alapú rendszereknél. Ezek gyakorlatilag szoftverek, amelyeket a blockchain alapú rendszer végrehajt. Ezekkel a szoftverekkel pedig igen sokféle szolgáltatás építhető, a blockchain ezek segítségével fordul át fizetési rendszerből általános alkalmazásokat futtatni képes rendszerekké. A fent említett tokenek pedig ezen alkalmazások egyes funkciói igénybevételének az ára. Pont úgy viselkednek, mint az autó és a benzin: egy adott autó fogyasztása legyen pl. 10 liter/100 km. A crypto világban ez azt jelenti, hogy pl. 100 darab programlépést lehet végrehajtani 10 darab token ráfordításával (ezt amúgy az Ethereum rendszerben ráadásul *„gas"*-nak, benzinnek nevezik, pont a fenti példa kapcsán). Azonban ahogy a benzin ára is változik, úgy a *„gas"* ára is változik a kereslet-kínálat függvényében. Így, bár az Ethereum *„pénze"*, az ether nem a pénzhez hasonló, mint pl. a bitcoin, de mégis értéket képvisel, mintha pl. egy marmonkanna benzint adnánk egy szoftver X ideig, vagy Y programlépésig való végrehajtásáért.

3. Crypto-tőzsdék, cryptoasset-ek

Ezek, a csak a digitális világban létező értéket képviselő *„valamik"* ezért kereskedelmet is lehetővé tesznek, amelyeket ún. crypto-tőzsdéken bonyolítanak. A *„valami"*-k gyűjtőfogalom a mai napig nincs definíciószerűen tisztázva, leginkább a cryptoasset (kriptoeszköz) elnevezést használják rá.

A crypto-tőzsdék pedig igen hasonlóan működnek a hagyományos tőzsdékkel, pár eltéréssel. A crypto-tőzsdéken csak craptoasset-ekkel lehet kereskedni, de bárki kereskedhet, nem kell hozzá pl. brókervizsga, nem csak koncentrált, azaz egyvalaki által üzemeltetett crypto-tőzsdék vannak, hanem elosztott tőzsdék is (DEX-ek), és nincs direkt *„átjárás"* a cryptotőzsdéken kereskedett cryptoasset-ek, valamint a fizikai világban létező pénzeszközök (ún. fiat-ok), és/vagy egyéb fizikai értéket megtestesítő eszközök (például arany) között. Vannak kísérletek az egyszerű átjárás, azaz a pénzügyi befektetés/befizetés, illetve kivétel megkönnyítésére, de ez leginkább crypto-ra szakosodott pénzváltóknál lehetséges (például Shapeshift, Peaceful, CEX.IO).

4. Stablecoin-ok

A cryprotőzsdék egyike-másika pedig kitalált egy-egy fizikai világban létező pénzhez kötött cryptocurrency-t is. Ezek között első volt a Bitfinex nevű tőzsde USD tether (USDT) nevű cryptocurrency-je, amelynél 1USD egyenlő volt 1USDT-vel, és amennyi USDT létezik, annyi USD van elhelyezve ténylegesen létező bankoknál. Mivel így ezen cryptocurrency-k értéke a hozzákötött fiat-hoz, vagy más, értéket képviselő eszközhöz (pl. arany) képest nem változik, ezért ezeket ún. stablecoin-oknak is nevezik. Ezzel a módszerrel a stablecoin-ok nem olyan volatilisek, azaz nem érzékenyek az árfolyam ingadozásokra, mint a többi cryptoasset (csak a fiat-ok, vagy más eszközök egymás közti árfolyamváltozásától függ).

A blockchain technológiát tekintve, amit ezek a cryptoasset-ek használnak, több lényeges szempontot ki kell emelnünk. Arról, hogy ezek csak a digitális világban léteznek, már volt szó. További tulajdonságuk, hogy nincs központjuk (kivéve a később részletesebben kifejtendő, fenti stablecoin-ok és speciális cryptocurrency-k esetét), azaz a világon bárki csatlakozhat egy ilyen rendszerhez egyenrangú félként. A cryptoasset-ek közti tranzakciókat is központ nélkül ellenőrzik, szintén egyenrangú felek, akiket semmi más nem köt egy-egy tranzakció valósnak való elismeréséhez, mint az adott, blockchain alapú rendszer matematikai algoritmusa. Ezt az algoritmust minden résztvevő kénytelen betartani, kénytelen az algoritmus megbízhatóságában, *„erejében"* megbízni, egyébként rövid úton kikerül a rendszerből, hiszen a többség, mint résztvevőt kizárja.

5. Adatbázisok

A blockchain mindazonáltal egy ma biztonságosnak tartott rendszer, amely eltérő a banki, vagy egyéb más adatbázisoktól. A banki adatbázisokat tekintve a bankoknál lévő számlánkon lévő pénzt az adott bank egy sima adatbázisban tárolja, mint egyszerű bitsorozatot. A pénznek fizikai megjelenése csak készpénz befizetésekor, illetve kifizetésekor van (még bankkártyás tranzakciónál sincs, hiszen ott a bankkártya csak a hozzáférést biztosító, authentikációs eszköz, és a közhiedelemmel ellentétben nem a bankkártyán van pénz, hanem akkor is a banknál, szintén bitsorozat formájában).

Léteznek ún. elosztott adatbázisok, ahol az adatbázisok egyes darabjai fizikailag máshol vannak (akár geográfiailag is). Ezek egy részét a Distributed Ledger (DL) kifejezéssel illetik, az ehhez tartozó informatikai technológiát pedig Distributed Ledger Technology (DLT) néven (magyarul elosztott főkönyvi technológia). Sőt, vannak ún. replikált adatbázisok is, amikor is ugyanaz a teljes adatbázis több fizikailag elkülönült helyen jelenik meg, többnyire a biztonság növelése céljából (gondoljunk *például* az Apple iCloud-jára, vagy a Google Drive-ra, amelyek a telefonon lévő adataink informatikai felhőben lévő replikátumai, backup-jai (mentései), amelyek a telefonunkkal folyamatosan szinkronizálva vannak).

6. A blockchain megszorításai

A blockchain ugyanakkor egy olyan DL (esetenként DLT néven is hívják), amely további megszigorításokkal rendelkezik. Az elsőről már volt szó, ami nem igazi megszorítás, azaz, hogy a blockchain replikált adatbázis. Ezt a replikált adatbázist minden teljes jogú, a rendszerben részvevő partner, azaz node (csomópont) tárolja. Természetesen vannak

további felhasználók, akik szintén teljes joggal igénybe veszik a rendszer szolgáltatásait, de nem kívánnak csomópontok lenni, csak pl. tranzakciókat végrehajtani, vagy smart contract-okat futtatni.

Az igazi megszorítás azonban az, hogy minden felhasználó egyenrangú, és általában nem is bíznak meg egymásban, hiszen nem is ismerik egymást. További megszorítás pedig az, ami a használt informatikai szabályrendszeren alapul (és ennek szigorú matematikai alapjai vannak), amelyet mindenki el kell, hogy fogadjon, ha a rendszerben részt akar venni, és ez szükségképpen konszenzust teremt az egyes felhasználók között (egészen pontosan a node-ok között). Miután a node-ok sem bíznak meg egymásban, mindazonáltal egyenrangúak, ezért ez a konszenzus a legtöbbször kényszerkonszenzus, amit a fent említett matematikai alapokon nyugvó algoritmus kényszerít ki.

Megszorítás ezen felül az a körülmény, amiből maga a blockchain kifejezés is származik, mégpedig az, hogy a (node-ok által replikált) adatbázis elemei adott méretű blokkokba vannak rendezve, és ezek a blokkok megszakíthatatlan láncot alkotnak.

Végül a megszorítások közt említendő, hogy az adott matematikai algoritmus kriptográfiai elveken nyugszik, ami egyébként a blockchain legbonyolultabb eleme.

A fentiekből látszik, hogy miután a blockchain alapértelmezése a központnélküliség (decentralizáltság), ezért, ha pl. cryptocurrency-ről van szó, akkor a *„pénz"* kibocsátását valahogy meg kell oldani, hiszen nincs központi bank, ami ezt megtenné. Ezt lehet úgy tenni, hogy az egyes node-ok folyamatosan bocsátják ki a cryptocurrency-t (például a Bitcoin rendszerben), illetve úgy, hogy a blockchain üzemelésének kezdő időpontjában (az ún. genezis blokk létrehozásakor) már megtörténik a pénzkibocsátás (pl. a NEO blockchain rendszerénél), azaz a genezis blokk már tartalmazza az összes cryptocurrency-t. Az előbbit ún. bányászható (mineable) cryptoasset-eknek nevezik[6], az utóbbit pedig nem bányászhatónak (non-mineable)[7].

7. Szabadság és egyenlőség

Más kérdés azonban a fent említett stablecoin-ok esete, amiről már volt szó a Bitfniex által kibocsátott USDT kapcsán. Noha van már sok stablecoin, például a TrueUSD, a PAX vagy az USDC[8], ezek mind egy-egy kitüntetett kibocsátóhoz kötődik. Más szóval, ebben az esetben nem minden résztvevő egyenlő, hiszen a stablecoin kibocsátója vállal valamilyen kötelezettséget a stablecoin árfolyamának fixen tartására. Orwell szavaival élve *„minden állat egyenlő, de egyes állatok egyenlőbbek a többinél"*, azaz sérül az egyenlőség elve (nem minden résztvevő egyenrangú fél).

Míg a Bitcoin rendszer alapja alapvetően bankoktól, mint trusted third party-któl (megbízható harmadik felektől) való függetlenség volt, más blockchain alapja pedig mindenféle más, hasonló, megbízható harmadik féltől való függetlenség. Így az egyenlőség, sőt valamiféle szabadság biztosítása a cél. Azonban, amint a fentiekből is látszik, ez nem mindig tartható fenn.

Már említettük az ún. mineable cryptocurrency-ket, ahol a pénzkibocsátás is elosztott módon megy. Ez nagy vonalakban úgy történik, hogy az a node, amely sikeresen előállítja az adatbázis következő blokkját, *„láncszemét"*, jutalomban részesül (a tranzakciókból adódó kis összegű könyvelési díjakon felül). Azaz a semmiből írhat magának jóvá adott mennyiségű cryptocurrency-t, és ez így rajta keresztül kerül forgalomba. Miután azonban a cryptocurrency-k (és a tokenek is) értéket képviselnek a fizikai világban is, ezért minden ilyen node-nak az az érdeke, hogy ő állítsa elő sikeresen a következő blokkot (ezt nevezik mining-nek, bányászásnak). Az adott blokk sikeres előállítását a matematikai algoritmus alapján a többi node kénytelen elismerni (ezért is a kényszerkonszenzus) és a blokkot, mint az egyetlen érvényes, a láncban következő blokkot elfogadni (validálni).

Mivel a blockchain algoritmusában a blokk sikeres előállítása ez egy igen nehezen megoldható kriptográfiai feladat, nem olyan könnyű a következő blokk előállítása, igen nagy számítási kapacitás szükséges hozzá. Ennek a szükséges kapacitásnak az összegyűjtése minden node-nak másképpen sikerül, ezért akinél több az ilyen kapacitás, nagyobb valószínűséggel állítja elő a következő blokkot, így a nagyobb kapacitású node *„egyenlőbb"* a többinél. Ennek extrém esete, amikor egy adott node annyira eluralkodik a rendszeren, hogy több mint 50 % valószínűséggel ő nyeri a blokk előállítási versenyt.[9] Így akár azt is megteheti, hogy felülírja az informatikai szabályban lefektetetteket, és ő diktálja, hogy melyek az új szabályok. Azaz tőle függ, hogy a következő blokk milyen algoritmus alapján áll elő, hiszen az ő validálása nélkül az adott blokk nem érvényes.[10] Ebből pedig az következik, hogy az adott node már nem csak egyenlőbb a többinél, hanem diktátorrá válik. Így ezekben az esetekben szintén sérül az egyenlőség elve.

A szabadság és az egyenlőség elve tehát nem férhet meg egymással, bár az eredeti, blockchain alapú rendszerek pont ezt tűzték ki célul. Hiszen, ha minden résztvevő szabad, akkor azt csinál a rendszer matematikai algoritmusainak keretén belül, amit akar. Ha van elég tőkéje, akár magához is tudja ragadni a *„hatalmat"*. Így viszont nem lesz mindenki egyenlő. Ha viszont az egyenlőség elvét tartjuk elsődlegesnek, akkor nem csinálhat mindenki azt, amit akar, hiszen valakinek/valakiknek biztosítaniuk kell, hogy az egyenlőség fennmaradjon. Tehát a szabadság elve sérül. Ez a megállapítás nagy valószínűséggel nem csak a blockchainre igaz, a szabadság és az egyenlőség minden ökoszisztémában fordítottan arányos.

[6] Ezeket a kifejezéseket az ún. Proof-of-Work (PoW-munkabizonyíték) alapú rendszereknél használják

[7] Megjegyzendő, hogy vannak olyan rendszerek, ahol a minting, illetve a forging kifejezések használtak, az ún. Proof-of-Stake (PoS-érdekeltség alapú) rendszereknél.

[8] Lásd pl. https://www.binance.vision/glossary/stablecoin (lekérdezés ideje: 2019. 07. 30.)

[9] Ez az u.n. 51% attack a PoW rendszereknél

[10] A PoS rendszereknél általában nem 51%, hanem 66% feletti ez a szükséges arány, hogy a konszenzust sikeresen meg lehessen törni.

8. Hype

Mindezeket összevetve nem lehet csodálkozni azon, hogy a blockchain úgy „*en bloc*" a Gartner Group Hype Cycle diagramján[11] már túl van a csúcson. Most éppen a kiábrándulás szakaszát éljük bár egyes speciális blockchain megoldások még csak kúsznak fel a csúcsra.

Mára általánosságban nem igaz az, hogy a blockchain mindenre jó, a hitelesség, az átláthatóság, az információ megbízhatóságának záloga. Végül a blockchain is meg fogja találni a helyét az innovációk között. Bár a szerző fenntartja azon álláspontját, hogy mára a technológiai innovációk a társadalom minden szegmensét érintik, azaz nem csak az infokommunikációhoz, illetve más, az adott innovációhoz köthető technológia területét. Anélkül, hogy a fentiekből túlságosan messzemenő következtetéseket vonnánk le, megjegyzendő, hogy a blockchain is, mint olyan, már első alkalmazásakor, a Bitcoin rendszer bevezetésekor sem az informatikához volt köthető, hanem a bankrendszer 2008-as válságán túllendülni akarók, a bankrendszer megbízhatóságát – jogosan – megkérdőjelezők innovációja, egy lehetséges függetlenedés, a bankoktól való menekülés útja. Sőt mára olyan fejlesztések vannak, amelyek sok más iparágat reformálnának meg, sőt vannak olyanok, akik a teljes gazdasági és politikai berendezkedés, az establishment reformját tűzik ki célul.

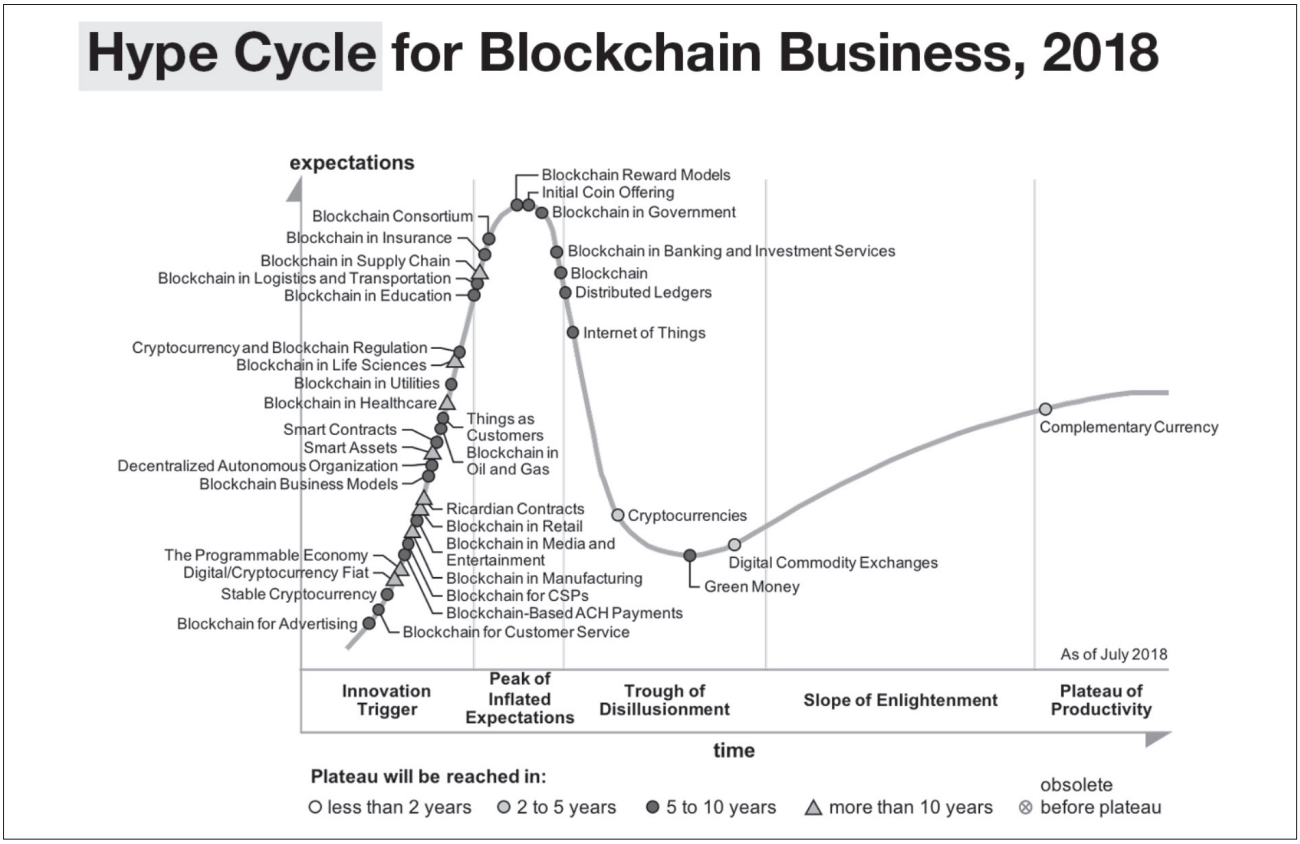
9. Használati esetek

Az ambiciózus elképzeléseket, terveket és projekteket látva mindazonáltal érdemes elgondolkozni azon, hogy mikor érdemes, és mikor nem érdemes használni a blockchain-t.

Ehhez lássuk először is, hogy milyen típusú blockchain rendszerek léteznek. Az egyik, amelyet a jelen írás már eddigiekben is vázolt, az ún. publikus blockchain. Ennek lényege a fentiek szerint, hogy nyitott, bárki, bármilyen feltétel nélkül csatlakozhat hozzá (természetesen a technológiai minimum feltétek adottak, azaz megfelelő hardver eszköz, valamilyen hálózati kapcsolat – többnyire internet –, valamint az adott blockchain szabályrendszerét maradéktalanul betartó szoftver, vagy szoftver komponens).

A másik blockchain rendszer az ún. permissioned (engedélyezett), más néven privát, vagy konzorciális blockchain[12]. Ebben nem mindenki vehet részt, függetlenül attól, hogy a technológiai feltételeknek megfelel, csak azok, akiket egy adott, a többieknél *„egyenlőbb"* körbe tartozók megengednek. Ezek lehetnek pénzügyi, vállalati, állami, NGO, országok közti, vagy más entitások által közösen használt blockchain-ek.

A kérdés megválaszolása, hogy mikor érdemes, és mikor nem érdemes használni blockchain alapú megoldást, nem bonyolult, azonban jól át kell gondolni. A publikus blockchain-ek alkalmazása azok definíciójából és a működés módjából



1. ábra
A Blockchain Hype cycle diagramja
Forrás: Gartner, Inc.

[11] Gartner: The Reality of Blockchain: https://www.gartner.com/smarterwithgartner/the-reality-of-blockchain/ (lekérdezés ideje: 2019. 07. 30.)

[12] Lásd pl. https://101blockchains.com/permissioned-blockchain/ (lekérdezés ideje: 2019. 07. 30.)

adódóan indokolt. Hiszen egyenrangú felek használják, egymást nem ismerik, szükségképpen nem bíznak egymásban, mégis együtt kell működniük egy-egy tranzakció és/vagy smart contract végrehajtásában. A smart contract-ok, mint programok által nyújtott szolgáltatásokat pedig a szereplők veszik igénybe (már amennyiben olyan szolgáltatást nyújt valaki a blockchain technológia segítségével, aminek értelme van). Mindemellett megjegyzendő, hogy a *„felek"* nem csak természetes személyek, sőt nem csak ezek csoportja, netán vállalatok lehetnek, de például informatikai eszközök, vagy ezek által vezérelt, vagy szabályozott eszközök [lásd például Internet of Things (IoT), önvezető autók, okos városok].

Más a kérdés a permissioned blockchain-ek esetében. Hol van az a határ, ahol érdemes a használat, és hol helyettesíthető egy egyszerű adatbázissal? Azoknál az intézményeknél, vállalatoknál, más entitásoknál, vagy ezek csoportjainál, amelyek alapvetően hierarchikusak, nyilvánvalóan nem érdemes blockchain alapú megoldáson gondolkozni. Hiszen ezek, a hierarchiából adódóan kénytelenek bízni egymásban, de legalább a magasabb szinten lévőben. A magasabb szint utasíthatja az alacsonyabb szinten lévőt, hogy annak mit kell tennie. Egy blockchain esetében tehát a felsőbb szint meg tudja mondani, hogy mely blokk elemeket kell, és melyeket nem kell, vagy milyen sorrendben kell beépíteni a blokkokba, azaz melyik az a *„valóság"*, amelyet hitelesnek kell elfogadni. Sőt, miután a felsőbb szint utasíthat, így, a már felépített blokkláncot is egy ponttól kezdve hatalmi szóval (és nem matematikai algoritmusokat használva) érvénytelennek nyilváníthatja. Ezután pedig egy adott blokktól kezdve más blokkok összeállítására késztetheti a hierarchiában alatta lévő node-okat. Azaz *„alternatív valóság"* létrehozására utasíthatja, csakúgy, mint Orwell 1984 című regényében az Igazság Minisztériumban (Minigaz), ahol a híreket visszamenőleg módosítják a Nagy Testvér akarata szerint, hogy most épp Eurázsia és Óceánia hadakozik Kelet-Ázsiával, esetleg Eurázsia és Kelet-Ázsia Óceániával. Így tehát ebben a blockchainben, és a benne tárolt adatokban nem lehet megbízni, semmivel sem nyújt többet, mint egy adatbázis.

Tovább menve, ha olyan szereplők alkalmaznak permissioned blockchain-t, akik függetlenek ugyan egymástól, de bíznak egymásban, szintén nem indokolt a blockchain használata. Hiszen, ha megbíznak egymásban mindannyian, akkor egy adatbázis használatában is megegyezhetnek.

A fenti két esetet tekintve megjegyzendő, hogy a résztvevőknek maximum attól kell tartaniuk, hogy vis maior, szabotázs stb. következtében sérül, kompromittálódik, vagy elérhetetlenné válik az adatbázis.[13] Ennek a problémának a megoldását a megfelelő információbiztonsági mechanizmusok, protokollok, kritikus infrastruktúra védelem stb. adják, nem a blockchain. Egy redundáns (replikált), megfelelően szinkronizált, fizikailag eltérő helyeken telepített, megfelelő mentési rendszereket, naplókat és az eléréshez használt authentikációt használó adatbázis pontosan elég erre. A blockchain technológia esetlegesen akkor lehet megfontolandó, ha nagyságrendekkel olcsóbb megoldást kínál a hagyományos információbiztonsági elemek alkalmazásánál, hiszen az információbiztonsági elveket bizonyos fokig a blockchain is teljesíti. Ezt azonban esetről esetre meg kell vizsgálni.

Abban az esetben, amikor szintén több szereplő van, ezek egyenrangúak, de legalább függetlenek, és nem bíznak egymásban, vagy legalább az egyik fél nem bízik a másikban, netán érdekeik ütköznek, ellenérdekeltek, az esetben érdemes blockchain-t alkalmazni. Ez alól azonban lehetséges kivételt képez az, amikor jogszabály, vagy valamilyen más szabályozás kötelezi valamelyik felet a másikban való megbízhatóságra. Ilyen kötelem van például az állam és az állampolgárok között (még akkor is, ha az állampolgárok meg is bíznak egymásban, de mindannyian a jogszabálynak alávetettek). Ekkor a kötelezett félnek mindegy, hogy blockchain-t alkalmaznak-e, vagy sima adatbázist, neki akkor is el kell hinnie azok valóságtartalmát. Viszont az a fél, amelyik kötelezi a másik felet arra, hogy megbízzon benne, ő maga nem feltétlen bízik meg a kötelezett félben. Ezért ebben az esetben pont annak a félnek lehet az érdeke a blockchain alkalmazása, amely a szabályozást bevezette,[14] akármelyik félnek is van joga módosítani az adatbázis bármely elemén. Esetleg gesztusból is alkalmazhatnak blockchain-t arra az esetre, hogy a kötelezett fél maga is közvetlenül meggyőződhessen arról, hogy a jogszabályt alkotó fél által a blockchain-ben tárolt, a megbízhatóság elfogadására kötelezett felet érintő adatok a valóságnak megfelelnek.[15]

Visszatérve az egyenrangú, de legalább független, egymásban nem bízó felekben, még megvizsgálandó, hogy van-e olyan harmadik fél, akiben viszont meg kell bízniuk (például távközlési szolgáltatók a hatóságban). Ez esetben szintén az a helyzet, mint a direkt függésnél, azzal, hogy itt nagy valószínűséggel a független felek ab ovo nem bíznak egymásban sem, azonban a blockchain alkalmazásával kapcsolatos fenti fejtegetések itt is ugyanúgy érvényesek.

Ha azonban olyan, egymástól független, illetve egymásban nem bízó, akár ellenérdekelt felek vannak, akik kötelemben vannak egymással, és nincs megbízható harmadik fél, ott kifejezetten helye van a blockchain alkalmazásának. Ez vonatkozik arra az esetre is, amikor ugyan van felügyeleti szerv, bíróság stb., de bizonyos kérdésekben nincs a szereplők felett megfelelő hatóság, amely igazságot tenne, vagy nem kívánják azt igénybe venni, esetleg illetékességi/hatásköri vitákhoz, pereskedéshez vezetne egy mindegyik fél által megbízhatónak tartott és elfogadott fél szereplése. Ilyenkor is sokkal kedvezőbb és olcsóbb megoldás a blockchain használata. Ilyenekre példák az ellátási láncok, a szállítmányozás, a hálózatos közművek, a több biztosítós rendszereknél a biztosítók. Ezekben az esetekben az ellenérdekű felek önös gazdasági érdeke, hogy egymással kapcsolatban álljanak, rendszereiket fizikailag is összekapcsolják, hiszen egymás nélkül például gazdasági tevékenységet sem tudnának kifejteni. A fenti példák közül ilye-

[13] Lásd az információbiztonság ún. CIA alapelvét: Confidentiality, Inegrity, Availability (bizalmasság, sértetlenség, rendelkezésre állás)

[14] Például az állam az egyes ellátások igénybe vételéhez való jogosultság igazolásánál, vagy pályázati feltételeknek való megfelelésnél, közbeszerzések formai és tartalmi követelményeinek betartásánál.

[15] Ilyen lehet például az egészségügyi alkalmazás a beteg anamnézisekre, diagnózisokra, terápiákra, vagy például a nyugdíjra való jogosultság ellenőrzésére, esetleg a szabálysértésekről készült képi és/vagy video felvételek ellenőrzésére.

nek a hálózatos közművek, amelyeknek definíció szerint össze kell kapcsolódniuk egymással, egyébként az adott szolgáltatási területükön nem lenne villanyáram, víz, gáz, Internet elérés, kábeltévé, vezetéses, és/vagy vezeték nélküli telefon.

Más típusú együttműködés pl. a biztosítók esete, hiszen ott jogszabály teszi lehetővé, hogy több biztosító is működjön azonos földrajzi területen. Az esetben, amikor egy adott esemény kapcsán több biztosító is érintett, netán érdekeik ellentétesek (például autóbalesetek kapcsán), a blockchain alkalmazása olcsó és kívánatos megoldás, hiszen a benne tárolt adatok minden érintett számára ugyanazok, és hitelesnek elfogadandók, bármi is az álláspontjuk egy adott eseményről. Ez mindamellett vonatkozhat egy baleset helyszínén eljáró hatóságra is.

Az ellátási láncok, a szállítmányozás, de akár az adott áru eredetének nyomon követése esetén is alkalmazható és olcsó megoldás a blockchain. Ezekben az esetekben sem bíznak meg a felek egymásban, de legalább az egyik fél nem bízik a másikban, azonban a termék útja, és a felelős kilétének megállapítása hiteles és visszakereshető módon bizonyítható. A feltétel ezekben az esetekben azonban az, hogy az adott áru/szolgáltatás előállításának/nyújtásának elejétől a végéig minden érintett szereplő részt vegyen az adott permissioned blockchain alapú rendszer alkalmazásában.

10. Társadalmi problémák megoldása, vagy generálása?

Kérdés lehet, hogy milyen társadalmi problémák megoldására jó a blockchain. Erre egyrészt sok, a nemzetközi gyakorlatban alkalmazott megoldás adhat választ. De amennyiben társadalmi problémákról beszélünk, ez esetben az államnak jut a fő szerep. Az előzőekben említettek alapján viszont az államban jogszabályok alapján kell megbíznia mindenkinek. Ezért csak azok a nemzetközi gyakorlatban ismert programok jelentősek, amelyek valamilyen módon az államhoz, vagy annak intézményeihez kapcsolódnak.

Svédországban például az ingatlan adásvételeket helyezték blockchain alapra, Grúziában a cégnyilvántartás, az Egyesült Királyságban a pályázatok nyilvántartása, Észtországban pedig az állampolgári nyilvántartások kerültek blockchain alapokra. Sőt, Japánban a tervek szerint ki akarják vezetni a készpénzforgalmat és blockchain alapú fizetőeszközre térnének át, a Palesztin állam pedig az izraeli sékel helyett vezetne be saját cryptocurrency-t[16], és még sorolhatnánk. Sőt, Venezuela például egyes nemzetközi szankciókat akar elkerülni a cryptocurrency-k használatával[17], Észak-Korea pedig hackerek segítségével *„tesz szert”* crypto-kra.[18]

Mi látszik mindebből? Azon felül, hogy az állam *„marketing”* célból, a közigazgatás átlátható működésének javítására, és annak az állampolgárok felé való demonstrálására használhatja a blockchaint, lényegében az állam nem bízik az állampolgáraiban, a gazdasági szereplőkben, stb.

Sőt, a japán példa alapján a készpénz kivezetésével a pénzügyi, de leginkább a gazdasági szektor tisztítása, kifehérítése, a tranzakciók átláthatóságának növelése, így nagyobb ellenőrzés, korrupcióellenesség, illetve adóztatás lehet a fő szempont. Ezért ezen esetekben az állam önös érdeke a blockchain használata.

Más oldalról, de szintén állami szempontból megvizsgálva a blockchain megoldások szerepét, az állam új, eddig nem létező társadalmi problémákkal szembesül, amit elsősorban szabályozással lehetséges megoldani. De amíg nincs globális egyetértés abban, hogy például a cryptocurrency-k kielégítik-e a pénz fogalmához kapcsolódó követelményeket, vagy árunak minősítendők, esetleg egyszerűen asset-nek (eszköznek), addig nem lehet arról beszélni, hogy nemzetközi szinten egységes szabályozás valósuljon meg.

A token-ekkel ugyanez a helyzet, hiszen azok mögött valamilyen szolgáltatás nyújtása van, legalábbis azon esetekben, ahol a kibocsátás eleve nem *scam*[19], azaz átverés, amiből sajnos sok volt 2017-18-ban, az ún. ICO[20] láz idején. Mindemellett külön tárgyalandók az ún. platform token-ek, amelyek a mögöttük lévő blockchain rendszereket tekintve nem adnak szolgáltatást, hanem lehetővé teszik azokat megfelelő blockchain infrastruktúra kialakításával.

Az ICO alapon történő befektető gyűjtésnél, azaz a befektetési célból tartott cryptoasset-eknél a befektetők nem kapnak tulajdonjogot a főleg startup cégekben, úgyhogy részvénynek nem minősíthetők, de nem is kötvényt testesít meg, hiszen a cégnek nincs visszavásárlási kötelezettsége. Sőt, az sem egyértelmű, hogy értékpapírról beszélünk-e egyáltalán, vagy sem. A kibocsátott, és a befektetők által lejegyzett crypto-k egy jó része átmegy az ún. Howey-teszten[21], másik részük megbukik. A Howey-teszt pedig pont arra hivatott, hogy eldöntse, hogy az adott cryptoasset értékpapír-e vagy sem. Ha az, akkor annak kibocsátásához az adott állam pénzügyi felügyeletének engedélye kell, és az eszköz eszerint is adózik (nyereségadó), míg, ha nem, akkor sok helyen az árukhoz sorolva rögtön ÁFA-köteles a cryptoasset. Holott nincs még mögötte semmiféle áru, vagy szolgáltatás, hiszen épp induló vállalkozásokat finanszíroznak vele. Ezért a szabályozás itt sem egyértelmű, ráadásul a startup-ok megpróbálják kikerülni mind az engedélyhez kötöttséget (pre-ICO-k[22], Airdrop-ok), mind az adófizetési kötelezettséget. Egyes államokban azonban a Howey-teszten megbukó cryptoasset

[16] Palestinian Authority Considering Crypto to Replace Israeli Shekel: https://cointelegraph.com/news/palestinian-authority-considering-crypto-to-replace-israeli-shekel (lekérdezés ideje: 2019. 07. 30.)

[17] Venezuela Turned Airport Taxes into Bitcoin to Avoid Sanctions: Report: https://www.coindesk.com/venezuela-turned-airport-taxes-into-bitcoin-to-avoid-sanctions-report (lekérdezés ideje: 2019. 07. 30.)

[18] North-Korea Hacked $670 million from Crypto Exchanges: https://www.crowdfundinsider.com/2019/03/145210-north-korea-hacked-670-million-from-crypto-exchanges/ (lekérdezés ideje: 2019. 07. 30.)

[19] Ez nem azonos az ún. *shitcoin*-okkal, ahol a bevezetés nem átverésre alapult, hanem tényleges terméket, vagy szolgáltatást akartak fejleszteni, de az ötlet nem jött be, így a kibocsátott cryptoasset (coin) elértéktelenedett.

[20] Initial Coin Offering, ami hasonlít a hagyományos részvénytársaságok eredeti részvénykibocsátására az IPO-ra (Initial Public Offering).

[21] Lásd például: What Is the Howey Test?: https://consumer.findlaw.com/securities-law/what-is-the-howey-test.html (lekérdezés ideje: 2019. 07. 30.)

[22] Előzetes ICO-k, hogy ne kelljen Howey-tesztet végezni.

kibocsátást ezért STO-kkal[23] engedélyezik, de ez már azon múlik, hogy a pénzügyi felügyelet engedélyével rendelkezik-e a kibocsátó. Mára pedig kialakult az IEO[24] is, amikor is cryptotőzsdéken keresztül bocsátják ki az adott cryptoasset-et.

A fent említett platform tokenek bonyolultabb esetnek minősíthetők, hiszen ott a szolgáltatás maga az infrastruktúra, azaz a platform. Ezeknek legismertebbje az Ethereum rendszer. A platformok magukban nem adnak a végfelhasználók számára értelmezhető megoldást valamilyen problémára, hanem egy adott szolgáltatás nyújtását célként kitűző startup vállalkozás által használható keretrendszer. Hasonlóan viselkedik, mint maga az Internet, ami szintén egy platform, attól van értéke, hogy különböző szolgáltatások elérhetők rajta. Ellenben az Internethez képest a blockchain platformoknak maguknak is van értéke, vannak saját tokenjeik (az Ethereum rendszernél az ether). Ugyanez az Internetnél nem mondható el, nagy valószínűséggel állítható, hogy a világon senkinek sincs *„Internet részvénye"*, blockchain platform token-je azonban sokaknak van, kereskednek vele, sőt, az Ethereum tokenje az egyik leginkább kereskedett cryptoasset.

További szabályozási problémaként merül fel, hogy például a cryptotőzsdék mivel is kereskednek? Hogyan, milyen alapon váltják át a pénzváltók a cryptoasset-eket fiat-tá és viszont? Mit kap a pénzéért az, aki cryptoasset-et vesz? Csak egy bitsorozatot, amit azonban nem bankok, értékpapírcégek, biztosítók tartanak nyilván, hanem egy egyenrangú felekből álló közösség, akinek tagjai a világ minden részén megtalálhatók. Hogyan lehet a cryptoasset-eket bevezetni a fizikai világban létező tőzsdékre[25], és melyikre? Részvénytőzsdére, valutatőzsdére, vagy árutőzsdére? Hogyan lehet az ilyen óriási árfolyam ingadozással rendelkező cryptoasset-eket kordában tartani? Hiszen, ha egy tőzsdén egy adott papír árfolyama 10 %-ot meghaladóan változik a nap folyamán, annak a kereskedését azonnal felfüggesztik, mert *„valami nincs rendben"*. Ugyanakkor például a bitcoin árfolyama akár 20-30 %-ot is változhat egy adott napon belül. A crypto-ba befektetők örülnének a legjobban, ha például *„csak"* 10 %-ot változna napon belül az árfolyam. A cryptoasset-ek kiszámíthatatlanok, hiszen a cryptocurrency-k esetében nincs mögöttük semmi, csak egy matematikai algoritmus, amit be kell tartani, a token-ek esetében pedig csak egy ígérvény, hogy majd valamikor lesz egy termék vagy szolgáltatás, de az is lehet, hogy végül nem. A crypto-k világában tehát semmilyen fundamentum nincs (jelenleg), így például egy tőzsdei befektetés fundamentális elemzésének nincs létjogosultsága, kizárólag technikai, a befektetők tömegének viselkedését, pszichológiáját alapul vevő elemzéssel lehet megjósolni a jövőbeni árfolyamot. Hogyan tud ilyen esetben egy szabályozó, egy hatóság bármilyen szerepet vállalni, bármiféle befektető védelmet biztosítani? Hogyan tud egy bíróság dönteni, ha abban sem lehet biztos, hogy mi az, és hova sorolandó az az ügy, amiben döntenie kellene? Mennyire nehéz a dolguk a bűnüldöző szerveknek, ha nincs definiálva, hogy mit is foglalnak le adott nyomozás során, és annak adott időpillanatban mennyi az értéke?

Hogyan lehet szabályozni a cryptoasset-hez való hozzájutást, költést, annak ellenére, hogy a cryptotőzsdékre és crypto pénzváltókra az államok – a fizikai világban lévő eszközökkel foglalkozó pénzintézetekhez hasonlóan – rákényszerítették a felhasználó azonosítást és minősítést (KYC[26])? Hiszen crypto-hoz nem csak tőzsdén való kereskedés által lehet hozzájutni, hanem például egy kávézóban való fizetéskor, on-line játékokkal, vagy bányászattal, amikor is a *„villanyszámlában"* jelenik meg[27] a cryptoasset ára. Hogy lehet követni a cryptoasset útját, megelőzni a pénzmosást (AML)[28], terrorizmus finanszírozást stb.? Hiszen bárki a mobiltelefonján, számítógépén, mindenféle felügyelet, bejelentési kötelezettség vagy felhasználó azonosítás nélkül és bármikor létrehozhat egy wallet-et (cryptoasset-ek tárolására szolgáló tárcát), amelyben annyi crypto-t tárol, amennyit akar? Sőt, ha megsemmisül a wallet-je, elég 20 angol szót sorrendben megjegyeznie[29], és a világ másik felén egy új mobiltelefon segítségével bármikor visszaállíthatja azt, benne az összes coin-jával. Ne feledjük, hogy abban a mobiltelefonban több milliárd USD értékű coin is lehet, és nem kell a több pénz tárolásához nagyobb táska mint pl. a készpénz használat esetén.

Visszatérve a crypto-tőzsdékre, ezek közül a legutóbbi időkig sok állami felügyelet, regisztráció, sőt bármiféle engedély nélkül működött. Azonban 2017-től megnőtt az a trend, hogy ezeket a tőzsdéket engedélyeznie kell az állami felügyeletnek. De mit csináljon az állam az elosztott, központ nélküli cryptotőzsdékkel (DEX[30]-ek), amelyek nem is köthetők egyetlen állam fennhatóságához sem. Ugyanígy mit csináljon az állam a központ nélküli, autonóm módon működő szervezetekkel (DAO[31]-k)?

Ezen felsorolt problémák esetén sem sui generis módon, sem más, már létező társadalmi helyzet analógiájára alapuló szabályozására még csak ötlet sincs. Sőt, léteznek kezdeményezések olyan *„virtuális"* államok létrehozására, amelynek tagjai a blockchain technológia alkalmazásával szavazhatnak, vehetnek részt a társadalmi folyamatokban, sőt hatással vannak a több ezer éve kialakult hagyományos társadalmi berendezkedésekre. Ennek egyik prominens példája a *„Democracy.Earth"*[32], amelynek jelszava a *borderless governance*, a határok nélküli kormányzás.

Jelenleg[33] pedig a pont az i-re a Facebook által bejelentett Libra[34] névre keresztelt, blockchain alapú *„cryptocurrency"*, amely minden, csak nem az, aminek beállítják. Nem is *„e-money"*, hanem egy öszvér megoldás, egy *„globális pénz"*, amelyet nem pénzügyi szervezetek, nem államok, hanem egy multinacionális vállalat kontrollál. A Facebook válasza ter-

[23] Security Token Offering.

[24] Initial Exchange Offering, lásd például: https://www.binance.vision/glossary/initial-exchange-offering (lekérdezés ideje: 2019.07.30.)

[25] Exchange Traded Funds (ETF).

[26] Know Your Customer.

[27] Hiszen a bányászat sok áramot fogyaszt az óriási számítási igény miatt.

[28] Anti Money Laundering.

[29] Ez az ún. HDWallet-ek (Hiearchical Deterministic Wallet-ek) esetében van így, amelyekre már minden wallet szoftver gyártó kezd áttérni.

[30] Distributed Exchange.

[31] Distributed Autonomous Organization.

[32] Lásd: https://democracy.earth/(lekérdezés ideje: 2019. 07. 30.).

[33] 2019. július vége.

[34] Lásd: https://libra.org/en-US/ (lekérdezés ideje: 2019. 07. 30.).

mészetesen erre az, hogy nem ők kontrollálják, hanem egy nonprofit szervezet van mögötte, a *„The Libra Association"*[35], amelyben olyan szervezetek, multinacionális vállalatok vesznek részt, mint a Mastercard, Visa, Paypal, Ebay, Spotify, Uber, Vodafone, valamint blockchain vállalatok, sőt kockázati tőkebefektetők is.[36] Nem is véletlen, hogy a legtöbb állam, nemhogy nem támogatja, vagy tűri[37] a Librát (Németország, Oroszország), hanem ellene van,[38] szabályozni akarja (USA, EU),[39] vagy egyszerűen megtiltja (India).[40] Sőt, Kína egy alternatív eszközt dolgoz ki a Libra helyett,[41] mondván, hogy a kínai állam azért mégis erősebb, mint egy magáncég.[42] A legutóbbi hírek szerint azonban a Facebook meghátrál a nemzetközi ellenállás miatt.[43] De legalább a pénzügyi kormányzatok szereplőit felébresztette.

Akárhogy is áll azonban a Libra helyzete, akárhogyan is értelmezzük a fentieket, látszik egy trend: mégpedig az, hogy az állam, a pénzügyi kormányzat szerepe, illetve a monetáris politika át fog értékelődni.

11. Összefoglalás

A fent leírtakból tehát levonható az a következtetés, hogy amellett, hogy a blockchain egyes társadalmi problémák megoldására használható, de sokkal súlyosabb, és eddig ismeretlen társadalmi problémákat generál, mint amelyekkel eddig szembesült az állam. Summázva: a blockchain technológia kiterjedt alkalmazása jelenleg több társadalmi problémát okoz, mint amennyit megold.

Mindazonáltal a blockchain alkalmazhatóságára itt csak egyetlen szempont, a szereplők egymáshoz képesti viszonyának vizsgálatával került sor. A jelen írásban leírtak az irodalom alapján a szerző által kialakított véleményt tükrözik, mellyel lehet egyetérteni vagy egyet nem érteni. Végső soron azonban, bár nem mindenütt, és nem minden esetben van létjogosultsága a blockchain megoldások használatának, azonban ott, ahol a megfelelő vizsgálódás és előkészítés után szükséges, ott a használat mellőzésére nincsenek igazi érvek.

[35] Lásd: https://libra.org/en-US/association/ (lekérdezés ideje: 2019. 07. 30.).

[36] https://libra.org/en-US/association/#founding_members (lekérdezés ideje: 2019. 07. 30.).

[37] Germany's Central Bank: Govt's Should Be Neutral on FB's Libra: https://cointelegraph.com/news/germanys-central-bank-govts-should-be-neutral-on-fbs-libra (lekérdezés ideje: 2019. 07. 30.).

[38] How 10 Countries respond Facebook's Libra Cryptocurrency: https://news.bitcoin.com/how-countries-respond-facebooks-libra-cryptocurrency/ (lekérdezés ideje: 2019. 07. 30.).

[39] Például: France Calls for Central Bank Review of Facebook Cryptocurrency: https://www.bloomberg.com/news/articles/2019-06-18/france-calls-for-central-bank-review-of-facebook-cryptocurrency (lekérdezés ideje: 2019. 07. 30.), vagy: Thanks Facebook. More Cryptocurrency Regulations Are Coming: https://edition.cnn.com/2019/06/19/tech/facebook-libra-cryptocurrency-regulations/index.html (lekérdezés ideje: 2019. 07. 30.), vagy: European Central Bank Exec Calls for Fast Regulatory Action Regrding Libra: https://cointelegraph.com/news/european-central-bank-exec-calls-for-fast-regulatory-action-regarding-libra (lekérdezés ideje: 2019. 07. 30.).

[40] Indian Authorities Express Concerns Over Facebook's Libra: https://cointelegraph.com/news/indian-authorities-express-concerns-over-facebooks-libra (lekérdezés ideje: 2019. 07. 30.).

[41] Central Bank of China Is Building Its Own Cryptocurrency To Fight Against Facebook's Libra Asset: https://insidebitcoins.com/news/central-bank-of-china-is-building-its-own-cryptocurrency-to-fight-against-facebooks-libra-asset/231992 (lekérdezés ideje: 2019. 07. 30.).

[42] Lásd: Huawei CEO: Why Wait For Facebook? China Can Issue Its Own 'Libra': https://cointelegraph.com/news/huawei-ceo-why-wait-for-facebook-china-can-issue-its-own-libra. (lekérdezés ideje: 2019. 07. 30.).

[43] Facebook Admits Libra Crypto Project May Never Launch: https://bitcoinist.com/facebook-admits-libra-crypto-project-may-never-get-launched/ (lekérdezés ideje: 2019. 07. 30.).