A kis Bitcoin könyv

Timi Ajiboye
Luis Buenaventura
Alex Gladstein
Lily Liu
Alexander Lloyd
Alejandro Machado
Jimmy Song
Alena Vranova

A mű eredeti címe: The Little Bitcoin Book
Copyright © 2019 by The Bitcoin Collective
All rights reserved. This translation published with permission from the original authors.
https://littlebitcoinbook.com

Fordították:
Kovács Andrea (BitcoinBázis), Bánfi Balázs Miklós, ‘OptOut’.
Hungarian translation © Kovács Andrea & Bánfi Balázs Miklós, 2023

Minden jog fenntartva.

Illusztrációk: Luis Buenaventura.
„Venezuelai blokád” illusztráció: Timi Ajiboye.
Borítóterv: Fazekas Csilla.

A fordítás az alábbi kiadás alapján készült:
The Little Bitcoin Book
21 Million Books, Redwood City, CA
First Edition (ISBN 978-1-64199-050-9)

A kis Bitcoin könyv

Tartalom

Előszó

Aktivisták, nevelők, vállalkozók, igazgatók, befektetők és kutatók vagyunk. Afrikából, Ázsiából, Európából, Észak-Amerikából és Dél-Amerikából jöttünk. Sokban különbözünk, de mindannyiunkat megigézett a Bitcoin, és hisszük, hogy nagy hatása lesz a világra és az életünkre.

2019 márciusában Jimmy beszélt néhányunkkal egy 'könyv sprint' ötletről: hogy közösen elvonulnánk pár napra egy könyvet írni a bitcoinról és társadalmi fontosságáról. Két hónap múlva, az Oslói Szabadság Fórumon, összejöttünk egy háztetőn, több kontinensről összesereglett emberjogi aktivista és újságíró zsibongása közepette. Beszélgetésünk szükségszerűen a bitcoinra és a világmegváltó lehetőségeire terelődött. Alex arra biztatta a társaságot, hogy írjunk egy könyvet, ami elmagyarázza a bitcoin jelentőségét, de a technológiai szakzsargon nélkül, ami a meglévő bitcoin könyvek többségére jellemző. Segíteni akartunk az érdeklődőknek megérteni e napjaink egyik legmélyrehatóbb innovációját, és hogy az hogyan hathat az emberek életére. Néhány hónap múlva mi nyolcan összeültünk egy kaliforniai házban, hogy megvalósítsuk ezt az ötletet.

Amit most a kezedben tartasz, kedves olvasó, az ennek a négynapos munkának az eredménye. Ennek a könyvnek a célja bemutatni, hogy mik a problémák ma a pénzzel, miért született alternatívaként a bitcoin, hogyan hathat a politikára és a társadalomra, és mit jelent a jövőnkre nézve.

Őszintén reméljük, hogy e könyv olvasása során téged is lenyűgöz a Bitcoin, mint ahogy minket is.

2019. augusztus 8.
Redwood City, Kalifornia

A szerzőkről

Timi Ajiboye szoftverfejlesztő és vállalkozó a nigériai Lagosból. Társalapítója és jelenlegi működtetője a BuyCoins váltónak (buycoins.africa), ahol az afrikaiak könnyen tudnak bitcoint adni és venni helyi pénzek ellenében. Twitter: @timigod

Luis Buenaventura a BloomX társalapítója (bloom.solutions), ami egy startup a Fülöp-szigeteken, amely biztonságos kriptovaluta kereskedést kínál a fejlődő országoknak. Termékeny előadó és szerző, többek között a Cryptopop.net létrehozója, egy művészeti kezdeményezés amely a kriptót próbálja közérthetővé tenni a nagyközönség számára. Twitter: @helloluis

Alex Gladstein vezető stratéga (Chief Strategy Officer) a Human Rights Foundation-nél (hrf.org), ami egy globális nonprofit szervezet a szabadságjogok védelméért. Előad a Singularity Egyetemen a bitcoinról és kormányzásról, és gyakran ír a technológia és szabadság összefüggéseiről olyan helyeken, mint a TIME, CNN vagy a Bitcoin Magazine. Twitter: @gladstein

Lily Liu befektető és vállalkozó. Mostanában társalapító és pénzügyi vezető az Earn.com-nál, ami egy olyan platform, ahol szabadidőben lehet bitcoint keresni; 2018-ban megvette a Coinbase. Korábban kórházat épített Kínában, dolgozott a KKR-nél és McKinsey-nél, és tanult a Stanfordon és a Harvardon. Twitter: @calilyliu

Alexander Lloyd korai fázisban lévő startupokba fektet be 1998 óta, 2008-ban megalapította az Accelerator Ventures-t. Első munkahelye a Goldman Sachs-nál volt mint deviza kereskedő. 2016-ban csatlakozott a Human Rights Foundation-hoz, ahol Észak-Korea a fő fókusza. Twitter: @alex01

Alejandro Machado az Open Money Initiative egyik alapítója (openmoneyinitiative.org), ami egy nonprofit szervezet, amely a pénz használatát kutatja zárt gazdaságú és összeomlófélben lévő pénzügyi rendszerű országokban. A Venezuelában élők digitális pénz elérésének javítására fókuszál. Twitter: @alegw

Jimmy Song Bitcoin fejlesztő, oktató és vállalkozó. Az O'Reilly által kiadott Bitcoin Programozás könyv szerzője (programming-bitcoin.com). Az erős pénz terjesztésén fáradozik. Szinte mindig cowboy kalapot hord, aminek színe jelzi, hogy épp kedves vagy szigorú szerepben lép fel. A PGP ujjlenyomata C1D7 97BE 7D10 5291 228C D70C FAA6 17E3 2679 E455. Twitter: @jimmysong

Alena Vranova sikeres pénzügyi szolgáltatási céget fejleszt 2003 óta. Az utóbbi 7 évben azon dolgozott, hogy bitcoin tárolási termékekkel és szolgáltatásokkal segítsen magánszemélyeknek és kis cégeknek. 2013-ban vezette be a Trezort, az első bitcoin hardver tárcát, és jelenleg a Casa (keys.casa) stratégiáját vezeti, mindenki számára elérhetővé téve a személyes bitcoin biztonságot és pénzügyi szuverenitást. Twitter: @AlenaSatoshi

A szerzők a könyv sprint harmadik napján.

A magyar fordítás előszava

Ezt a könyvet azért fordítottuk le, mert úgy gondoltuk, hogy hasznos lenne, ha magyarul is elérhető lenne egy könnyen emészthető, bevezető könyv a bitcoinról.

A könyv megírása és a fordítás között eltelt két évben sok minden történt a világban, de a könyv aktualitása nem csökkent, inkább nőtt. Sajnos a szűkebb környezetünkben is megjelent a háború, és az infláció is valós, kézzelfogható problémaként jelent meg egyre több ember életében.

A szövegben lévő adatokból néhányat aktualizáltunk, de az összefüggések miatt ez nem mindenhol volt lehetséges.

Budapest, 2023.

1. FEJEZET

Mi a baj a pénzzel ma?

1981-et írunk.

Manilában egy fiatal fülöp-szigeteki párnak épp megszületett első gyermekük, néhány hónappal azután, hogy tíz év után először szűnt meg a statárium. A diktátor, Ferdinand Marcos, még pár évig hatalmon marad, de Luis szüleit most csak a kis családjuk érdekli. Van egy megtakarítási számlájuk, de igazából csak most tudtak elkezdeni félretenni, a bizonytalan jövőre készülve. Az árfolyam hét fülöp-szigeteki peso egy USA dollárért.

1993-at írunk.

Lagosban hatalomra kerül Sani Abacha nigériai tábornok, és 22 nigériai nairában rögzíti az USA dollár árfolyamát. Ezzel az agresszív lépéssel a gazdaságot szeretné stabilizálni és elejét venni a naira további gyengülésének. A rögzített árfolyam egy egész párhuzamos gazdaságot kelt életre, ahol a nairát sokkal alacsonyabb értéken váltják. 1998-ban, Abacha halála idején, egy dollárért már 88 nairát is elkérnek a feketepiacon, a hivatalos árfolyam négyszeresét. Emberek millióinak jelent egyre nagyobb nehézséget a stagnáló közalkalmazotti fizetésükből megvenni az egyre dráguló napi élelmüket.

2018-at írunk.

A venezuelai határ mentén mindenütt emberek szöknek át Kolumbiába és Brazíliába, menekülve a 400.000%-os hiperinfláció elől. Több mint 3 millióan már elmenekültek a lesújtó éhezés és széteső társadalom elől.

Lorena, egy 48 éves pék, meghozta a nehéz döntést, hogy Kolumbiába szökik. A határon a határőrök átvizsgálják a csomagjait, elkobozható értékeket keresve. Semmit sem találnak. Nem tudják, hogy Lorena órákat töltött azzal, hogy dollár bankjegyeket tekert szorosan hajcsatjai köré, és gondosan elrejtette őket hajfonataiban. Emelt fővel érkezik egy új országba.

Manilában Luis szüleivel nem kegyes a sors. Az árfolyam most 50 fülöp-szigeteki peso egy amerikai dollárért, így az évek alatt gondosan félretett pénzük értékének több mint 80%-a elveszett. Bár már nyugdíjba mehetnének, nincs más választásuk, mint továbbra is dolgozni és félretenni egy hálátlan és bizonytalan jövőre.

Lagosban a naira egy rövid viszonylagos stabil időszakban van, miután 50%-ot gyengült a dollárhoz képest pár év leforgása alatt. A helyi termékek ára ismét megugrott. Már senki sem hiszi, hogy a kormány képes elejét venni egy újabb gazdasági válságnak, még a kormány vezetői sem.

2019-et írunk.

Sanghajban Annie, egy fiatal dolgozó nő, egy barátjával beszélget a WeChat-en, ami egy több mint egymilliárd kínai által használt, népszerű közösségi média platform. A barátja elmondja, hogy bajban van marihuána fogyasztás miatt, aztán nem válaszol többet, hirtelen abbahagyva a társalgást.

Másnap két civil ruhás rendőr keresi Anniet az irodájában, és magukkal viszik. Ezután munkatársai néhány hétig egyáltalán nem látják őt. Mire végül visszatér, a WeChatjéből eltűnt néhány fizetés funkció. Nem tud vonat vagy repülőjegyet venni. Az adós besorolása leromlik. Egyetlen üzenetváltás tönkretette az életét.

Oaklandben Alex betér egy kisállatboltba, kutyatápot venni. Megtalálja, amit keres, ráadásként pedig egy érdekes új terméket, amitől állítólag jobb lesz a kutya szájszaga. Alex a Chase Visa kártyájával fizet, majd kimegy. Néhány perc múlva, mikor ránéz a Twitterére, egy kutyatáp reklám jelenik meg, ugyanattól a gyártótól, akitől épp vásárolt. Be kell hogy lássa, hogy a Chase bank megosztja a napi fizetési információit más cégekkel.

A tudat, hogy életének privát részletei kerülnek hirdető cégekhez, rossz érzéssel tölti el, és ez sajnos nem ismeretlen az ‘okostelefon generáció’ tagjai számára. Manapság még az USA-ban is egyre inkább eltűnik a pénzügyi magánélet.

Ezek a történetek mutatják, hogy milyen gondok vannak a pénzzel.

Luis szülei, több millió fülöp-szigeteki és nigériai középosztálybelivel együtt keserűen szemlélték, ahogy megtakarításuk kevesebb mint egy generáció alatt elolvad. Lorena mindenképpen meg akarta úszni az elkobzást, hogy kis vagyonkáját átmentse Kolumbiába, jobb híján így csinált belőle kontyalávalót. Anni most ‘pénzügyi börtönben’ van, csak azért, mert egy barátja füvezett. Alex minden egyes vásárlását eltárolja a bankja, és az adatokat átadja más cégeknek.

Ezek nem egyedi esetek.

2000 óta szinte az összes nemzeti valuta vesztett az értékéből az USA dollárhoz képest. Nem egy az értékének majdnem felét is – ilyen a dél-afrikai rand, az argentin peso és a török líra. Néhány még pechesebb, mint az ukrán hrivnya és a dominikai peso, 70%-ot is. Ráadásul a dollár és az euró is 33%-ot veszített a vásárlóerejéből ez idő alatt.

Világszerte 250 millió bevándorló és menekült küzd azzal, hogy hogyan küldjön haza vagy vigyen magával pénzt egy másik országba. Durván két milliárd embernek nincs bankszámlája vagy nincs olyan hivatalos igazolványa, ami előfeltétele egy bankszámlának. Az egyre inkább globalizálódó világunkban a pénz makacsul helyhez kötött.

Az érzés, hogy állandóan megfigyelnek, egyre kézzelfoghatóbb, főleg az olyan nagyvárosokban mint Sanghaj vagy San Francisco. Egyrészt a Nagy Testvér figyel. Másrészt az adatgyűjtő kapitalizmus megfigyel minden mozgást és vásárlást, és az érintett beleegyezése nélkül eladja az adatokat más cégeknek. A privát szféra lassan egy napról napra drágább luxuscikké válik.

Mi a pénz?

Alapvetően a pénz egy társadalmi megegyezés.

A pénz úgy tud működni, hogy az emberek elhiszik, hogy a bankók a pénztárcáikban, a számok a bankszámláikon, vagy az ajándékkártyáik egyenlegei mind felhasználhatók lesznek később azokra a dolgokra, amit szeretnének illetve amire szükségük van. Az eladónak el kell fogadnia, hogy a vásárló pénze értékes.

A történelem során az emberi közösségek különböző módokat használtak e megegyezés megvalósítására: kagylókat, sót,

aranyat, egészen a mai központi bankok komplex rendszeréig. Egyes pénzek jobban megalapozottak, mint mások, vagyis jobban tartják az értéküket.

Ösztönösen mindenki tudja, hogy a pénz fontos, és mindenki a megalapozottabb pénzt szeretné. A legtöbb ember a munkájáért cserébe kap pénzt, úgyhogy a pénz az ember idejét és erőfeszítését reprezentálja. A pénz segítségével tudjuk munkánkat termékekre és szolgáltatásokra váltani, mind ma, mind pedig a jövőben. Ilyen értelemben a megalapozott pénzhez való hozzáférés egy időtálló személyes hatalom.

A pénz a kormányzatok számára is roppant jelentőséggel bír. A mai világgazdaság nemzetállamokból tevődik össze, és ezek kormányai ellenőrzik a pénzt. Viszont a pénz feletti ellenőrzés sokszor csábít visszaélésre. A döntéshozók gyakran saját érdekük szerint kihasználják ezt a hatalmat. Csak azok a legdemokratikusabb kormányok tudnak ténylegesen védekezni az olyan pénzügyi visszaélésekkel szemben, mint a szabadjára engedett infláció, önkényes eltulajdonítás és a korrupció, akik messzemenően védik az egyéni szabadságjogokat, a hatalmi ágak szétválasztását és a törvény hatalmát.

Hogyan működik a modern pénz?

Minden ma létező nemzeti fizetőeszközt *fiat* pénznek hívnak, ez egy latin szó, aminek a jelentése 'legyen'. Ezeknek a pénzeknek az értékét az őket kibocsátó és elfogadó nemzetállamok rendelete határozza meg. Mivel a kormányok minimális költséggel tudnak pénzt létrehozni, bármikor és bármennyi új pénzt tudnak létrehozni.

Alan Greenspannek, a Fed (amerikai jegybank) korábbi elnökének egy elhíresült mondása, hogy az USA „mindig vissza

fogja tudni fizetni az adósságát, hiszen bármikor tudunk pénzt nyomtatni ehhez". A legrégebbi nemzeti valuta, az angol font vásárlóerejének 99,5%-át veszítette el 300 év alatt. Az amerikai dollár 90%-ot veszített értékéből egy évszázad alatt. Egy steak, ami 0,36 dollárba került 1925-ben, 1990-ben 3 dollárba, ma pedig 12-be kerül. Ráadásul ezek a valuták a stabilabbak közé tartoznak. Egy átlagos pénz élettartama nem több mint 27 év.

Alacsony és stabil infláció – ez minden modern központi bank kimondott célja, de ezt – időszaktól és országtól függően – nem mindig sikerül elérni. Hosszú távra vetítve a világ szinte minden országában magas inflációról beszélhetünk, ami megtizedeli a megtakarítások értékét. Ez különösen igaz azokra, akik nem engedhetnek meg olyan kemény befektetéseket, mint az ingatlan vagy elsőosztályú részvények, amelyek értéke az inflációval együtt növekszik. A magas infláció a gazdagok kivételével mindenki más számára megnehezíti a tartós megtakarítást.

Milliárdnyi ember él tekintélyelvű rendszerekben, ahol a megtakarítások elértéktelenedése olyan vezetők döntésétől függ, akiket nem az emberek választottak. Kizárólag az elit fér hozzá értékálló dollárhoz, aranyhoz vagy ingatlanokhoz. Ehhez képest a gazdag demokráciák polgárai védettebbek. Ők hozzáférnek olyan viszonylag stabil pénzhez, mint a dollár vagy az euró. Ezen országok gazdaságai általában jól működnek, a legtöbb embernek van jól fizető állása. Befektetési eszközökhöz is hozzáférnek, amelyek kiegyenlítik, vagy akár túl is teljesítik az inflációt.

Az elit mindig aránytalanul több előnyre tesz szert az újonnan nyomtatott pénzből – ez a hatás olyan erős, hogy külön neve is van: a *Cantillon hatás*. Richard Cantillon, egy XVIII. századi angol közgazdász, figyelte meg, míg egy bankban dolgozott. A drasztikus vagy nagy mértékű infláció egy igazságtalan elosztó rendszer, hiszen a gazdagokat jutalmazza a szegények

kárára. És bár ez a hatás nem feltétlenül szembetűnő egy átlag amerikainak vagy angolnak, annál fájdalmasabb kevésbé fejlett országokban élő milliárdok számára.

A fiat pénzrendszerek továbbá hozzájárultak a modern kor elnyúló háborúihoz. A hadban álló kormányok több pénzt tudnak nyomtatni, a költségekkel a későbbi generációkat terhelve az infláción keresztül. Ennek eredményei a hosszabb és költségesebb háborúk. Az első világháború egy tragikus példa, hiszen a fő résztvevők a későbbi költségeket infláció segítségével fedezték. Oroszország és Németország is felfüggesztette az *arany standardot*, amely alatt a fiat valutájuk egy fix arany mennyiségre volt váltható. Inkább felfüggesztették az átválthatóságot, és fedezet nélkül nyomtattak pénzt a háború finanszírozására. Ennek tudható be, hogy a háború sokkal tovább tartott, mint amit sokan lehetségesnek gondoltak. Miután Németország vesztett, egyetlen módon tudták fizetni a hatalmas kártérítési összegeket: még több pénzt nyomtatva. 1923-ra a német márka a háború előtti értékének egy billiomodjára értéktelenedett, előrevetítve a második világháborút.

Hasonló tékozló költekezés a közelmúltban is többször előfordult. Függetlenül attól, hogy ki mint ítéli meg az USA afganisztáni és iraki beavatkozását, ezek költsége 5,9 billió dollár fölötti. Ez háztartásonként több mint 46 ezer dollárra jönne ki, ha az amerikai adófizetők közvetlenül finanszírozták volna a háborút.

Egy másik gond a modern pénzrendszerekkel, hogy néha csak nagyon nehézkesen lehet pénzt mozgatni a világ különböző országai között. Egyes országok kormányai, például Kína, Oroszország, Argentína vagy Indonézia, szigorúan ellenőrzik, hogy az állampolgárok mennyi pénzt válthatnak, küldhetnek vagy vihetnek külföldre.

Ezt elsősorban úgy érik el, hogy korlátozzák az egyének pénzváltását, saját pénznemről külföldi valutára, mint például az amerikai dollár. Például egy átlag kínai legfeljebb évi 50.000 dollárnyi renminbit válthat be.

A világ más helyein még az egyén saját pénzéhez való hozzáférését is korlátozhatják. A 2015-ös görög pénzügyi válság után az emberek egy nap nem vehettek fel 60 eurónál többet saját bankszámlájukról, éles emlékeztetőként, hogy nem rendelkeznek a saját pénzük fölött.

Ha küldhetnek is az emberek pénzt külföldre, ez sokszor nehézkes és költséges. 2018-ban vendégmunkások és menekültek közel 700 milliárd dollárt utaltak más országokba családtagjaiknak. Ebből 45 milliárdot emésztettek fel az átváltási és küldési költségek – ez nagyon jelentős hányad, főleg azoknak, akiknek nincs mit félretenniük.

Egy globális közös hibaforrás

Minden központi bank egy lehetséges hibaforrást jelent saját nemzeti gazdasága számára. Az amerikai jegybank bizonyos tekintetben egy központi bank a világ összes bankja számára. Az amerikaiak szemszögéből ez a felállás jól működik. A dollárt mindenhol elfogadják, és a legtöbb amerikai gond nélkül tud bankszámlát nyitni, hitelt felvenni, árukért és szolgáltatásokért fizetni. Az infláció sem okoz különösebb gondot (fordító megjegyzése: e könyv megírása óta jelentősen nőtt az amerikai infláció).

A dinamikus amerikai gazdaság kihat a globális gazdaságra, megalapozva és meghajtva azt. Egyik fő pillére a *dollár standard*, a globális uralom, ami egy kevéssé ismert eseménnyel

kezdődött 1944-ben egy hotelszobában New Hampshire-ben: a Bretton Woods megállapodás.

A világhatalmak összeültek Bretton Woodsban, hogy kidolgozzanak egy egységes pénzügyi rendszert, a végéhez közeledő második világháború utáni időre készülve. 44 ország több mint 700 küldötte három héten keresztül vitatta meg és egyezkedett a jövő pénzügyi rendszerének felépítéséről. Néhány küldött egy új, nemzetközi tartalék valuta létrehozását javasolta, *bancor* néven. Végül a küldöttek megállapodtak, hogy valutájuk az USA dollárhoz lesz kötve. Ennek a máig tartó hatása az, hogy a nemzetközi kereskedelem legnagyobb részét dollárban számolják el, és minden ország dollár tartalékra törekszik.

Az amerikai dollár globális központi szerepe abban is tükröződik, ahogyan az országok közötti pénzküldés működik. Példaként nézzünk meg egy Dél-Koreából a Fülöp-szigetekre való utalást. Általában nem lehetséges a dél-koreai wont közvetlenül fülöp-szigeteki pesóra váltani, mert a két ország nem tart egymás valutájából eleget. Ezért a dollárt használják, és több tranzakciót. Először a wonból dollárt vesznek Szöulban. Ezt egy amerikai bankon keresztül elutalják egy dél-koreai bankból egy fülöp-szigetekibe. Végül a manilai bank a dollárt fülöp-szigeteki pesóra váltja. Ez legalább néhány napot vesz igénybe, és átváltási valamint utalási költségekkel jár: ez lehet pár százalék népszerűbb útvonalakon, de lehet akár alacsonykétszámjegyű százalék is kevésbé népszerű esetekben. A hasonló nemzetközi utalások díja átlagban 7% fölötti, kis összegű utalások esetében is.

A dollár standard több módon is hasznos a világnak, másrészt viszont egy törékeny állapotot is eredményez: minden gazdaság függ valamilyen mértékben az amerikai dollártól, és sebezhető egy esetleges dollár zuhanás esetén. Ebben a rend-

szerben pár bank csőd amerikában egy globális gazdasági katasztrófához vezethet.

A pénzügyi magánélet vége

A pénz digitalizálódása az utóbbi két évtizedben a személyes pénzügyi magánélet folyamatos eltűnéséhez vezetett, hiszen a pénzügyi tranzakciót is felhasználják politikai ellenőrzésre és kereskedelmi haszonszerzésre. Elektronikus pénz már régebb óta létezik, de a tömeges megfigyeléshez szükséges 'nagy adat elemzés' csak mostanában vált lehetségessé. Sem az online, sem a fizikai vásárlás nem biztonságos, mert kormány entitások és hirdető cégek egyre gyakrabban figyelik az egyes személyek preferenciáit, döntéseit és kapcsolatait tartalmazó profilokat. Ezek a profilok, mint valami adat ujjlenyomat, egyediek, és minden egyes vásárlással pontosabbá és könnyebben beazonosíthatóvá válnak. Ez vezet egy olyan világhoz, ahol egy termékre keresve a Google-n, az adott termék célzott hirdetése megjelenhet a Facebookon vagy Instagramon, perceken belül.

Helytől függően a személyes digitális lenyomatnak komoly utóhatásai lehetnek. 2019 nyarán hongkongi diákok tízezrei álltak össze, hogy egy új törvénytervezet ellen tiltakozzanak, amely lehetővé tette a kínai kormány számára, hogy bárkit kiadjon Pekingnek megfelelő eljárás nélkül. Tudták, hogy ha a diákigazolványhoz kapcsolt *Octopus kártyájukat* használják a metrón, követhető a mozgásuk, ezért inkább készpénzért vettek egyszer használatos jegyeket. Ez egyelőre egy biztonságos alternatíva, de a papír- és fémpénzek akár teljesen is eltűnhetnek a nagyvárosokban a következő évtizedben. Akkor már nem lesz mód úgy használni a tömegközlekedést, hogy a személyes és hely adatok ne kerülnének a hatóságokhoz és cégekhez. A digitális ujjlenyomatok ott lesznek mindenhol.

Az emberek különféleképp vélekednek arról, hogy fizetési szokásaikat cégek és kormányok megfigyelik. Egyeseket kicsit zavar, míg mások a magánélet erős megsértéseként ítélik meg, viszont a legtöbbeket ez egyáltalán nem is érdekli. Bárhogyan is, de az tény, hogy a hatóságok nemcsak a pénzkészletet és lehetséges használatát ellenőrzik, hanem gyakorlatilag mindent megtudhatnak az eladókról és vevőkről is. A világ egyre digitalizálódó fizetési rendszerei a személyes magánélet eltűnéséhez vezethetnek.

Van-e más mód?

Négy olyan globális jelenség is van, ami veszélyezteti az emberek boldogulását a 21. század pénzügyi rendszerében: a személyes tulajdon elértéktelenedése, az érték transzfer korlátozása, a pénzügyi centralizáció és a magánélet korlátozása. Az emberek világszerte érzik a nyomást, amint az országok a status quo fenntartásán ügyködnek.

Mi lenne, ha egy olyan új rendszer tűnne fel, ahol a kormányoknak nem lenne lehetőségük tetszőlegesen leértékelni a pénzt, és a személytelen cégek nem tudnák senki számláját befagyasztani vagy utalásait letiltani? Mi lenne, ha a pénz teljesen digitális lenne, és a használatához nem kellene semmilyen hatóság jóváhagyása, csak egy internet hozzáférés?

A 2008-as pénzügyi válság idején valaki elhatározta, hogy felépít egy ilyen rendszert, megteremtve egy igazi pénzügyi forradalom lehetőségét.

2. FEJEZET

Mi a bitcoin?

2008. szeptember 15-én a Lehman Brothers, egy neves befektetési bank, csődöt jelentett, az USA történelmének legnagyobb csődjét. Az 1850-ben alapított Lehman Brothers csődje a globális hitelezési válság csúcsa volt. A cég saját eszközértékét meghaladó összeget fektetett ingatlanfedezetű eszközökbe, melynek egy jelentős része magas kockázatú (subprime) hitel volt. Miután az ingatlan hitelt felvevők egy nagyobb része nem tudott tovább törleszteni, a cég fizetésképtelenné vált, és nem tudott kilábalni.

A bankok Lehman Brothers-be és egymásba vetett bizalma egy pillanat alatt elpárolgott. A válságban a cégek egyre nehezebben jutottak hitelhez, hogy finanszírozzák működésüket. Alapanyagokra, fejlesztésekre vagy fizetésekre fordítandó források híján, sok cég került csődközeli állapotba, számos iparágban. Egy vészjósló, süllyedő spirál kezdett kibontakozni.

Az amerikai kincstár (US Treasury) és jegybank (Fed) gyorsan lépett a gazdasági katasztrófát megelőzendő, pénzt adva a bankoknak, felszínen tartva a pénzügyi rendszert. 2008. október 3-án az amerikai kongresszus több bajba került banknak ítélt mentőcsomagot (2008. évi Gazdasági Vészhelyzeti Stabilizációs törvény). A kormány több száz milliárd dollárt költött a megbicsaklott pénzügyi szektor megsegítésére.

Megjelenik a Bitcoin

Egy pár héttel az amerikai kormány 700 milliárd dolláros bankmentő csomagja után, 2008. október 31-én egy ismeretlen szerző (vagy szerzők) Satoshi Nakamoto név alatt közzétett egy tanulmányt egy új elektronikus fizetési rendszerről, amit Bitcoinnak nevezett el. Satoshi az írást egy kriptográfiai kutatók által használt kiberpunk internetes levelezési listán osztotta meg olyan aktivistákkal, akik olyan eszközökön dolgoztak, amik védik a magánszférát és visszaszorítják az állami megfigyelést és ellenőrzést.

Az írás első érdekessége, hogy a szerző álnevet használt. Satoshi valódi személyazonossága a mai napig sokakat izgató titok. Másodsorban egy olyan dolgot írt le, ami addig nem létezett: egy digitális pénzt, amely nem egy központi autoritáson alapul. Sokan ezt megoldhatatlan problémának gondolták.

Néhány hónap múlva Satoshi el is indította a Bitcoin hálózatot, és hagyott egy utalást a motivációjára: a Bitcoin főkönyv legelső bejegyzésébe, mint egy alapkőbe, ezt a rövid szöveget helyezte el:

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

Ez a *The Times* angol napilap akkori számának egy főcíme: 'A kancellár a bankok második mentőcsomagjának küszöbén'. Satoshi azt üzenthette ezzel az idézettel, hogy a jelenlegi pénzügyi rendszer, ahol bankokat az emberek költségén mentenek meg, nem működik jól. A Bitcoin új decentralizált pénzügyi rendszerét egy kiútként hozták létre.

Ahhoz, hogy megértsük a Bitcoin tudományos innovációját, először a szűkösség fogalmát kell tisztázzuk.

Kétfajta szűkösség

A kézzelfogható dolgok kétféleképpen lehetnek ritkák. Az első típus ember alkotta és mesterséges: gyűjtői darabok, mint limitált kiadású Chanel táskák, Michael Jordan kosaras kártyák, ritka régi évjáratú gyűjtői borok, vagy egy művész számozott alkotásai. Ezt *központosított* szűkösségnek nevezhetjük. Ezek a ritka dolgok viszonylag könnyen hamisíthatók.

A második szűkösség természetadta. Ide tartozik a só (érdekesség, hogy az angol fizetés szó (salary) a sóból származik), üveggyöngyök Ghánában, tengeri kagylók az észak-amerikai őslakos kultúrában, az ezüst Kínában, és persze az arany világszerte. Ezek példák *decentralizált* szűkösségre, és nehezebben hamisíthatók.

Nem véletlen, hogy olyan decentralizált ritka alapanyagok mint a só vagy arany pénzként is használatosak voltak. Első fontos tulajdonságuk, hogy ezeket a javakat nem ellenőrzi egy személy vagy egy csoport, ezért használatuk pártatlan. Második, hogy nehezen hamisíthatók. Harmadik, hogy szűkösségből adódóan könnyű velük gazdasági tranzakciókat végrehajtani, mert nem kell nagy mennyiséget cipelni belőlük.

A szűkösség két formáját az ellenőrzés határozza meg. Központosított szűkösséget egy cég vagy egy személy hoz létre – legyen az a Kínai Népi Bank, a Fed, egy művész, vagy egy nagy multi cég. Ez az entitás, egy *központi hatóság*, ellenőrzi a javak szűkösségét a létrehozáson, kiadáson, visszavásárláson és elkobzáson keresztül.

A decentralizált, ritka javakat a természet hozta létre, azaz nem egy központi hatóság állítja elő. Nincs kibocsátás vagy gyártás, hanem inkább összegyűjtésről vagy betakarításról be-

szélhetünk. Amikor olyan természetéből adódóan ritka anyagot bányásznak, mint az arany vagy olaj, a bányász az eleve ott létező anyagot termeli ki.

Az arany esetében, a felhalmozáshoz nem kellett senkitől engedélyt kérni, legfeljebb a bányaterület tulajdonosától. Tehát nincs egy központi hely, ahonnan az összes arany útjára indulna, és nincs egy globális autoritás, akinek hatalmában állna az arany bányászatát korlátozni vagy növelni a kínálatot.

Ez a fő különbség a központosított és a decentralizált szűkös javak között, kiváltképpen a pénzként is használatosaknál.

Mitől lehet jobb a decentralizált pénz?

Az előzőek szerint a központosított pénzek letagadhatatlan tulajdonsága, hogy a kibocsátó tetszőlegesen növelheti a mennyiséget, inflálhatja a pénzt, új pénzt nyomtatva. Bár ez elnyomó rezsimekben gyakrabban és durvábban fordul elő, mint demokráciákban, de minden társadalomban megfigyelhető.

A *Bugsy* című filmben a főszereplő befektetőknek ad el részesedést a Rózsaszín Flamingó kaszinóból, többször is. Mindenkinek 20%-ot ad el tízezer dollárért. Tucatnál is több befektetőnek ad el részesedést, valótlanul magasabb részesedést mondva nekik. Mindegyikük úgy gondolja, hogy 20% az övék, de a valóságban jóval kevesebb. Bugsy természetesen jól jár, hiszen több pénzt zsebel be.

Minden központosított jószág ki van téve ennek az ösztönzési problémának. A központi autoritás tud több darabot létrehozni, ezzel felhígítva az összes tulajdonos által birtokolt érték. A központi bankok szinte mindig jó célokra hivatkozva nyomtatnak pénzt: infrastruktúra építés, jóléti intézkedések, vagy gazdasági válság kezelés. Viszont emlékezzünk a Cantillon hatásra az első fejezetből: ennek a hatalomnak az elfogadható gyakorlása is jobban előnyhöz juttathatja a gazdagokat és a hatalomhoz közelebb állókat, a szegényebbek és gyengébbek kárára. A pénz nyomtatásának lehetősége egy morális kockázatot hordoz.

Hígulás a decentralizált javaknál is előfordulhat. Egy új technológia sokkal olcsóbbá teheti egy természetesen előforduló áru kitermelését, aminek hatására a piacot elöntheti az új kínálat. Ha egy árucikk elveszti szűkösségét, sokkal gyengébb és kevésbé megalapozott lesz. Ez történt a sóval, a kagylókkal és üveggyöngyökkel: már nem használatosak pénzként. Ezeket nehéz volt nagy tömegben begyűjteni vagy előállítani, de a technológiai fejlődésnek köszönhetően ez ma már nem így van.

Az arany az egyik kivétel, és egészen jól tartja értékét több ezer évnyi bányászat után is. Habár az aranynak van ipari és dekorációs hasznosítása is, bányászatának örökös nehézsége miatt egy viszonylag jól megalapozott pénz lett, és stabil vásárlóereje miatt nagyon jó értéktároló. Bizonyos országokban még napjainkban is értékőrzőként is használják az aranyékszereket gazdasági válságok idején. Az arany hátránya a súlya, azaz fizikai mivolta, ami nehezíti a tárolását, megőrzését és mozgatását.

A bitcoin több szószólója szerint a bitcoin előbb-utóbb leváltja az aranyat, mint a hosszú távú értékmegőrzés preferált formáját. Amint ebben a fejezetben megmutatjuk, a bitcoin decentralizált, az aranynál szűkösebb, és sokkal könnyebb szállítani és biztonságosan tárolni.

Decentralizált Digitális Szűkösség

Az internet elterjedésével mindenféle információ digitalizálhatóvá és könnyen terjeszthetővé vált. Egy digitális adatfájlt sokkal egyszerűbb és olcsóbb lemásolni mint egy fizikai tárgyat.

Az e-kereskedelem elterjedésének fontos előfeltétele volt a pénz digitalizációja, mert ezáltal a fizetéshez semmilyen fizikai átadásra nincs szükség. Minden elküldhető az email vagy weboldal betöltés gyorsaságával, ami hatékonyabbá és globálisabbá teszi a kereskedelmet. A fiat pénzek digitális változatának létrehozói a bankok, feldolgozói a hitelkártya hálózatok (Visa, MasterCard), illetve kereskedő cégek (Alibaba, Amazon, Apple) és internetes fizetési feldolgozók (WeChat, PayPal, Square).

Mivel ők a feldolgozói a digitális pénznek, ezek a cégek cenzúrázhatnak is tranzakciókat. Akár el is vehetnek pénzt, le is zárhatnak fiókokat, amint ez nem egyszer megtörtént a felhasználó beleegyezése nélkül. Továbbá mivel ezek központosított entitások, könnyen kormányzati nyomás alá kerülhetnek, illetve a kiberbűnözőket is jobban vonzzák, aminek gyakran pénz- vagy adatlopás a vége. A bitcoin előtt a digitális pénz két lehetőség közül választhatott: vagy a mesterségesen biztosított szűkösség, vagy egy központi ellenőrző entitás. Nem látszott megoldás valódi szűkösség létrehozására a digitális világban.

Satoshi Nakamoto 2008. október 31-én tette közzé újszerű megoldását: bemutatta a bitcoint, egy új digitális pénzt, aminek szűkössége a digitális világban létező természetes szűkösségből származtatható – ez a ritka számok szűkössége.

A prímszámok viszonylag ritkák. Egy prímszám, mint a 2, 3, 5, stb., csak önmagával és eggyel osztható.

Ahogy a nagyobb számok felé haladunk, a prímszámok egyre ritkábbak. Például 1 és 100 között 25 prímszám van. Azt gondolhatnánk, hogy 250 prímszám van 1 és 1.000 között, de valójában csak 168 van. Száz milliárd fölött már hihetetlenül megritkulnak a prímszámok, olyannyira, hogy világszerte matematikusok hada állandó jelleggel keresi a következő legnagyobb ismert prímet.

A bitcoin hálózatban az új érmék létrejötte egy globális versengés eredménye, ahol a résztvevők prímekhez hasonló ritka számok után kutatnak. Ez a decentralizált digitális szűkösség alapja. Ez adja Satoshi találmányának a mélységét. A bitcoin előtt létezett áruk vagy teljesen központosítottak voltak (arany World of Worldcraftban), fizikaiak (arany), vagy végtelenül másolhatók (MP3 fájlok). Decentralizált, digitális szűkös áru nem létezett a bitcoin megjelenése előtt.

Bitcoin bányászat: decentralizált fizetésfeldolgozás

A bitcoin decentralizáltsága azon alapszik, hogy hasonlatos a szűkös természetes árukhoz mint az arany, és nehéz kitermelni. Hasonlóan az arany bányászatához, a bitcoin bányászat egy temérdek anyagtengerben megbúvó ritka dolgok keresése. Amint egy bitcoin bányász megtalál egy megfelelő ritka számot, mások azt könnyűszerrel ellenőrizhetik, hasonlóan az aranyhoz, aminek a valódisága viszonylag egyszerűen ellenőrizhető.

A bitcoin bányászok nem csákányt vagy markológépet használnak, mint az aranybányászok, hanem erős számítógépekkel kutatják a ritka számokat. Egy megtalált ilyen ritka számot *munka bizonyítéknak* hívnak (‹proof-of-work›), mert bizonyítja, hogy valaki sok munkát fordított a megtalálására.

A bányászathoz nem kell semmilyen központi entitástól engedélyt kérni, mint ahogy az aranyál sem (a terület felügyelőjén kívül): bárki letöltheti a bányász szoftvert és elkezdeti a keresést.

Nem kell hozzá különleges földterület, mint az aranybányászathoz, csak megfelelő számítógép hardver és az azt tápláló áram. Ennek megfelelően világszerte bányászok ezrei egymástól függetlenül és egymással versengve keresik a bitcoint, pontosabban a helyes munka bizonyítékot.

A független bányászok hadának köszönhetően a bitcoinnak nincs egy központi sebezhető pontja. Ez merőben eltér a központosított rendszerektől. Ha a Visa hálózat nem működik, senki sem tud a Visa kártyájával fizetni. Hasonlóan járna a PayPal vagy az Amazon is, ha valamiért leállna a rendszerük. Ezekkel a cégekkel ellentétben a bitcoinnak nincs központi autoritása vagy meghibásodási lehetősége. Nincs senki, aki el tudná érni, hogy cenzúrázzanak egy bizonyos tranzakciót. A bitcoin bányászok megállíthatatlan hálózata egy kritikus szolgáltatást működtet, feldolgozza a tranzakciókat, egy központi entitás sebezhetősége nélkül.

Hogyan működnek a bitcoin tranzakciók?

De hogyan is működik egy bitcoin tranzakció?

Egy analógiaként nézzük meg, hogyan működik egy banki főkönyv. Ha egy bank ügyfele bemegy a bankba, hogy átutaljon egy összeget egy másik ügyfélnek, a bank egyszerűen megterheli az utaló számláját, és jóváírja az összeget a fogadó számláján. A folyamat során mindössze két, a bank főkönyvében tárolt számot változtatnak meg: az egyikből kivonják, a másikhoz hozzáadják az összeget. Szó sincs arról, hogy a banki ügyintéző a páncélteremben kiszámolná az összeget az egyik ügyfél elkülönített készpénzhalmából és áttenné a másik ügyfeléhez, hiszen ilyenek nem is léteznek. A papíron vezetett könyvelés egy olyan újítás volt, ami sokkal egyszerűbben valósítja meg a pénz átadását. Az ehhez hasonló műveletet a bitcoinnál is *tranzakciónak* hívjuk.

A bitcoin a főkönyvnek megfelelő információt speciális formában, egy *blokkláncban* tárolja. Többezer ember futtatja a bitcoin validációs szoftverét, ők ellenőrzik folyamatosan a blokkláncot, nem pedig egy központi entitás. Mindenki, aki futtatja a szoftvert, rendelkezik a teljes blokklánc másolatával, és ellenőriz minden új bejegyzést. Ezt hívjuk *teljes csomópont* ('full node') futtatásnak. Az összes csomópont érvényesíti ugyanazokat a bitcoin szabályokat, ezáltal senki sem tudja megmásítani a bejegyzéseket, pénzt lopva el mástól vagy nem létező pénzt költve el. A bitcoin blokklánc egy *publikus blokklánc*, mert bárki megnézheti a tranzakciókat.

Egy bitcoint használó utalása hasonló egy banki átutaláshoz vagy egy csekk íráshoz. Meghatározzák a címzettet, az összeget, és aláírják az utalást. Természetesen az aláírás az nem pár tollvonás egy papíron, hanem egy kriptográfiai *digitális aláírás*.

Az aláíráshoz szükség van egy titkos adatra, amit csak a küldő ismer. Ezt a titkos adatot nevezzük *privát kulcsnak*. A privát kulcs segítségével tudja a küldő elkészíteni a digitális aláírást, amiből a fogadó ellenőrizni tudja, hogy a küldő valóban rendelkezik a küldött összeggel.

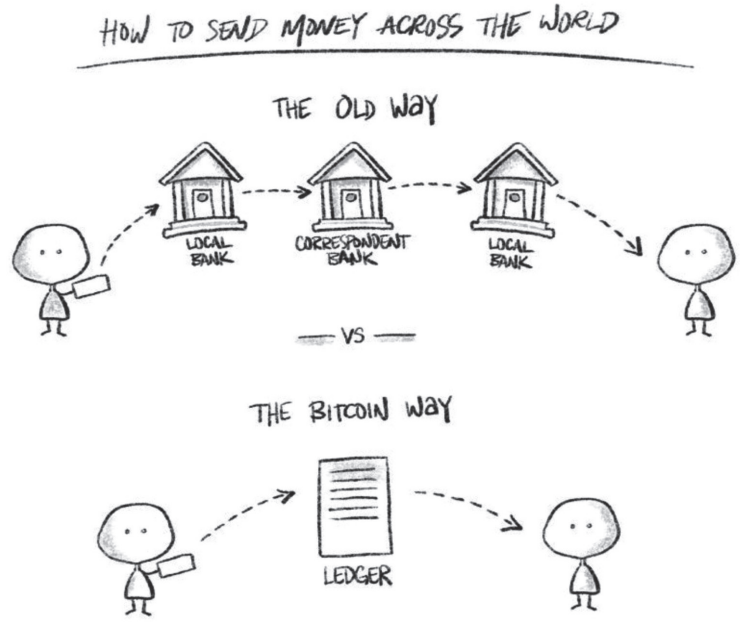
A felhasználók a bitcoinjaikat egy *tárcában* tartják, ami egy szoftver a számítógépen vagy mobiltelefonon vagy egy cél esz-

közön. A világszerte éppen futó tárcák folyamatosan kezdeményeznek új tranzakciókat, de ezek nem egy központi feldolgozóhoz futnak be. A világ bányászai egymással versengenek, hogy beírják a tranzakciókat a főkönyvbe. A számítógépeikkel keresik a megfelelő ritka számot. Átlagban tíz percenként valahol egy bitcoin bányász talál egy megfelelő munka bizonyítékot, és ezt egy *blokkba* foglalja az éppen feldolgozásra váró tranzakciókkal együtt. Ezt a blokkot nyomban kihirdeti validálásra a bitcoin hálózaton.

Egy új blokk olyan, mint egy új oldal a bitcoin globális főkönyvében, és a hálózat csomópontjai ellenőrzik a blokk tranzakcióinak érvényességét. Bárki futtathat csomópontot, úgyhogy felhasználók ezrei validálnak minden egyes új blokkot. Amint a hálózat egyetértésben elfogadja az új blokkot, az véglegesen hozzáadódik a blokklánchoz, a benne lévő tranzakciókkal együtt. Minden blokkal keletkezik 6,25 egység új bitcoin is, ami a szerencsés bányász jutalma. Egy tranzakció a létrejöttétől számítva egy órán belül nagy valószínűséggel bekerül egy blokkba, és véglegesedik a blokkláncon.

Blokkáncnak nevezzük az összes blokk láncolatát, amik mint egy könyv lapjai, sorrendben követik egymást. Ily módon a blokklánc a megmásíthatatlan története az összes tranzakciónak, ami valaha létrejött a bitcoin 2009-es indulása óta.

A több ezer futó csomópont alkotja a bitcoin hálózatot. Minden csomópont egymástól függetlenül ellenőrzi a bányászok által kihirdetett új blokkokat. Egy csomópont futtatáshoz nincs szükség nagy kapacitásra, egy átlagos mai laptop bőven elég hozzá. Az, hogy viszonylag könnyen lehet csomópontot futtatni, hozzájárul ahhoz, hogy a hálózat decentralizált maradjon.



A bitcoin pénzügyi politikája

A központi bankok gyakran változó és nem átlátható pénzügyi politikájával szemben a bitcoin pénzügyi politikája teljesen transzparens és kőbevésett.

Hogyan keletkezik új bitcoin? Amint említettük, a bányász aki elsőnek talál egy munka bizonyítékot és összecsomagolja egy tranzakció listával egy új blokkba, blokk jutalomban részesül. Jelenleg a blokk jutalom 6,25 bitcoin, de ez az összeg négy évente feleződik, azaz 2024-től már csak 3,125 lesz, 2028-tól 1,5625, és így tovább.

Ha egy bányász csalni próbál, és egy nagyobb jutalmat ítél magának, a csomópontok elutasítják ezt a blokkot. A teljes cso-

mópontok ellenőriznek minden tranzakciót minden közzétett blokkban (beleértve a jutalom tranzakciót is), és ha bármi eltérés van a szabályoktól, nem adják hozzá a saját blokklánc másolatukhoz. Ez hasonló ahhoz, amikor egy bank elutasít egy elégtelen fedezettel bíró utalást vagy csekket. A végeredmény az, hogy nem lehet csalni, nem lehet bitcoint hamisítani. A csomópontok elutasítanak minden tranzakciót, ami nem létező bitcoint próbál elkölteni, és minden blokkot, ami ilyen tranzakciót tartalmaz.

Egy érvénytelen blokk sokba kerül egy bányásznak, hiszen a megtalálására fordított energia kárba vész, ha a blokkot elutasítják. Ha csak kevés csomópont létezne, egy rosszindulatú bányász lefizetéssel vagy máshogy rávehetné a pár csomópontot, hogy fogadják el az érvénytelen blokkot. Mivel valójában több ezer csomópont van, szétszórva a világban, és egymást nem ismerik, ez a gyakorlatban lehetetlen. Végeredményben a bányászat decentralizáltsága és nagy erőforrás igénye őrzi a bitcoin biztonságát.

Satoshi már induláskor meghatározta az összes bitcoin mennyiségét 21 millióban. Jelenleg ennek 90%-a már ki lett bányászva, tehát majdnen 19 millió bitcoin van forgalomban. A maradék a következő években fog létrejönni a bányászoknak adott jutalom formájában, az előre meghatározott, csökkenő menetrend szerint.

Blokklánc technológia: még várat magára

A bitcoin megjelenése után több projekt indult útnak azzal a céllal, hogy lemásolja vagy javítsa a bitcoint. Egy népszerű megközelítés a bitcoinból a blokklánc technológiáját emeli ki is igyekszik más felhasználási területen felhasználni. 2014 óta

sok ismert cég próbált blokkláncot meghonosítani különböző területeken, dollármilliókat befektetve. A *blokklánc technológia* egy felkapott fogalom lett a médiában.

Sajnos, a legtöbb ilyen próbálkozás kicsit olyan, mintha egy villástargoncát használnánk amikor bevásárolunk a sarki zöldségesben. A blokklánc tökéletesen működik az eredeti célra (egy decentralizált pénz főkönyvének tárolására), de gyakran túl lassú, pazarló vagy egy sor más felhasználási esetben működésképtelen (mint pl. blokkláncon tárolt egészégügyi, gyümölcskereskedelmi, vagy időjárási adatok).

A bitcoin négy fontos alkotóeleméből a blokklánc csak az egyik. Az első, hogy a bitcoin egy szűkös digitális áru. A második a teljes csomópontok peer-to-peer hálózata, amely ellenáll a leállításnak és a cenzúrának. A harmadik a matematikai munka bizonyítékon alapuló, versengő bányászat, ami véd az esetleges csalásoktól. A negyedik a teljeskörűen és nyilvánosan átvilágítható blokkláncon történő adattárolás. Ez a négy technológia szorosan összefügg, és ha egy részt eltávolítunk, a maradék sokkal kevésbé lesz hasznos.

Egy teljesen digitális eszköznél, mint a bitcoin, van értelme nyilvános blokklánc tárolást használni. Minden bitcoin létrejötte és minden tranzakciója csalhatatlanul tárolható. De a valós világban létező dolgokból, mint pl. kávé termés vagy egészségügyi adatok, származó információ esetén nem lehet garantálni a csalhatatlanságot, hiszen még az adatfelvétel során vagy előtt történhet hiba, figyelmetlenség, vagy szándékos csalás. Szükség van egy központi szereplőre, aki tanúsítja az adatokat, ami mellett értelmét veszti a blokklánc használata.

Ennek ellenére, hatalmas összegeket fordítottak blokklánc kutatásra, a decentralizált pénzen kívül más felhasználást ke-

resve. E könyv írásáig senkinek sem sikerült olyan nagyszabású blokklánc alapú adattárolási rendszert létrehoznia, aminek lényeges előnyei lennének más hagyományos megoldásokkal szemben.

Mi a helyzet a többi kriptovalutával?

Nemcsak a bitcoin blokklánc megoldását próbálták lemásolni, hanem több más kriptovalutát is létrehoztak már. Ezek a bitcoinhoz hasonlatos digitális pénzek, és szintén digitális kriptográfiai aláírásokat használnak. Az ún. altcoinok és tokenek jó része nem decentralizált, vagy egyszerűen csalás. A Bitconnect projekt egy hírhedt példa kriptovaluta átverésre.

Néhány kriptovalutának lehet jogos fehasználása. Ilyen a Monero (XMR) vagy a Zcash (ZEC), melyek a bitcoinnál privátabb tranzakciókat tesznek lehetővé, vagy az Ethereum (ETH), amely platformra különböző alkalmazásokat lehet fejleszteni. Nagy cégek is kísérleteznek kriptovalutákkal. A Facebook bejelentette a Libra kriptovalutát, ami akár el is terjedhet, a cég többmilliárdos felhasználó bázisára építve. Viszont a Libra központosított, és nem lesz cenzúra ellenálló, sem szűkös. (Fordító megjegyzése: a Libra nem valósult meg.)

Vannak csoportok, melyek Satoshi sikerét elvtelen módon próbálták lemásolni, olyan projektekkel, amelyek nevében a Bitcoin szerepel. Így több felhasználó elbizonytalanodhat, hogy melyik is az igazi bitcoin. Fontos a bitcoin szimbólumát, a BTC-t keresni váltókon vagy tárcákban. Egy-egy ilyen variáns a 'bolondok aranya', hasonlónak tűnik, de központosított, és jóval kisebb az értéke. Ebbe a kategóriába tartozik a *Bitcoin Cash* (BCH), *Bitcoin Gold* (BTG) és a *Bitcoin Satoshi's Vision* (BSV).

Összefoglalás

A bitcoin egy lényeges mérnöki áttörés, ami alternatívát kínál az aktuális pénzügyi rendszernek.

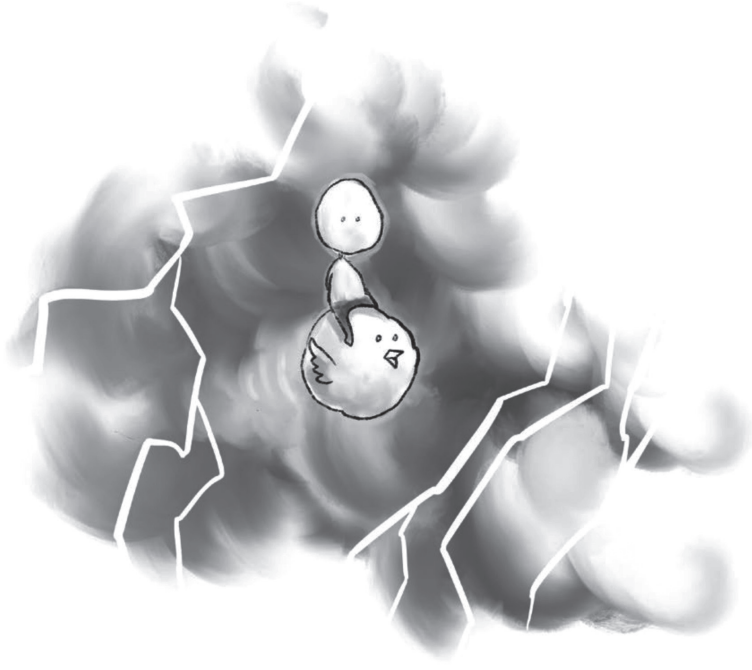
A bitcoin egy digitális pénz, amivel kényelmesen lehet nemzetközi tranzakciókat végrehajtani, hiszen napok helyett percek alatt lezárul.

A bitcoin egy szűkös eszköz, ami védelmet jelenthet az inflációval szemben.

A bitcoin decentralizált, így nincs senki, aki képes lenne cenzúrázni utalásokat.

A bitcoin a világon az eddig egyetlen decentralizált, digitális, szűkös pénz.

A bitcoinban benne van a lehetőség, hogy alaposan megbolygassa a jelenlegi pénzügyi rendszert.



3. FEJEZET

A bitcoin árfolyama és volatilitása

Jogi nyilatkozat: Ezen könyv szerzői nem befektetési szakemberek. Ez a fejezet a bitcoin árfolyammozgásának és volatilitásának lehetséges okait vizsgálja, és nem nyújt befektetési tanácsokat.

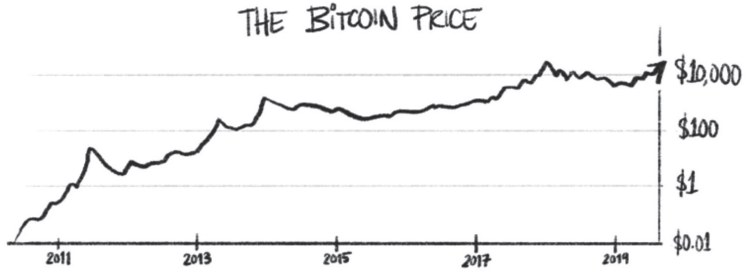
Amit mindenki tudni akar: Miért is értékes a bitcoin? Miért emelkedett ekkorát az árfolyama? Miért olyan volatilis? Miért ér bármit is a bitcoin, ha a dollárral ellentétben a bitcoin mögött nincs gazdaság, vagy ami még cinikusabb, bírságokkal és börtönbüntetéssel való fenyegetés?

Egy eszköz árfolyama akkor mozog, ha a vevők és az eladók között nincs egyensúly. A bitcoin esetében ezeket az egyensúlytalanságokat néhány olyan tényező határozza meg, amelyek a hosszú, közép- és rövid távú kilátások tekintetében különböznek egymástól.

A hosszú távú kilátások

Az elmúlt évtizedben a bitcoin árfolyama az egy cent alatti értékről a közel 20.000 dolláros csúcsra emelkedett. Az árfolyama 2019 augusztusában 11.000 dollár körül volt.

A bitcoin árfolyama a kezdetektől napjainkig (logaritmikus skála)



A bitcoin szűkös. A kínálata 21 millió érme, a második fejezetben leírtak szerint.

A bitcoin rögzített token készlete és a kibocsátás átlátható módja azért vonzó a vásárlók számára, mert az alternatívája – a fiat pénz – általánosságban véve gyengülésnek, ennélfogva pedig inflációnak van kitéve, ami azt jelenti, hogy ugyanaz a pénzmennyiség minden évben kevesebbet ér. Hosszú távon valószínű, hogy egyre több ember fogja vonzónak találni a bitcoint, mert a kormányok nem tudnak belőle többet nyomtatni, a tranzakciókat nem tudják blokkolni, és nehéz elkobozni.

Az összes kibányászott bitcoin összértéke még mindig csak 200 milliárd dollár. Ezzel szemben az összes kibányászott arany értékét nagyjából 9 billió dollárra becsülik. Az arany összértékének mindössze 2%-ával rendelkező bitcoin piaca kicsi, így érzékenyebb az árfolyam-ingadozásokra. A napi kereskedési volumen is viszonylag kicsi: hozzávetőlegesen 10 milliárd dollár naponta, szemben az arany napi 300 milliárd dollárjával. Mivel a *likviditás* kicsi, vagyis az a mennyiség, amelyet egy adott időszakban meg lehet vásárolni vagy el lehet adni, még a kis vevők vagy eladók is nagy hatással lehetnek az árfolyamra. Ahogy a bitcoin elfogadottsága bővül, és globális eszközosztályként növekszik, úgy fog csökkenni a volatilitása. Ez több évtizedet is igénybe vehet.

A középtávú kilátások

Ha a bitcoint hónapok és évek távlatában nézzük, az árváltozás legnagyobb mozgatórugói a bányászati költségek, a nagy intézményi vevők kereslete és a feleződések.

A bányászatnak költségei vannak: berendezések, adatközponti műveletek, villamosenergia. Ezeket a kiadásokat fiat valutában kell megfizetni. Ezért a legtöbb bányász rendszeresen eladja az általa bányászott bitcoin egy részét vagy egészét, hogy kifizesse a működési költségeket, amelyek nagyjából havi 250-300 millió dollárt tesznek ki. E könyv írásakor ez a havonta kibányászott bitcoin értékének 40-50%-a.

A bitcoin iránti ilyen jellegű kereslet rendszerint az intézményi vevők, a tehetős magánszemélyek, a családi irodák és az alapítványok részéről érkezik, akik kriptovalutákba szeretnének fektetni, és jellemzően a bitcoinnal kezdik.

Az árat középtávon befolyásoló másik fontos tényező a *feleződés*. A 2. fejezetben leírtaknak megfelelően a bányászati jutalom négyévente a felére csökken. A bitcoinnak eddig két feleződése volt, 2012-ben és 2016-ban. Mindkét feleződés olyan kínálati korlátot hozott létre, amely fokozta a volatilitást. (Fordító megjegyzése: 2020-ban volt a harmadik feleződés.)

A bitcoin emelkedő árfolyama általában több spekulánst vonz, a lakossági befektetőktől kezdve, akik csak 100 dollár értékű bitcoint akarnak vásárolni, egészen az intézményi befektetőkig, akik több millió dollár értékben vásárolnak. Ez viszont felhajtja a bitcoin árát, mivel a média figyelme és a kimaradástól való félelem csak olaj a tűzre. Ez a lendület nagy árbuborékokat hozott létre, amelyek 80%-os vagy annál is nagyobb árzuhanás-

ban végződtek. Könnyen lehet, hogy ezek az árciklusok a jövőbeni feleződésekhez közelítve folytatódnak.

A rövid távú kilátások

A központi hatalom hiányának van egy lényeges mellékhatása: a volatilitás.

Az, hogy hol kereskednek a befektetők a bitcoinnal, összefüggésben áll a rövid távú volatilitás okaival. Erre számos hely létezik, például a *fiat-kriptovaluta tőzsdék*, amelyek lehetővé teszik, hogy közvetlenül fiat pénzt cserélj bitcoinra, a *peer-to-peer tőzsdék*, amelyekhez személyes találkozó szükséges és a *kriptovaluta-kriptovaluta tőzsdék*, amelyek csak a kriptovaluták közötti cserét teszik lehetővé. Mivel a kereskedők a volatilitásból igyekeznek profitálni, vannak olyan *tőkeáttételes tőzsdék*, ahol a letéti összeg akár 100-szorosával is lehet kereskedni.

A kripto tőzsdék elsősorban online léteznek. Ezért az év minden percében működnek, és közvetlenül szolgálják ki a lakossági befektetőket. Ezzel szemben a hagyományos piacok jellemzően egy nagy pénzügyi központban, például Londonban, New Yorkban vagy Hongkongban vannak, a kereskedéshez pedig hétfőtől péntekig csak körülbelül 7,5 órán át tartanak nyitva, és elsősorban brókerek, nem pedig lakossági befektetők használják őket.

Mivel bárki küldhet és fogadhat bitcoint egy számítógép és internet kapcsolat segítségével, egy vállalkozó számára viszonylag könnyű egy egyszerű tőzsdét létrehozni. Mivel a bitcoin nem minősül értékpapírnak, a tőzsdékre, amelyeken kereskednek vele, kevésbé szigorú szabályozási előírások vonatkozhatnak, mint a hagyományos piacokra. Ezenkívül a kripto tőzsdék olyan barátságos fogadó országokat is választhatnak, mint Málta, a Seychelle-szigetek vagy a Fülöp-szigetek, mivel nincs szükségük fiat bankszámlára, és a csapataik távmunkában is dolgozhatnak. A tőzsdére történő befizetés azt jelenti, hogy bízol abban, hogy a tőzsde biztonságban tartja a pénzeszközeidet. Sajnos sok tőzsdét nem megfelelően irányítanak. Bizonyítékokkal alátámasztott, nagyszabású lopást eredményező hanyagság vagy hozzá nem értés miatt az Mt.Gox, a Bitfinex és a Quadriga együttesen több tízezer bitcoint (több milliárd dollár értékben) veszített el.

Tanulság az olvasóknak: számos tőzsdét feltörtek, vagy azok elvesztették az ügyfeleik bitcoinjait. Az olvasók mindig legyenek óvatosak, amikor tőzsdét használnak, és csak annyi bitcoint kockáztassanak, amennyit hajlandóak elveszíteni.

A bitcoin lakossági online kereskedésre való alkalmassága hozzájárul rövid távú volatilitásához. Míg a központi bankok általában a volatilitás minimalizálására törekszenek, addig a kereskedők az áringadozást részesítik előnyben, mert az a jövedelmező.

A bitcoin árfolyam-ingadozása egy hónaptól akár egy percig terjedő időintervallumon belül is szélsőséges lehet. 2019. január 1-jén egy bitcoin 3500 dollárba került. 2019 augusztusában már közel 11 000 dollárt ért. A napi 20%-os áringadozások normálisnak tekinthetők. A befektetők számára ez ijesztő lehet, de a spekulánsok számára maga a paradicsom, hiszen az ármozgásból profiltálnak.

A hagyományos részvény- vagy kötvénypiacokkal ellentétben a bitcoin nem rendelkezik olyan üzleti fundamentumokkal, amelyek meghatározzák az árstabilitást. A bitcoinnak nincsenek alkalmazottai, nincs termékteljesítménye, és cash flow-ja (pénz-

forgalma) sem. Az efféle rövid távú teljesítménymutatók hiánya a kereskedés technikai elemeire helyezi a hangsúlyt, ami gyakran zéró-összegű. A spekulánsok számára a kriptovalutával való kereskedés az online póker egy másik formája, amely hosszú távon kisebb előnyt kínál, és amelyet a nappalijuk kényelemében játszhatnak.

A hagyományos piacokhoz hasonlóan a bitcoin árfolyama is reagál a fontos hírekre – de nem minden esetben mozdul felfelé a jó hírekkel, vagy lefelé a rossz hírekkel. Például 2013-ban az Mt.Gox-ot, az akkori legnagyobb tőzsdét hackerek támadták meg, emiatt jelentős áresés következett be. 2018-ban viszont a Binance-t, napjaink legnagyobb tőzsdéjét törték fel mintegy 40 millió dollárért, a bitcoin árfolyam viszont emelkedett.

Ahogy a bitcoin egyre értékesebbé és likvidebbé válik, a volatilitás valószínűleg csökkenni fog. Ez hasonlít a híres részvények árfolyam-ingadozásához a kevésbé ismert részvényekhez képest. Például egy egyéni kereskedőnek sokkal nehezebb az Apple árfolyamát mozgatnia, mint egy filléres részvény árfolyamát.

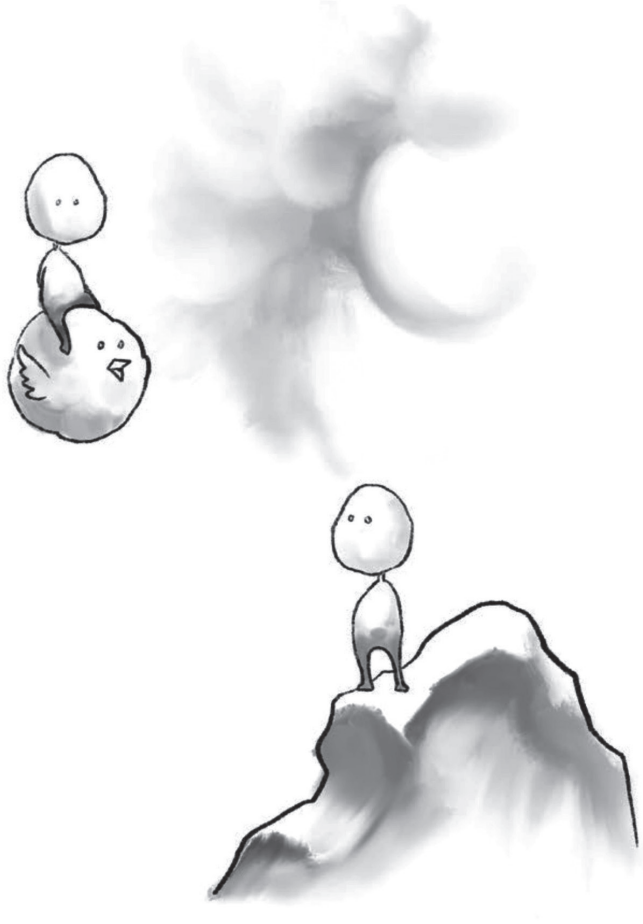
A bitcoin egy egyedülálló és igen kockázatos kerkedési eszköz. A kereskedők számára a bitcoin vonzereje, valamint a likviditás hiánya és a tőkeáttételes kereskedés elérhetősége jelentős rövid távú volatilitást eredményez az árfolyamában.

Összefoglaló

A kezdetektől fogva a bitcoin ára a rögzített kínálat és a növekvő kereslet függvényében felfelé és jobbra mozog. Rövid távon az árfolyam spekulációnak, piaci manipulációnak és hatalmas volatilitásnak van kitéve.

Végső soron a bitcoin rögzített token készlete és decentralizált jellege adja az értékét és az árfolyam-ingadozását.

Ha a bitcoin az értékmegőrzésen túl tovább fejlődik és a digitális gazdaságot képviseli (csakúgy, mint ma a fizikai gazdaságok esetében a fiat valuta), akkor fizetőeszközzé és elszámolási egységgé is válik. Ezen a ponton a volatilitás csökkenhet, mivel a bitcoin inkább az értékcserén, mint a spekulatív tevékenységen alapul. Addig is az árfolyam az e fejezet középtávú és rövid távú bekezdésében leírt piaci erők szeszélyétől függ, és továbbra is drámaian ingadozik.



4. FEJEZET

A bitcoin és az emberi jogok

A bitcoin lehetővé teszi, hogy az emberek a munkájukkal megkeresett értéket digitális információ formájában tárolják. Ez segít elejét venni annak, hogy rezsimek vagy cégek önkényesen ellenőrizzék, hogy az emberek mit csinálnak a pénzükkel, hogyan tárolják azt, vagy adják át egymásnak. Ennek a forradalmi pénzügyi változásnak az emberjogi vonatkozásai már ma is érződnek, és a jövőben még erőteljesebbé válnak a világban, elsősorban a diktatúrákban, de a liberális demokráciákban is.

Az első fejezetben bemutattunk néhány történetet, Nigériától Venezueláig, olyan emberekről, akiknek a magas infláció, a pénzügyi megfigyelés, a bankok elérhetetlensége, vagy éppen a nem működő gazdasági infrastruktúra okoz gondot.

Ezek nem egyedi esetek. Az Emberjogi Alapítvány (Human Rights Foundation) szerint a Föld lakosságának nagyjából a fele él önkényuralmi rendszerekben. Ez kb. 4 milliárd embert jelent, Kubától Fehéroroszországig és Szaúd-Arábiától Vietnámig, akiket valamilyen szinten elnyom a kormányuk. Sokan gazdasági menekültek vagy politikai elítéltek. Ezek az emberek nem mindig élvezik a törvény hatalmát, nincs meg a lehetőségük hogy tüntessenek a változásért. Időnként még az amerikai és európai

kormányok is pénzügyi elnyomásban részesítik polgáraikat, egyre növekvő megfigyeléssel, inflációval. Bankmentőcsomagok, külföldi katonai beavatkozások, megerősített határvédelem és támogatott juttatások mind olyan megkérdőjelezhető tevékenységek, amiket a pénznyomtatás tesz lehetővé.

Amikor egy ország lakói olyan központosított fizetési szolgáltatásokat kell használjanak, mint a WeChat Kínában, amely emberek millióiról gyűjt adatokat, vagy amikor egy emberjogi szervezet bankszámláját befagyasztja egy diktátor, vagy amikor egy országra kivetett szankciók az embereket büntetik olyan bűnökért, amiket a nem megválasztott vezetőik követtek el, akkor a bitcoin egy kivezető utat jelenthet.

Satoshi innovációja valós segítség lehet a bankszámla vagy hivatalos iratok nélkül élők millióinak abban, hogy pénzt birtokoljanak és használjanak. Egy mobiltelefonnal és internet kapcsolattal a világ legkiszolgáltatottabb emberei is gyorsan és olcsón fogadhatnak bárkitől bitcoint, cenzúrázás vagy elkobzás veszélye nélkül.

Ezzel összhangban, a bitcoin kezdi átírni a határon átívelő pénzküldés és utalványozás rendszerét, és magában hordozza a lehetőséget, hogy több társadalmi problémán is enyhítsen. A bitcoin hozzájárul egy valóban globális áru és szolgáltatás piachoz és egy igazságosabb játéktérhez.

Legyél a saját bankod

Egyes országokban, mint Bahrein, Oroszország vagy Zimbabwe, a kormány diktatorikus ellenőrzés alatt tartja a bankrendszert, ami így a sikkasztás és korrupció melegágya. A bitcoin világban a rezsimek és megacégek kevesebb kontollal bírnak, az emberek viszont több szabadsággal és egyéni választással.

A bitcoin egy látra szóló instrumentum *(bearer instrument)*, ami azt jelenti, hogy a tulajdonosa teljes mértékben rendelkezik felette. Továbbá amikor bitcoint utalunk, nincs olyan köztes fél, aki ezt cenzúrázhatná vagy visszaélhetne a személyes adatokkal. Ez a védelem hasznos csalók és tolvajok ellen, de tisztességtelen cégek vagy kémkedő kormányok ellen is. Ez egyetlen másik pénz típusra vagy fizetési szolgáltatásra sem igaz.

Készpénz a matrac alatt – ez egy bevett módszer sok problémás gazdaságban élő ember számára. Ez messze nem ideális megoldás, mert a készpénzt nehéz biztonságosan tárolni és nehézkes postázni is. Egy hatósági szerv megjelenhet az ajtónál és fizikailag elkobozhatja. Ezzel szemben a bitcoint könnyebb tárolni és biztosítani, mert a privát kulcsot vagy titkos jelszót el lehet tárolni papíron, számítógépen, vagy egy pendrive-on, vagy akár fejben. A bitcoint könnyen le is lehet tagadni, és a hatóságoknak nem nagyon van módja ezt ellenőrizni, vagy a letagadott bitcoint elkobozni.

Menekülés a magas infláció elől

Irán vagy Szomália lakosai olyan rezsimek alatt élnek, amelyek nyakló nélkül nyomtatnak pénzt, megsarcolva a megtakarításokat. Az inflációval minden központi bank foglalkozik. Az elfogadott nézetük az, hogy a mértékletes készpénz hígítás kívánatos, mert mozgásban tartja a piacokat. A demokratikus rendszerekben mindez általában ellenőrzötten történik, de amint láttuk, az infláció gyorsan el tud szabadulni.

A fogyasztói árindex statisztikák szerint 2018 és 2019 között az árak 1,7%-kal emelkedtek Németországban és 1,9%-kal az USÁ-ban. Sok országban ennél jóval több volt az emelkedés: 3,75% Brazíliában, 5% Indiában, 11% Nigériában, 20% Törökor-

ságban, és igen jelentős 47% Argentínában. Ahol az áremelkedés üteme évi 10% felett van, az emberek már komolyan megérzik jövedelmük és megtakarításuk elértéktelenedését. (Fordító megjegyzése: 2022-ben ennél jóval magasabb inflációs számokat láthattunk világszerte.)

Egy kiugró példa Venezuela. A nyakló nélküli pénznyomtatás, rendszerszintű korrupció és általánosan rossz gazdaságpolitika eredményeként az árak 2.300.000%-kal nőttek 2018-ban – ami olyan szintű hiperinfláció, amelyben lehetetlen megtakarítani. A megkapott pénz szinte órák alatt elpárolog. Emiatt a venezuelaiak kénytelenek egyik napról a másikra élni, és gyakorlatilag azonnal létfontosságú árukra váltani a jövedelmüket. A venezuelaiak egy autoriter rendszerben élnek, amelyben nincsenek szabad és tiszta választások, ami által a kormány elszámoltatható lenne. Az elmúlt néhány évben több mint 4 millióan, ami az ország lakosságának tíz százaléka, menekült el, főként a szomszédos Brazíliába és Kolumbiába, komoly menekültválságot okozva.

A gazdaság kizsigerelése mellett a venezuelai rezsim szigorúan ellenőrzi a tőke mozgását. Nagyon nehéz pénzt küldeni külföldre vagy külföldről. Ez leginkább olyan közvetítőkön keresztül lehetséges, akiknek két országban van számlájuk: például valaki kolumbiai pesot ad egy közvetítőnek, aki venezuelai bolivárt utal a címzettnek. De ez a kerülő út is egyre kevésbé járható, mert a bankok a kormány nyomására megcímkézik azokat, akik a venezuelai számlájukat külföldről használják. Emlékezzünk vissza az 1. fejezetre: a kormány nem akarja, hogy a lakosság hozzáférjen a bolivárnál jobb, erősebb pénzhez.

Egy másik megoldás, hogy ha egy barát vagy családtag az USÁ-ban él, és a Western Unionnal küld pénzt egy kolumbiai határközeli fiókba. A fogadónak sokat kockáztatva ki kell szöknie Venezuelából, elutaznia a kolumbiai városba, felvennie az USA dollárt, és a készpénzt például a ruhájába rejtve vissza kell jutnia az országba. Könnyen belátható, hogy ez időigényes és veszélyes vállalkozás, annál is inkább, mert a közúti határátkelőkön és reptereken a korrupt hivatalnokok vadásznak az elkobozható dollárokra.

A megoldás bitcoint használni a határon túli pénzküldésre. Egy venezuelai üzenhet a külföldön élő barátnak vagy családtagnak, hogy bitcoinra van szüksége, és azt rövid időn belül meg is kaphatja, egy csekély díj ellenében. Egy ilyen tranzakciót lehetetlen cenzúrázni és nehéz nyomonkövetni. Egy stabil pénzhez szokott embernek a bitcoin árfolyama hullámzónak tűnhet, de egy venezuelainak egy hirtelen 20%-os változás sem tűnik soknak a 2.300.000%-os bolivar inflációhoz képest.

Amint megkapták a bitcoint a mobiljukra vagy számítógépükre, át tudják váltani helyi pénzre például a LocalBitcoins.com-on keresztül; ez az eBay jellegű weboldal összekapcsolja a vevőket és az eladókat. A frissen megkapott bitcoint meghirdetik az oldalon, és hamarosan ajánlatokat kapnak rá. Negyed óra alatt el lehet adni a bitcoint, bankba utalt bolivárért cserébe. Több millió dollárnak megfelelő pénz cserél így gazdát nap mint nap Venezuelában. 2019 közepén a bitcoin már egy létező párhuzamos gazdaság olyan problémás gazdaságokban, mint Venezuela.

Egyetemes hozzáférés a pénzhez

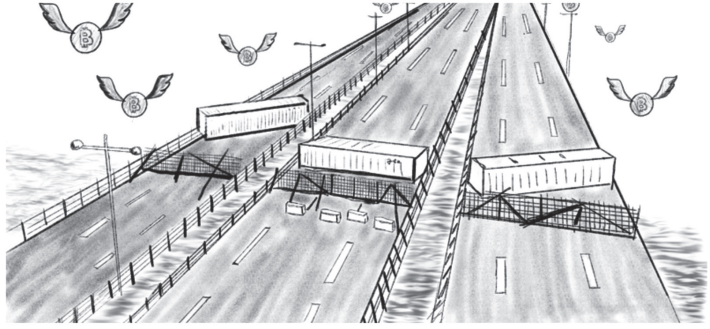
Egy stabil demokráciában élő tájékozott embernek nem gond bankszámlát nyitni. De ez egyáltalán nem ilyen természetes több milliárd embernek a Földön. Íme néhány elgondolkodtató példa. Afganisztánban és Szaúd-Arábiában a nőknek nem

lehet bankszámlájuk, a pénzügyeket a férfi családtagok intézik. A nők számára nem létezik pénzügyi szabadság.

Számukra a bitcoin felszabadító lehet. 2014-ben egy afgán tech vállalkozónő, Roya Mahboob azzal szembesült, hogy nem tud a női alkalmazottainak fizetést utalni. Ha készpénzben fizette volna őket, azt elvette volna a családjuk. A férfi rokonok nem engedték őket bankszámlát nyitni. Alternatív megoldások, mint pl. PayPal nem voltak elérhetőek az országban. Egy barátja említette a bitcoint, és ő elkezdte bitcoinban fizetni az alkalmazottait. Ez pénzügyi önállóságot adott nekik.

Ezen fiatal nők egyike úgy döntött, hogy elhagyja Afganisztánt, egy komoly fenyegetés miatt. A megkeresett bitcoinját magával vitte az okostelefonján. Iránon és Törökországon át utazva eljutott Németországig. Ott a bitcoint – aminek időközben feljebb is ment az értéke – euróra váltotta, és új életet kezdett. A bitcoin hasznos lehet az elnyomottaknak és bankon kívülieknek, amikor nincs más opciójuk.

A bitcoin, az infrastruktúra és a helyi közvetlen piacterek várható növekedésével, egyre inkább hatással lesz a nemzetközi segélyezésre és humanitárius támogatásra. Egy, a venezuelai



határon 2019 februárjában készült fotó élénken mutatja, hogy milyen gondokkal küzd a segélyezés: a Maduro rezsim traktorokkal és utánfutókkal zárt el egy határátkelő hidat, hogy megakadályozza a segélyszállítmányok bejutását. Ami nem látható a képen, az a sok, több millió dollárnyi bitcoin, ami ellenőrizhetetlenül áramlik be és ki az országból.

A jelenlegi segélyezési rendszernek nagyon gyenge pontjai vannak. Legyen az egy állam segélye egy másik államnak, vagy egy segélyező szervezet ajándéka egy másik NGO-nak, vagy egy személy adománya egy egészségügyi vészhelyzetben lévő családnak, a pénz csak közvetítőkön keresztül tud célba jutni.

A legegyszerűbb esetekben is legalább három közvetítő van: a küldő bankja, egy központi bank és a fogadó bankja. Sokszor több közvetítő, akár hét is bekerülhet a képbe. Ezek mindegyike egy lassító tényező a folyamatban, de akár el is akaszthatja a fizetést vagy ellophatja a pénzt. Bam Ki-moon, korábbi ENSZ főtitkár egy 2012-es beszédében azt becsülte, hogy a korrupció „akadályozta meg az összes fejlesztési támogatás 30%-ának a célba jutását".

A GivenDirectly és a Világbank eredményei alapján a közvetlen készpénz átadás a leghatékonyabb módja a segélyezésnek. A bitcoin lehetővé teszi, hogy bárkinek, bárhová, gyorsan, engedélyek nélkül utaljanak. A fogadónak nincs szüksége bankszámlára vagy hivatalos iratokra, csakis internet kapcsolatra.

A Pew szervezet jelentése szerint a fejlődő gazdaságokban élők több mint 45%-a rendelkezik okostelefonnal, és ez a szám évről évre növekszik. Hogy jobban lássuk a bitcoin potenciálját, vessük össze ezt olyan statisztikákkal, mint például hogy a Fülöp-szigeteken a felnőtt lakosság csak 20%-ának van bankszámlája.

Hogy praktikus fizetési csatornaként működhessen, a fogadóknak a bitcoint könnyen kell tudniuk helyi pénzre váltani. A bitcoin csak akkor hasznos segítség, ha árukat és szolgáltatásokat lehet rajta venni. Matt Ahlborg részletes helyi bitcoin piac elemzése azt mutatja, hogy a bitcoin helyi váltása egyre könnyebb a feltörekvő gazdaságokban, Kelet-Ázsiától Nyugat-Afrikáig. Mi több, a bitcoin akkor is működik, amikor a hagyományos bankrendszer nem. A bitcoin globális infrastruktúrája egyre gyakrabban lesz a hatékony segítségnyújtás médiuma.

Kiépülőben vannak olyan cella hálózatok, műholdas rendszerek és rádió alapú technológiák, melyek lehetővé teszik a bitcoin működését még akkor is, ha nincs hagyományos internet. Ezek a mérnöki újítások is hozzájárulnak ahhoz, hogy a kormányok ne tudják megtiltani az embereknek, hogy hozzáférjenek a bitcoinhoz, a pénzhez, amit ők nem tudnak elinflálni vagy eltulajdonítani.

A készpénz nélküli társadalom

A készpénz nélküli társadalmat egy kívánatos, kényelmes dologként tálalják. De emberjogi szempontból erősen aggályos, hiszen minden eddiginél erősebb ellenőrzést ad a kormányok és a bankok kezébe.

A készpénz az egyik fontos eszköze a személyes magánélet védelmének. Amikor papírpénzzel történik a fizetés, csak a vevő és az eladó tud a tranzakcióról, és a vevő tevékenységét nem könnyen tudja monitorozni az állam. Névtelenül lehet fizetni készpénzzel akkor is, ha valaki egy adománygyűjtőbe dob pénzt.

Sajnos a készpénz eltűnőben van a világon. A venezuelai vagy szomáliai hiperinflációban a papírpénzek annyira elértéktelenednek, hogy kilós kötegekben kell mérni őket. A másik oldalon egy fejlett urbánus környezetben, mint Stockholm vagy Sanghaj, az emberek szinte kizárólag digitális fizetést használnak. Egy becslés szerint világszerte minden pénztranzakció mindössze 8%-a történik papírpénzzel és érmékkel. 2030-ra azok száma, akik kényelmesen meg tudnak élni főként készpénzt használva, szinte nulla lesz.

Ez egy ijesztő jövőkép minden tiltakozó számára, akik mint azt az 1. fejezetben említettük, a készpénz anonimitása mögé rejtőznek amikor pl. Hongkongban metrójegyet vagy SIM kártyát vásárolnak. Készpénz vagy valamilyen digitális megfelelő nélkül szinte lehetetlen lesz bármilyen politikai tiltakozást szervezni a személyes biztonság feladása nélkül.

Észtországban a kormány ingyenessé teszi a közösségi közlekedést. Ez nagyszerűen hangzik, de van benne egy csavar: az utazók csak a személyi igazolványuk használatával érik el az ingyenes utazást. Ily módon lehetővé válik, hogy a kormány nyilvántartsa az utazókat. Igaz, hogy egy átlagos észtnek nem kell sokmindentől tartania, de a környező autoriter országok, mint Oroszország vagy Fehéroroszország, polgárainak már komolyabb aggódnivalójuk van.

Mindeközben a Kínai Kommunista Párt olyan milliárdnyi felhasználós rendszereket tart ellenőrzése alatt, mint az Alipay vagy a WeChat. A hatóságok nem csak monitorozzák és ellenőrzik az emberek pénzét, de szabályozzák a polgárok tevékenységét és véleményét a ‘társadalmi pontrendszeren’ keresztül. Egy társadalmi pontrendszerben, mint amilyet Kína-szerte bevezettek, a polgárok ‘osztályzata’ nemcsak pénzügyi helyzetüktől függ, hanem politikai véleményüktől, azonosságuktól és társadalmi kapcsolataiktól is. A kormányzat a lojális viselkedést jutalmazza és a problémásat bünteti, pl. meggátolva a külföld-

re utazást, gyors internet hozzáférést, hogy jó iskolába küldjék a gyerekeiket, vagy jó feltételekkel vegyenek fel hitelt. Ezek a pontrendszerek még kiépülőben vannak, de abba az irányba haladunk, hogy minden eddiginél nagyobb befolyást biztosítsanak a kínai kormánynak, a történelem egyik legnagyobb társadalmi kísérleti projektjében.

Ugyan jóval enyhébb formában, de hasonló rendszerek jelennek meg a nyugati demokráciákban is, amelyek egyik alapja a kártyatársaságok által profitért eladott tranzakció információ.

Bitcoin versus a Nagy Testvér

Ne azt nézd, hogy mit mond valaki, hanem azt, hogy mit vásárol! Egy emberről rengeteget elárulnak tranzakciói: hogy ki ő, mit csinál, hová jár, mit szeret és mit nem. Minél kiterjedtebb a költések nyomonkövetése, annál valószínűbb egy orwelli jövő.

Néhány demokratikus társadalomban vita alakult ki arról, hogy nagy tech cégek, mint a Facebook, létrehozhatnak-e saját pénzt. A Facebook elképzelése az, hogy több száz millió felhasználónak tenné elérhetővé a Libra pénzt a közösségi média applikációkon keresztül (WhatsApp, Instagram, Messenger). Bár egy Libra kaliberű projekt sok olyan ember számára nyitna meg pénzügyi hozzáférést, akiknek nincs lehetősége bankot használni, sokan attól tartanak, hogy a Facebook eltárolná a felhasználók pénzügyi műveleteit, befolyásolná a választást, kizárhatna bizonyos személyeket vagy korlátozná fizetési műveleteiket, bizonyos véleményeik miatt.

A Nagy Testvért csak akkor lehet leállítani, ha mindenki csökkenti az amúgy egyre növekvő adat hegyeit. Minél kevesebb személyhez kötött információ kerül letárolásra és megosztásra cégek és kormányszervek között, annál nehezebb megfigyelni, manipulálni és kontrollálni az embereket.

Egy készpénzmentes társadalom az egy lehallgató társadalom. Akár egy kormányzat által ellenőrzött WeChat modellen keresztül, vagy nagy privát cég által ellenőrzött Libra modellen keresztül, nyomon tudják követni a pénzügyi tevékenységeket, profitszerzési céllal, vagy akár polgárok ellenőrzése vagy büntetése céljából.

Biztosan ez a jövő? Mi lenne, ha a készpénz digitális formában is létezne? Igaz, hogy a bitcoin tranzakciók csak pszeudoanonimak (nem teljesen névtelenek), a fejlesztők több területen dolgoznak, hogy növeljék a bitcoin hálózat és felhasználók névtelenségét. A közeljövőben, amikor valaki online vásárol valamit, busz- vagy metrójegyet vásárol, feliratkozik egy politikai témájú magazinra vagy podcastra, a fizetésnél nem kell felfednie személyazonosságát.

Privátabb bitcoin a Lightning által

A fogyasztók egyre inkább elveszítik pénzügyi magánéletüket. Erre lehet egy megoldás a Lightning hálózat, ami egy bitcoinra épülő fizetési rendszer.

A jelenlegi fizetési rendszer tele van csapdákkal, mivel minden pénzügyi közvetítő egy lehetséges biztonsági rés. A bitcoin abban más, hogy kiküszöböli a közvetítőket, így elvileg ez a fajta probléma nem áll fenn. Viszont a bitcoin esetében a tranzakciók adatai a nyitott blokkláncra kerülnek, ahol bárki láthatja őket (személyazonosságok nélkül). Többen kutatják annak a módját, hogy hogyan lehet úgy bitcoinnal fizetni, hogy közben el lehessen rejteni a tranzakciók egyes adatait. Ez lehetséges a Lightning hálózattal.

A Lightning hálózat nem rögzíti a tranzakciókat a bitcoin blokkláncon. A Lightning hálózat fő célja a gyors, olcsó és nagyszámú bitcoin tranzakciók lehetővé tétele. Hogy ez privátabb tranzakciókat is jelent, az ezen célnak egy hasznos mellékhatása.

Ez a technológiai áttörés, ugyanúgy mint a bitcoin, nyílt forráskódú, nem engedélyez kötött, és bárki számára elérhető élőhelytől, kortól, keresettől, nemtől és állampolgárságtól függetlenül. A bitcoin és a Lightning hasznos lehet elkerülni egy olyan antiutópia jövőt, melyben a privát szféra védelme pénzbe kerül és csak a gazdagok kiváltsága.

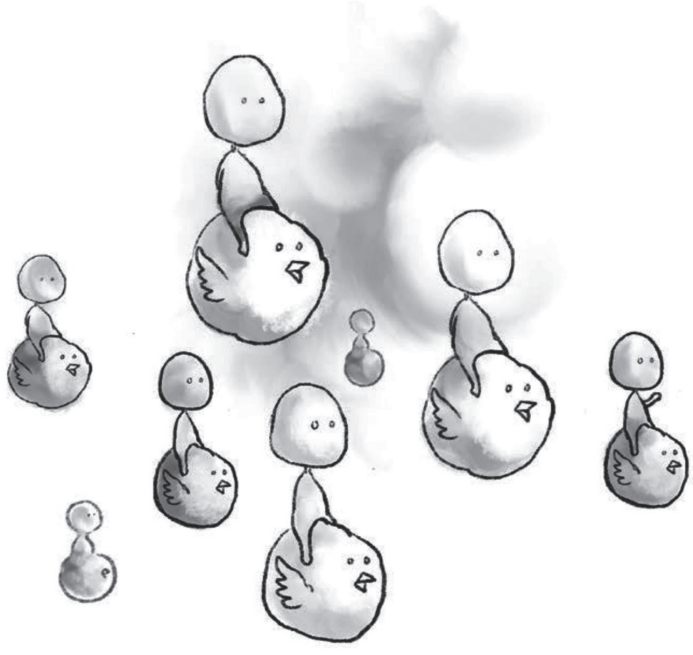
Egy készpénz nélküli világban is lehetséges lesz a közeljövőben egy mobilos Lightning applikációt használva névtelenül venni metrójegyet egy tüntetésre tartva, vagy politikai könyveket vásárolni online. A metrójegy automata vagy az Amazon nem fog tudni semmit a vásárlóról, így kizárt lesz, hogy ezek az adatok kiszivárogjanak vagy átadásra kerüljenek a kormánynak.

Mindezzel együtt a Lightning nem egy csodaszer a magánéletre. A fizetési információk védelme fontos pillére a magánélet védelmének, de csak egy a sok közül, hiszen egyéb rések mint lehallgató appok a telefonon, geolokáció követés és megfigyelő kamerák szintén problémásak.

Nassim Taleb, a *Fekete Hattyú* szerzője írta hogy a bitcoin „egy biztosítás egy orwelli jövő ellen". Amíg a növekvő megfigyelés és készpénz háttérbe szorítása trendek folytatódnak a világban, a jövőnk nyomasztóan néz ki.

A technológia nem mindig növeli a szabadság fokát a világban. Pont ellenkezőleg, mesterséges intelligenciát és adatbányászatot használnak a személyi szabadság korlátozására, főleg olyan helyeken, mint Kína. Yuval Noah Harari történész, a *Sa-*

piens szerzője figyelmeztetett arra, hogy a modern információ technológia inkább a zsarnokságnak kedvez, de szolgálhatja a szabadságot is, ha kifejezetten erre a célra lett kifejlesztve és használatba ültetve. A bitcoin, új kiegészítőkkel mint a Lightning hálózat, egy fontos eszköz lehet az emberi szabadságért vívott küzdelemben.



5. FEJEZET

Két mese a jövőről

A 2039-es évben járunk.

Az elmúlt 20 évben egyre több széleskörű háború tört ki. Számos ország igyekszik kibillenteni az USA dollárt és a kínai jüant vezető pozícióikból. A gazdasági viharok időnként erőszakos konfliktusokba torkollnak. A gazdag országok politikailag gyengülnek, kezelhetetlen gazdasági hanyatlással küzdenek, míg a szegény országok a teljes összeomlás szélére sodródnak. Az egymást követő gazdasági válságok sora az állami testületek kezébe adja a vagyont és a hatalmat.

A vezető tech-cégek, mint az Alibaba, a Tencent, a Facebook, a Google és az Amazon irányítják a globális piacokat, és a gyakori kormányzati nyomásgyakorlások, trösztellenes perek és megállapodások eredményeként átadják a felhasználók adatait a kormányzatnak a piacvédelemért cserébe.

A vállalatok az egész világon megosztják a kormányzatokkal felhasználóikra vonatkozó óriási adattömegüket (mit vásárolnak, mit hallgatnak, mit posztolnak ki, és hol vannak az emberek). A vállalatok az állam szatelitjeivé válnak. A magánélet megszűnik.

Ez lehetővé teszi, hogy a kormányok korábban nem tapasztalt mértékű kontrollt gyakoroljanak polgáraik felett. To-

vább nő a szakadék a gazdagok és a szegények között, ahogy a Cantillon-hatás felerősödik, és a hatalmi kapcsolatokkal rendelkezők aránytalanul gazdagodnak. A digitális megfigyelés bevett gyakorlattá válik, közben a tekintélyelvű kormányzással szembeni ellenállás megszűnik. Az erőforrások feletti kormányzati és vállalati kontroll miatt csökken a szólásszabadság, mivel a protest-tartalmakat készítők nem kapnak fizetett állásokat, sem más bevételi lehetőségeket.

A máshogy gondolkodás egyben tiltakozást jelent. A rendőrállamok világszerte felhasználják a dolgok internetével, az implantátumokkal, a telefon-nyomkövetéssel, a tranzakciótörténettel és internetes keresésekkel kapcsolatos adatokat a disszidensek megtalálására és szankcionálására. Az ellenállás gyakorlatilag lehetetlen, mivel a készpénz eltűnik, és minden vásárlás (a metrójegytől az újságig és maszkokig) digitális és követhető, ezzel felfedve a személy identitását. Az államok és a multinacionális vállalatok erősebbek, mint valaha.

2039-et írunk.

A globális gazdaság továbbra is virágzik. Világszerte egyre többen takarékoskodnak, vagyonokat halmoznak fel, ingatlanokat vásárolnak, és új vállalkozásokat indítanak el. A korábban harmadik világnak nevezett országok vállalkozói állnak a globális gazdasági innovációk élére. Az igazságszolgáltatás gördülékenyen működik. A kormányok versengenek, hogy a szabadon költöző polgárok náluk éljenek, dolgozzanak és fizessenek adót. A jövedelemadók mértéke csökken, miközben az infrastruktúra, a szolgáltatások és az oktatás színvonala, a globális versenynek köszönhetően fejlődik.

Rengeteg kisvállalkozás nyújt új, elképzelhetetlen mértékben innovatív termékeket és szolgáltatásokat. Számos korábbi vezető multinacionális vállalat elvesztette pozícióját a világ minden szegletéből érkező sok kis gazdasági szereplő térnyerése miatt. Bárki bármiért fizethet privát és engedélyeztetést nem igénylő fizetési módokon.

Számos autoriter rezsim megbukik vagy meggyengül, mert polgáraik képessé válnak a szigorú tőkekontroll megkerülésére, ezzel vagyonuk megtartására, ahelyett, hogy az állami elit magához ragadná azokat.

A kormányzatok rákényszerülnek, hogy a kontrollálás helyett versenyezzenek; az emberek személyes szabadsága nagyobb lett, mint valaha.

Hogy néz ki a bitcoin-alapú világ?

Mindig kockázatos dolog a jövő megjóslásába bocsátkozni. A fentiek a jelen állapotokból kiinduló két lehetséges jövőt írnak le. Valószínűleg a két szélsőséges lehetőség közül egyik sem ebben a formában fog megvalósulni, de az emberek hatással vannak arra, hogy a jövő társadalma merre indul.

A pénzügyi rendszer kérdése kulcsfontosságú. A bitcoin rendelkezik azzal a képességgel, hogy szétválassza az államot és a pénzt. Érdemes feltenni a kérdést, hogy a bitcoin globális bevezetése miképpen változtathatja meg a társadalmat?

A határok nélküli gazdaság eljövetele

A gazdaság működését a 20. század óta javarészt a nemzetállamok irányították. A digitális fizetésre történő átállás korábban nem látott mértékben tette lehetővé a kormányok számára

a gazdaság ellenőrzését, hiszen könnyen tudnak forrásokat teremteni a pénzállomány növelésén keresztül.

A digitális korszak fejlődésével azonban a gazdaság elkezdett túlnőni az állam keretein. A 21. század kezdetén a fogyasztók már olyan termékeket vásároltak, amelyek előállításában a fél világ részt vett. A cégek szabadúszó szoftverfejlesztőket, virtuális asszisztenseket, sőt radiológus szakorvosokat alkalmaztak a Fülöp-szigetektől Nigériáig. A kereskedelmi partnereket több ezer mérföld is elválaszthatta egymástól. Minden kommunikáció digitális, azonnali és zökkenőmentes lett. A határokon átnyúló fizetés azonban még mindig lassú és drága maradt. Az online vásárlás még mindig a hagyományos csatornákon zajlott USA dollár alapon, és sok időt emésztett fel, valamint gazdasági intézmények bevonását tette szükségessé. A pénzügyi rendszer még nem alkalmazkodott az egyre inkább összekapcsolódó világhoz.

A bitcoin felemelkedése az a szikra, ami lehetővé teszi a pénzügyi evolúció következő ugrását.

A digitális-alapú termékek, mint a közösségi-média tartalmak vagy videójátékok egyre nagyobb szeletet hasítanak ki a világgazdaságból. A bitcoint egyre gyakrabban fogják használni a határokon átívelő fizetési tranzakciókban a fiat eszközök nehézkessége miatt. A bitcoin mikrotranzakciók gyors elszámolása és a növekvő felhasználó-bázis arra sarkallja majd a kereskedőket, hogy bitcoinban is megadják az árakat.

Még korlátozottak a bitcoin-alapú üzletmenetek – a 90'-es évekbeli AOL közösségekhez hasonlóan – de növekedésükkel tovább erodálják az államok gazdasági kontroll-képességét. Minél nagyobb magánvagyon halmozódik fel a határok-nélküli hálózatokban és valutákban, annál könnyebb lesz ezt a vagyont felszabadítani a nemzetállamok fizikai korlátai alól.

A kormányok szembesülni fognak a háborúk valódi költségeivel

A bitcoin elterjedésével sokkal korlátozottabbá válik az államok lehetősége, hogy pénznyomtatással finanszírozzák a háborúkat. Ezzel a háborúk költségesebbé válnak, mint az elmúlt száz évben bármikor. Ha mégis kitör egy háború, várhatóan korlátozottabb és rövidebb lesz.

Az olyan hosszabb konfliktusok, mint az orosz beavatkozás Szíriában és Ukrajnában, vagy Irak és Afganisztán amerikai megszállása, a nehezebb finanszírozhatóság miatt egyre ritkábbakká válnak. A nemzetállamok közötti háborúk a jelenleginél is „végsőbb megoldássá" válnak, hiszen az államok fokozottan érdekeltté válnak az olcsóbb konfliktus-megoldások alkalmazásában.

Túl drágává válik a tekintélyuralom

Az autoriter államoknak nehézséget okoz a globális környezetben zajló verseny, mivel kevésbé képesek kontrollálni a határaikon kívül történő folyamatokat. Azok a produktív személyek, akik pénzügyeiket tekintve bárhol a világon teljes függetlenséget élveznek, a saját országuk feltételeinek kedvezőtlenné válásával, *vagyonukkal együtt* könnyen átköltözhetnek egy más jogrendszerű országba. Sikeres polgáraik visszatartása érdekében szigorú határőrizetet kell fenntartaniuk, vagy lehetőséget adni számukra, hogy beleszólhassanak a kormányzat döntéshozatalába.

A diktatúrák nem fogják könnyen feladni, de döntésre fognak kényszerülni: engedik megszökni a tőkét vagy csökkentik a kontroll mértékét. Az információs hálózatoknak köszönhető, hogy liberális irodalmi alkotások és filmek már könnyedén el-

jutnak az olyan zsarnoki rendszerek polgáraihoz is, mint Eritrea és Észak-Korea. Ezt a jelenséget felgyorsítja egy olyan pénz megjelenése, ami épp olyan könnyen és biztonságosan továbbítható, mint az információ.

A befektetések árazása reálisabbá válik

A bitcoin státusztól, nemzetiségtől, lakóhelytől függetlenül mindenki számára megfelelő értéktároló eszköz. A legtöbben – a fiat pénzeszközök inflációjára reagálva – ingatlanban, részvényben, nemesfémben tárolják a pénzüket, ezek az eszközök azonban centralizáltak, nehezebben hozzáférhetőek, mint a bitcoin. Egy olyan világban, ahol a pénz bitcoinban tartása a norma, egyre valószínűtlenebbé válik spekulatív buborékok kialakulása a befektetések területén.

Egyre kevesebb ingatlanbuborék fog kialakulni az infláció következtében, mivel kevesebb külföldi fog apartmanokat vásárolni kizárólag befektetési célból. A bitcoin jobb alternatívává válásával a külföldi ingatlanbefektetések vonzereje csökken, az árak nem fognak felrobbanni, és egyre többen engedhetik meg maguknak, hogy saját lakást vásároljanak a saját településükön.

Megérkezik a decentralizált finanszírozás

Az amerikai, európai és kínai gazdasági dominancia eltűnik, mivel az országok bitcoinban, valódi globális tartalékvalutában kereskednek, a regionális USD, EUR vagy CNY helyett. A munkaerő szabadon vándorolhat világszerte, nagyobb lesz a munkaerőkereslet, így a dolgozók által megtermelt érték nagyobb része jut vissza hozzájuk.

Az amerikai, európai és kínai bankok elveszítik túlzott befolyásukat, mivel minden személy a „saját bankárává válik", így idővel valódi megtakarításokkal fog rendelkezni. A vagyon azokban az országokban halmozódik fel, melyek exportálják a munkát, ezzel fejlődnek a helyi vállalkozások, az infrastruktúra és a szolgáltatások.

A nagy bankok hatalma csökken

Azok a bankok, melyek kormányzati kapcsolataiknak és a kormány pénzügyekre gyakorolt hatásának köszönhetik gazdagságukat, tönkremennek vagy összezsugorodnak. Már nem az lesz a norma, hogy „túl nagy ahhoz, hogy megbukjon", a bankok és nagyvállalatok már nem számíthatnak kormányzati mentőcsomagokra, ha elrontanak valami, mint például a 2008-as pénzügyi válság idején.

Ezek híján a bankoknak és a multinacionális cégeknek sokkal inkább az ügyfeleknek nyújtott szolgáltatásokra kell koncentrálniuk, mint arra, hogy a kormányok kegyeit keressék. A kisebb bankok és vállalatok – a bitcoin globális természetének köszönhetően – képessé válnak az ügyfeleik határokon átnyúló kiszolgálására, és a túl nagyra nőtt óriások a múlt ködébe vesznek.

A Nagy Testvér és a megfigyelő kapitalizmus hanyatlása

Manapság a digitális fizetési információkat a cégek profitnövelésre, a kormányok megfigyelésre használják. Az internet vált a nyílt piac fő területévé, és a titoktartási normák csak lassan követik ezt a fejlődést, korlátozottan védve az online elérhető egyre bizalmasabb és fontosabb információkat. Ennek eredménye-

képpen a személyes adatokat folyamatosan újracsomagolják, elemzik a tulajdonos tudta vagy explicit hozzájárulása nélkül.

A bitcoin Lightning fizetési lehetőségének használatával a legtöbb mindennapi vásárlás elválasztható a vásárló személyétől.

Ha valaki online vásárol, egy politikai magazinra fizet elő, egy civil szervezetnek adakozik, vagy egy gyógykezelést fizet ki, a vásárlón kívül senki nem fogja ismerni a tranzakció minden részletét. Nincs fizetés szolgáltató, amely köztes helyzetének köszönhetően információt szivárogtathatna, mivel a tranzakció közvetlenül zajlik a partnerek között, és a kereskedő csak a fizetést fogja látni. Ebben az azonosító információk nélküli közegben a megfigyelést végző szoftvereknek sokkal nehezebb lesz a vásárlók viselkedését követni, vagy megjósolni viselkedésüket.

Az önrendelkezés kezdete

A bitcoin komoly potenciális hatást gyakorolhat a demokráciára és az internetre egyaránt: nemcsak a politikai hatalom kizárólagosságát, hanem a tudás vállalati kontrollját is megingathatja. A demokrácia lehetővé teszi, hogy a polgárok közösen ellenőrizzék a kormányzati hatalmat és gyengítsék diktátorokat. Az internet segítségével a polgárok hangja felerősödik és szabadabb hozzáférésük lesz bármilyen tudáshoz.

A bitcoin hasonlóképpen rengetheti meg az államok és nagyvállalatok pénzügyi monopóliumát. Száz év múltán, 2019-re visszanézve, láthatóvá válik, hogy a kevesek hatalmában álló gazdaság éppúgy meghaladottá vált, ahogy korábban a királyságok feudális rendszere, vagy később az állami propaganda korszaka. Ez az evolúció, a bitcoin első számú világvalutává válása három lépésben történik majd.

Első fázis: Értékmegőrző

A bitcoin bevezetésének első fázisa az értékmegőrző funkció használata. Ez arra szolgál, hogy a befektetők világszerte megvédjék magukat a kormányaik gerjesztette inflációtól. Ez jelenleg nemcsak Venezuela és Zimbabwe hiperinflációs gazdaságaiban figyelhető meg, de az USA-ban és Európában is, hiszen a bitcoin többéves távlatban felülmúlta a fiat valuták teljesítményét. Az értéktároló fázisban a nyugdíjalapok és vezető pénzügyi intézmények elkezdenek bitcoint felvenni a portfóliójukra, ezt később a kormányok is követik majd.

A bitcoin bevezetése ebben a fázisban – az előnyök felismerésével párhuzamosan – fokozatosan és organikusan fog történni.

Második fázis: Fizetőeszköz

Amikor már a kereskedők is felismerik, hogy a nem-bitcoin pénzeszközök kevésbé értékállóak, bitcoinban fogják kérni termékeik ellenértékét. Hasonlóan a venezuelai feketepiaci kereskedőkhöz, akik USA dollárt kérnek a bolivar helyett. Ahogy egyre több kereskedő, vállalkozó és munkavállaló fogja a bitcoint preferálni, robbanásszerűen megnő rá az igény, ahogy az USA dollárnál is megfigyelhető volt a Bretton Woods arany konvertibilitási rendszer bevezetésekor.

Eleinte nem a fejlett gazdaságoknál történik meg az átállás, hanem az elszabadult inflációtól és követhetetlen korrupciótól szenvedő gyenge gazdaságoknál. Ezeket a társadalmakat jó eséllyel elnyomó rezsimek uralják, akik korlátozzák az egyéb értékálló eszközök (USD, arany) hozzáférhetőségét. Ezen országok polgárai azért vásárolnak bitcoint, hogy megakadályozzák az államot vagyonuk elkobzásában, vagy ha elmenekülnek országukból, a vagyonukat is kimenthessék.

Ebben a fázisban a jól megtervezett szoftverek, a gyorsabb elszámolási technológiák, a fejlett infrastruktúra kialakítása és a titkosítási innovációk kerülnek előtérbe. A bitcoin felhasználók azonnali és titkosított tranzakciókat tudnak elvégezni, melyeket sokkal nehezebb megfigyelni.

Harmadik fázis: Elszámolási egység

Ahogy egyre többen tartanak pénzt és kapnak fizetést bitcoinban nemzeti valutájuk helyett, a termékek és szolgáltatások árát is bitcoinban kezdik megadni a helyi valuta vagy USD helyett. Ekkor már jövedelmező arbitrázs lehetőségek is megnyílnak; például hitelfelvétel elértéktelenedő valutákban, melyeket bitcoinra váltanak, ezzel profit érhető el.

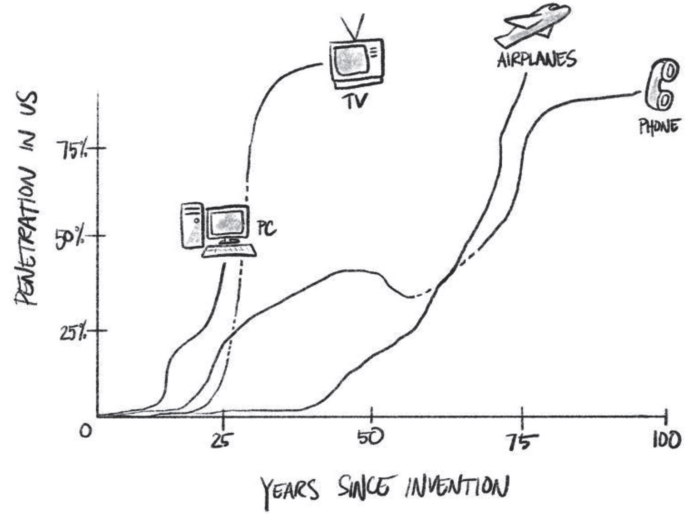
Ez lesz a hiperbitcoinizáció kezdete, amikor az USD és a CNY elveszíti kiemelt pozícióját, és a bitcoin válik a világ elszámoló-valutájává. Ennek következménye a valuták többségének hiperinflációja lesz, mivel az arbitrázs miatt nagyon megdrágulnak a hitelek. Ahogy a bitcoin válik az elsődleges értékmegőrző valutává, a pozitív visszacsatolási hurok jelentősen elértékteleníti a többi valuta jelentős részét.

Még mindig nincs késő

Az emberek többsége a világot alapvetően megváltoztató technológiák nagy részét eleinte elutasítja. Például nézzük az elektromosságot, amit rendkívül veszélyesnek tartottak; a telefont, amiért senki nem akart pénzt adni; az autót, ami nem is tudott rossz utakon boldogulni; a repülőgépet, ami szimplán nagyon veszélyesnek látszott; a mikrohullámú sütőt, amiről azt hitték, hogy minden tápanyagot tönkretesz az ételben; a rákkeltőnek hitt mobiltelefont; vagy az internetet, ami bukásra volt

ítélve. Emlékezzünk vissza Paul Krugman 1998-as szavaira a New York Times-ból: „2005-re ki fog derülni, hogy az internet gazdaságra gyakorolt hatása nem nagyobb, mint a fax-gépé."

Minden újító technológia – a hűtőgéptől a hitelkártyáig – bevezetési folyamata egy adott görbét követ, és kezdetben sokan szkeptikusan tekintenek az újításra. Egy idő után azonban a bevezetési görbe exponenciálisan felível, 'S' alakot vesz fel, és az új technológia elterjed. Nehéz annál egyenlőbb vagy demokratikusabb dolgot elképzelni, minthogy bárki – lakóhelytől, nemtől, beszélt nyelvtől, iskolai végzettségtől, életkortól vagy vagyoni helyzettől függetlenül – korlátozás nélkül használhatja a bitcoint, azt az exponenciálisan terjedő technológiát, ami még mindig a bevezetési 'S' görbe alján tart.



A bitcoin alkalmazása jelenleg messze elmarad attól, amit használhatósága, kapacitása, közismertsége és kereskedelmi értéke indokol. Kevés cég épít a bitcoinra; kevés diák hall róla; ke-

vés tanár beszél róla; kevés kereskedő fogadja el; kevés filantróp alapítvány támogatja az elterjedését; és kevés társadalmi szereplő használja ki a bitcoin jelentős potenciálját arra, hogy biztosítsa pénzügyi magánszféráját. Nagyobb érdeklődésre, elköteleződésre és kritikai gondolkodásra van szükség ezen a területen.

A világ teljes népességének kevesebb, mint 1%-a birtokolt valaha is bitcoint. Ha elegendő időt és erőforrást biztosítanánk felhasználóbarát pénztárcák, valutaváltó-platformok és oktatóanyagok fejlesztésére, a bitcoin világszerte milliárdok számára jelenthetne valódi előrelépést. A bitcoin mindenki számára nagyobb pénzügyi szabadságot adhat, de leginkább azoknak, akiknek a legnagyobb szüksége van erre.

Nigéria, Törökország, a Fülöp-szigetek, Venezuela, Irán, Kína, Oroszország és Palesztina lakossága nem rendelkezik ugyanazokkal a szabadság- és emberi jogokkal, és nem bízhat olyan mértékig saját országának pénzügyi rendszerében, mint a Nyugat polgárai. Számukra a bitcoin jelenti a menekülési útvonalat.

A csendes hallgatás és a kilépés maradtak az ellenállás utolsó lehetőségei. A változás eléréséhez már nem kell több ezer hasonló gondolkodású embert összehozni egy napra vagy hétre, hogy tüntessenek. Ezek az emberek olyan egyszerűen vonhatják ki vagyonukat az országukból, mintha egy emailt küldenének. Az ellenállás mostantól egyesével, személyenként is megvalósulhat. Cseppenként indul a folyamat, ami fokozatosan csordogálni kezd, majd áradattá változik.

A jövő a te kezedben van

A bitcoin nagyhatású találmány, jelen pénzügyi és gazdasági rendszerünk számos problémájára nyújt új megoldási lehető-

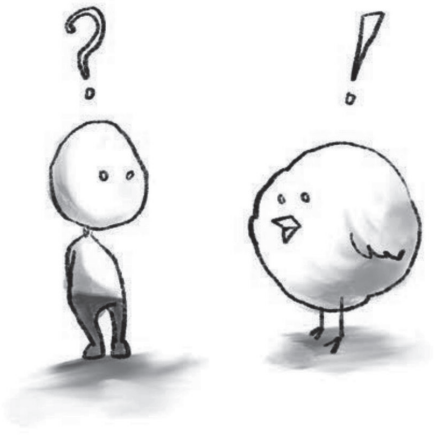
ségeket. Az egyenlőtlenségek, a monopolhelyzetű multinacionális vállalatok és a tekintélyelvűség növekedése mögött a pénz állami kontrollja áll. Ahogy a világ megismeri a bitcoint, és azt a módot, hogy miként segíti elő az egyes személyek függetlenségét; csökkeni fog a hatalomkoncentráció a világban. A tekintélyelvű rezsimek és kormányok rákényszerülnek az emberi méltóság, érték és tehetség tiszteletére. A távoli multinacionális óriáscégek helyett kisebb vállalatok jönnek létre ügyfeleik jobb kiszolgálása érdekében. Bár a vagyoni egyenlőtlenségek teljes megszüntetése nem lehetséges, a bitcoin segít az egyenlő esélyek kialakításában azzal, hogy az embereket képessé teszi arra, hogy megtarthassák azokat az értékeket, amiket ők hoztak létre.

Mi lehetne igazságosabb annál, hogy az eljövendő pénzügyi forradalomban való részvételhez csak egy olcsó mobiltelefon és internet kapcsolat szükséges? Se bank, se állami szabályozás, vagy engedély nem szükséges ahhoz, hogy valaki a jövő részesévé válhasson.

Azzal, hogy a vagyon ellenőrzését visszaveszik a mostani kontrollt gyakorlóktól, mindenki lehetőséget kap rá, hogy a kezébe vegye saját sorsát.

A bitcoin olyan mértékű szabadságot ad az emberek kezébe, ami a 21. század küszöbén még elképzelhetetlen volt.

Add tovább ezt a könyvet és terjeszd a tudást!



Bitcoin Kérdezz-Felelek

Az elmúlt néhány évben az újoncok és a szkeptikusok sok kérdést tettek fel a bitcoinnal kapcsolatban. Ez a fejezet próbálja megválaszolni a fontosabb és gyakoribb kérdeseket, illetve néhány mítosszal, kihívással, hátránnyal és zűrzavarral is foglalkozik a bitcoin vonatkozásában. Ennek a fejezetnek a célja, hogy elegendő alapvető információt nyújtson ahhoz, hogy egy kíváncsi elme jó kiindulópontot kapjon, ugyanakkor ne legyen túlságosan kimerítő sem.

Ki Satoshi Nakamoto?

Satoshi Nakamoto a bitcoin névtelen alkotója.

A bitcoin történetének első két évében Satoshi Nakamoto a közösség aktív tagja volt. Satoshi gyakran posztolta online gondolatait a bitcoin technológiájáról és társadalmi hatásáról, miközben hozzájárult a szoftverfejlesztéshez. 2010 végén Satoshi eltűnt.

Valószínűleg több száz millió dollár értékű bitcoinnal rendelkezik, amelyet a blokkláncon bárki láthat. Ezek az érmék

soha nem mozdultak meg, ami arra utal, hogy az eltűnése végleges. E könyv írása óta Satoshi kilétét nem fedték fel, így ez a 21. század egyik legnagyobb rejtélye.

Ki irányítja a bitcoint?

Egyetlen központi hatóság sem felelős a bitcoinért. Nincs vezérigazgató, nincs igazgatótanács, nincs irányító vállalat. A bitcoin egyik legerősebb tulajdonsága, hogy az alkotója már nem vesz részt benne.

Több ezer validátor van a világon, akik a bitcoin blokkláncát ellenőrzik, és a bitcoin tranzakciók teljes történetét őrzik. Ezeket a validátorokat *teljes csomópontoknak* (full node) nevezzük.

Amint azt a 2. fejezetben tárgyaltuk, a bányászok szerte a világon versenyeznek a blokkok előállításáért. Ezeket a blokkokat a teljes csomópontok érvényesítik. A teljes csomópontok futtatásához használt szoftvert a bitcoin fejlesztői írják. Természetesen a blokkokon belüli tranzakciókat a felhasználók kezdeményezik a tőzsdéikről, tárcáikból vagy fizetési feldolgozóiktól. Mindezek a résztvevők elengedhetetlenek a bitcoin működéséhez, de egyikük sem *irányítja* a bitcoint.

Ha egy fejlesztő úgy dönt, hogy teljes csomópont-szoftvert hoz létre, amely radikálisan különbözik a többitől, kevesen fogják futtatni azt. Ha egy bányász megpróbál becsempészni egy új tranzakcióblokkot, amely nem felel meg az érvényesítési követelményeknek, a teljes csomópontok elutasítják ezt a blokkot. Ha a bányászok puccsot kísérelnek meg, hogy új funkciókat vezessenek be a hálózaton, akkor kudarcot vallanak, mivel nem kényszeríthetik a felhasználókat olyan szoftverek futtatására, amelyeket nem akarnak futtatni.

Így a bitcoin bármilyen módosítása konszenzust igényel. Ebben az értelemben a bitcoin irányítási modellje hasonló a fékek és ellensúlyok demokráciájához. A bányászok olyanok, mint a kormány végrehajtó ága, kezelik a műveleteket és betartatják a szabályokat; a fejlesztők olyanok, mint a törvényhozó ág, új törvényeket dolgoznak ki és fogadnak el; a felhasználók az igazságügyi ág, ügyelve arra, hogy a másik két ág ne tegyen semmi alkotmányelleneset.

Nem túl volatilis a bitcoin?

A bitcoin 2009-es létrehozása óta óriási volatilitást tapasztalt. Hosszabb időtávlatból vizsgálva a bitcoin a kezdetektől fogva jelentősen felértékelődött, kevesebb mint 0,001 dollárról több mint 11 000 dollárig e könyv írásának idején. Amint azt a 3. fejezetben kifejtettük, hosszú távon számos tényező hajtotta fel az árat, és ez valószínűleg továbbra is így lesz.

Satoshi Nakamoto a kezdetekkor meghatározta a bitcoin monetáris politikáját. Egyetlen személy vagy csoport sem dönthet úgy, hogy több bitcoint hoz létre, vagy megváltoztatja a kínálat ütemezését, mivel a teljes csomópontok elutasítják az efféle változtatásokat.

Ennek eredményeként a bitcoin sebezhetőbb lesz a piaci manipulációval szemben, mivel nincs központi banki korrekciós mechanizmusa. A központi bank új pénzt nyomtathat, vagy többet vásárolhat vissza saját pénzéből az árstabilitás fenntartása érdekében. Decentralizált valutaként, korrekciós szabályozók nélkül, továbbra is volatilitást fog tapasztalni, míg az egész világon elfogadják.

A gazdasági valóság a következő: a valutáknak választaniuk kell a rövid távú árstabilitás között a központosítás révén, vagy

a decentralizáció révén a hosszú távú áremelkedés lehetősége között. Satoshi Nakamoto a decentralizációt választotta.

A legfontosabb, hogy a bitcoin volatilitása nem akadályozta meg abban, hogy hatalmas valós értékkel bírjon pénzügyi eszközként azok számára, akik csapdába esnek az instabil pénzügyi rendszerekben. A bitcoin felhasználási területei közé tartozik a szankciók alóli menekülés, a hiperinfláció, a tőkekontroll és a megfigyelés. Jelenleg a napi volatilitás olyan kompromisszum, amelyet a tulajdonosok hajlandóak megfizetni.

Mi adja a bitcoin értékét?

A rövid válasz az, hogy a bitcoin támasza az emberek. Elég befektető vásárolja meg, tehát értéke van. Lásd a 3. fejezetet a részletes magyarázatért, hogy mi adja a bitcoin történelmileg emelkedő értékét. Globális igény van a bitcoinra, mint olyan eszközre, amely szűkös, hasznos, és olyan technológiaként működik, amelyre más pénzügyi eszköz nem képes.

Hogyan lehet megbízni a bitcoinban?

A modern világ tele van komplex rendszerekkel vagy eszközökkel, amelyeket nem teljesen értünk, mégis megbízhatóak. Az egészségügyi ellátást olyan embereknek nyújtják, akik nem orvosok. Az időjárás-előrejelzéseket nem meteorológusok számára teszik közzé. A laptopokat olyan emberek használják, akik nem villamosmérnökök. Az utazóknak nem kell érteniük az aerodinamikát ahhoz, hogy repülőgépen utazhassanak.

Az új pénzügyi rendszerekben való bizalom normáinak szigorúbbaknak kell lenniük, mivel gyakran visszaélnek ezzel a bi-

zalommal, amelyek közül sokat megírtunk ebben a könyvben. De végső soron tárgyi szakértelemre nincs szükség a bitcoin használatához és a bitcoinban való bizalomhoz. Végsősoron a bitcoin küldése és fogadása ugyanolyan egyszerű lesz, mint egy e-mail küldése és fogadása. Jelenleg a bitcoin iránt érdeklődőknek mindenképpen saját kutatást kell végezniük. Számos jó információforrás szerepel a könyv *További források* részében, beleértve a Bitcoin Core forráskódját, más könyveket, weboldalakat és podcastokat.

Mennyire megbízható a bitcoin?

Megfelelő használat esetén a bitcoin sokkal biztonságosabb, robusztusabb és privátabb, mint bármely központi fizetési feldolgozó. A Mastercard és a Visa például időről időre leáll. A bitcoin története 99,98%-ában teljes mértékben működőképes volt a 2009. januári indulás óta. A hitelkártya-társaságok rendszeresen eladják az ügyfelek adatait, és hackertámadás áldozataivá válnak. A bitcoin nem adhat el semmilyen információt a felhasználóiról, mert senki sem irányítja. Ellentétben a fizetési feldolgozókkal és sok bankkal, a bitcoint nem sikerült egyáltalán feltörni, mióta az árfolyama 0,10 dollár fölé emelkedett 2010-ben. Soha senki érméit nem lopták el hálózati szinten. Ez figyelemre méltó eredmény.

Miért ért olyan sok bitcoin tőzsdét hackertámadás?

A kriptovaluta tőzsdék nagyon népszerűek, mind a befektetők számára – akik először vásárolnak bitcoint –, mind a spekulánsok számára – akik bitcoinnal vagy kriptovalutákkal kereskednek fiat valuta ellenében. Ennek eredményeként a tőzsdék

nagy mennyiségű bitcoint és fiat-pénzt tartanak ügyfeleik nevében, ami vonzó célponttá teszi őket a hackerek és a tolvajok számára. A letétkezelői szolgáltatások a KYC („Ismerd az ügyfeled") eljárásuk részeként tárolják ügyfeleik személyi igazolványainak, útleveleinek és otthoni címeinek másolatait is.

A támadások mind belső, mind külső támadások lehetnek. A belső támadások olyan alkalmazottaktól származhatnak, akik kiváltságos hozzáféréssel rendelkeznek a tőzsde rendszeréhez, és ezt felhasználják az ügyfelek pénzének ellopására. A külső támadásokat olyan hackerek hajtják végre, akik szoftveres sebezhetőségeket, gyenge működési biztonságot és tervezést használják ki a bitcoin ellopására.

Számos tőzsdét megtámadtak már mind belső, mind külső támadás keretében. Csak néhány példa az Mt.Gox Japánban, a Bitfinex Hongkongban, a Bitstamp az EU-ban és újabban a Quadriga Kanadában. Mindegyik révén több millió dollárnyi bitcoin veszett oda. Ezek a hackertámadások komoly figyelmeztetésként szolgálnak azoknak a felhasználóknak, akik engedélyezik, hogy valaki más őrizze a bitcoinjaikat. Az ügyfelek, akik a tőzsdéken kereskednek, időnként lehívhatják a bitcoinjaikat a személyes tárcáikba, hogy elkerüljék a hackertámadás okozta esetleges veszteségeket.

A bűnözők a bitcoint használják pénzmosásra?

Igen. A bűnözők pénzmosásra és illegális tevékenységekre használják a bitcoint, és ez a jövőben sem fog változni. A leghíresebb eset a Silk Road, egy darknet piactér, ahol a bitcoint az Egyesült Államokban illegálisnak minősített gyógyszerek vásárlására és eladására használták.

Mivel a bitcoin engedély nélküli technológia, bárki használhatja, mint például a mobiltelefont vagy az internetet. Kevesen kérdőjelezik meg ezeknek a mindenütt jelenlévő technológiáknak a legitimitását, vagy követelnek tiltást, mert a rossz szereplők használják őket. Sokan ellenséges szkepticizmussal rendelkeznek a technológiák iránt, amikor azok először megjelennek.

Mindenesetre a mai világban a pénzügyi bűnözés abszolút többségét a meglévő pénzügyi rendszer segítségével, szabályozott bankokon és pénzátutalási szolgáltatásokon keresztül hajtják végre. A legtöbb csalást a kormányok és a multinacionális vállalatok követik el, nem pedig a szélhámosok. A demokratikus kormányok pénzmosás elleni szabályokat (AML) vezettek be, hogy nyomást gyakoroljanak a bankokra bizonyos tranzakciók leállítására, mégis évente több mint 1 billió dollárt mosnak a bankrendszeren keresztül tisztára. Hogy egy példát említsünk, a jelentések nemrégiben nyilvánosságra hozták, hogy a dán Danske Bank egyetlen irodája megdöbbentő, 230 milliárd dollárt mosott tisztára, ami több, mint az írás idején forgalomban lévő összes bitcoin piaci értéke.

Tehát bár a bűnözők bitcoint is használnak, inkább a fiat pénzrendszert részesítik előnyben.

A bitcoin egy piramisjáték?

A Ponzi-rendszer nagy nyereséget ígér a befektetőknek, nagyon alacsony kockázattal. A Ponzi-rendszerek ezeket a hozamokat a korábbi befektetőik számára úgy érik el, hogy a későbbi befektetőktől összegyűjtött pénzzel fizetik ki őket. Nincs valódi nyereségszerzési mechanizmus azon kívül, hogy megpróbálnak minél több új befektetőt beszervezni, hogy kifizessék azokat, akik korábban érkeztek. Ezek a rendszerek összeomlanak, ha nincs új befektető.

A bitcoin nem egy Ponzi-rendszer. A bitcoin mögött nincs olyan embercsoport, amely megpróbálna új vásárlókat csábítani a régi vásárlók kifizetésére. Azok az emberek, akik Ponzi-rendszereket szerveznek, ugyanúgy elfogadhatják a bitcoint a befektetőiktől, mint minden más pénzt.

A bitcoin egy buborék?

A buborék akkor fordul elő, amikor a spekulatív befektetők tömegesen megvásárolnak egy pénzügyi eszközt olyan áron, amely messze meghaladja az alapvető értékét. A buborékok mindig kipukkadnak, amint az eszközbe vetett hit elvész, és más befektetők nem hajlandók megvásárolni a kért áron. A történelemből néhány példa a holland tulipán az 1500-as évekből, a South Sea Company az 1700-as évekből és a Dotcom részvények a 2000-es évek elejéről.

A 3. fejezet a bitcoin áringadozásának néhány fő mozgatórugóját írta le. Egy merev monetáris politikával rendelkező eszköz természetes volatilitása, a rendszeres kínálati sokkok, az egyéb kriptovaluták instabilitása és összeomlása, a piaci manipuláció és a bitcoin kereskedés tőkeáttételes jellege miatt számos áremelkedés történt, amelyeket jelentős összeomlások követtek. Ez a tendencia valószínűleg folytatódni fog.

Ha figyelembe vesszük a hosszú távú értéket, az árbefolyásoló tényezőket, a bitcoin decentralizált jellegét, annak értéke természetesen növekszik, ahogy egyre több ember használja. A tulipánokkal vagy a Dotcom részvényekkel ellentétben a bitcoin értéke minden nagyobb piaci összeomlás után többször helyreállt és felfelé fordult, mivel egyre több ember szerez bitcoint szerte a világon.

Mi az a Tether, és hogyan befolyásolja a bitcoint?

A Tether vagy USDT egy olyan érme, amelynek értéke elvileg az amerikai dollárhoz kötött. Ennek elérése érdekében a Tether mögött álló vállalat minden forgalomban lévő Tether tokent egy amerikai dollárral kíván fedezni a társaság bankszámláján. Az USDT megkönnyítette a kriptovaluta spekulációt, mivel a legtöbb ember még mindig fiat-pénzben gondolkodik, és az USDT az amerikai dollár helyettesítőjeként lehetővé tette, hogy bárki a kripto tőzsdéken aktívan kereskedjen amerikai dollár ellenében.

2019 áprilisában azonban a Tether főtanácsadója elárulta, hogy a forgalomban lévő Tether mindössze 74%-át fedezi amerikai dollárral. Ha a Tether dollártámasza megszakad, az ár összeomlása rövid távon a bitcoin volatilitását okozhatja – de számos olyan versenytárs van a Tether számára, akik készen állnak arra, hogy átvegyék a szerepét.

A kormányok betilthatják vagy lekapcsolhatják a bitcoint?

Mivel nincs cég, nincs központilag koordinált szerver, és nincs egyetlen csapat sem, mely a bitcoint működtetné, így nincs gyakorlati módja a hálózat leállításának.

A bitcoin nyílt forráskódú szoftver, ami azt jelenti, hogy a forráskód nyilvánosan elérhető az interneten. A szoftver korrumpálása vagy megváltoztatása nagyon nehéz, mert az emberek figyelik. Bárki letöltheti, használhatja, lemásolhatja és futtathatja a bitcoin szoftvert, és validálhatja a főkönyvet. Ezt

nevezzük a teljes csomópont futtatásának. Minél több teljes csomópont van a hálózaton, annál ellenállóbbá válik a bitcoin.

A kormányok megnehezíthetik a bitcoin használatát, de ezután az egész csak egy bújócskává válik. Nézzük meg a bitcoin és fiat-pénz cseréjét egy olyan országban, mint Kína. Amint azt az 1. fejezetben említettük, a kínai magánszemélyek évente legfeljebb 50 000 dollárnyi jüant válthatnak át, mégis továbbra is használják a bitcoint a pénz külföldre történő mozgatására.

Még egy nagy, gazdag rendőrállam sem tudja megakadályozni állampolgárait a bitcoin használatában. Mivel a hálózatnak nincs egyetlen meghibásodási pontja sem, a kormányok nem tudják kikapcsolni a bitcoin hálózatot.

A bitcoin ilyen módon hasonlít az internethez. A kormány megakadályozhatja, hogy a polgárok hozzáférjenek az internet egyes részeihez – például a Nagy Kínai Tűzfal – de a cenzúrázott polgárok olyan eszközöket fognak használni, mint a VPN-ek és a leleményesség, hogy megkerüljék ezeket a korlátozásokat. Egyetlen kormány sem tudja blokkolni a bitcoin hálózathoz való hozzáférést anélkül, hogy ne szüntetné meg magához az internethez való hozzáférést, és ezt a költséget Észak-Koreán kívül csak kevés kormány hajlandó vállalni.

Az autoriter kormányok betilthatják a bitcoin tartását, de ennek a végrehajtása rendkívül nehéz lenne. Digitális jellege miatt a bitcoin elrejtése viszonylag egyszerű. A bitcoin tárolása telefonon, USB-eszközön vagy akár az ember fejében mind olyan lehetőségek, amelyeket nagyon nehéz felfedezni és büntetni. Ezzel szemben az aranyat, az ingatlanokat, a részvényeket és a fiat-pénzt a bankszámlákon viszonylag könnyű a kormányok által megtalálni és elkobozni.

Legális a bitcoin?

Többnyire igen. 2019 augusztusától a tartása Namíbia, Algéria, Bolívia, Irak, Marokkó, Nepál, Pakisztán, Egyesült Arab Emírségek és Vietnam kivételével minden országban megengedett. Szabályozási szempontból a bitcoin hosszú utat tett meg: az elmúlt 10 évben a bitcoint az online bűnözők pénzének tekintették, ma az IMF, az amerikai kongresszus és a Wall Street is elismeri.

Kínában a kormány szabályozza a kriptovaluta tőzsdéket és az új tokenek létrehozását, de a bitcoint jogilag digitális tulajdonként ismerik el. Még Iránban is, a bitcoin bányászat legális iparággá vált.

Az afrikai kontinensen a legtöbb ország kormányának nincs nyilvános álláspontja. Olyan helyeken, mint Nigéria és Kenya, a köztisztviselők figyelmeztetnek a használatára, de nincsenek konkrét szabályok. Dél-Afrika jelenleg az egyetlen afrikai ország, ahol a bitcoin hivatalosan elfogadott és szabályozott.

Kanadában, az Egyesült Államokban és az EU-ban a bitcoin tartása és használata legális. Néhány ország létrehozott egy speciális engedélyezési keretet azoknak a vállalatoknak, amelyek kriptovaluta tőzsdéket kívánnak működtetni. Ezek közé tartozik Japán, Málta, a Fülöp-szigetek és Thaiföld.

Az adózási szabályok bonyolultabbak, és az egyes kormányok bitcoin osztályozásának módja határozza meg őket. Ha az adóhatóság a bitcoint ingatlannak tekinti, akkor a magánszemélyek ennek megfelelően adóznak a megszerzése, likviditása, felértékelődése és értékcsökkenése után, hasonlóan egy ingatlanhoz.

A jövőre nézve, ha a kormányok össze akarnának fogni a bitcoin betiltására, nem valószínű, hogy meg tudnának állapodni. Még ha egyes országoknak sikerülne is tilalmat bevezetniük, más országok közbe lépnének, és üdvözölnék a bitcoin bányászokat, vállalkozókat és kereskedőket. A tehetség és a gazdagság elvándorlása a barátságosabb joghatóságokba vezetne, ami arra késztetné a korlátozó kormányokat, hogy újragondolják politikájukat.

A bitcoin bányászat energiapazarlás vagy káros a környezetre?

2019 júniusától a bitcoin hálózat évente körülbelül 73 terawattóra villamos energiát fogyaszt. Ez valamivel több, mint Ausztria fogyasztása (évi 69 terawattóra), de sokkal kevesebb, mint Kínáé (évi 6100 terawattóra) és az Egyesült Államoké (évi 3900 terawattóra), a két legnagyobb energiafogyasztóé.

A kritikusok gyorsan rámutatnak, hogy ez hatalmas fogyasztás. Bár ez technikailag igaz, nem foglalkozik azzal, hogy a bitcoin pazarolja-e az energiát, vagy hogy káros-e a környezetre. A bitcoin bányászok által jellemzően használt energiaforrások és a bitcoin által nyújtott érték némi kontextust biztosíthatnak.

Az energiapazarlás megelőzése a bitcoin bányászattal

A bitcoin bányászat segíthet a felesleges kapacitás jó felhasználásában. A bányászat mind mobil, mind alacsony árrésű üzlet. Ezért a bányászati vállalatoknak különösen nagy az ösztönzésük és a képességük arra, hogy fizikailag a lehető legolcsóbb villamos energiát keressék. Gyakran a legolcsóbb energiaforrások távoli vagy megközelíthetetlen helyeken találhatók, ahol kihasználatlan kapacitás áll rendelkezésre.

A bitcoin bányászat nagy része Kínában zajlik, ahol az erőművek együttesen 200 terawattóra többletet termelnek egy adott időpontban. (Fordító megjegyzése: Kína 2021-ben betiltotta a bitcoin bányászatot, ezért az ott üzemelő bányák többsége más országokba költözött.) Mivel ennyi energiát nem lehet tárolni (a világ legnagyobb akkumulátorfarmja ennek a mennyiségnek csak mintegy 0,5%-át képes tárolni) – és mivel nem lehet hatékonyan továbbítani az energiát a távoli régiókba –, a villamos energia általában kihasználatlan marad. Ahelyett, hogy elpazarolnák ezt a potenciált, az erőművek megvásárolhatják a bitcoin bányászati berendezéseket, és a felesleges energiát új bitcoinokká alakíthatják. Ez minden olyan helyen igaz, ahol egy energiaforrás túl sokat termel az azonnali felhasználáshoz.

A bitcoin bányászat megújuló energiára támaszkodik

A bitcoin bányászat nagy része ma megújuló energiával történik, ami minimális környezeti költséggel jár. A legfrissebb becslések szerint jelenleg az összes bitcoin bányászat mintegy 75%-a víz-, nap-, szél- és geotermikus energiaforrásokat használ. A megújuló energiával működő bitcoin bányászat mintegy 50%-át Kína egyazon területén végzik, amelyet vízenergiával működő gátak táplálnak.

A vízerőművek hatalmas energiatermelő kapacitással rendelkeznek, de gyakran kihasználatlanok. A bitcoin bányászat kihasználja a többletkapacitást, mivel a bányászati művelet a vízerőmű mellé helyezhető, így az átviteli költségek megszűnnek. A keletkező bevétel a vízenergia termelését és kutatását teszi jövedelmezőbbé, ami ösztönzi a vízenergia használatát. Ily módon a bitcoin bányászat támogatja a vízenergiát.

A bányászat ösztönözheti a nap-, szél- és geotermikus energiatermelést is.

A bitcoin bányászat biztonságos, hozzáférhető pénzt tesz lehetővé

A bitcoin bányászok gondoskodnak a hálózat biztonságáról. Amint azt a 2. fejezetben tárgyaltuk, a bányászoknak a ritka proof-of-work számok kereséséhez áramra van szükségük, hogy érvényes blokkokat javasoljanak, ez viszont nagyon költségessé teszi a csalást. Minél több bitcoin bányász van, annál nehezebb megtámadni a hálózatot. A főkönyv védelmére fordított energiát össze lehet hasonlítani egy 200 milliárd dollár értékű vagyontárgyakat védő, nagybiztonságú páncélterem létrehozásának és fenntartásának költségeivel.

Lehet, hogy a bitcoin csak egy a sok pénzügyi lehetőség közül a fejlett világban élők számára, de a világ más részein az olyan fizetési szolgáltatások, mint a Venmo vagy az ApplePay nem állnak rendelkezésre. Ha a bitcoin bányászatot energiapazarlásnak tekintjük, azzal lebecsüljük a bitcoin hasznosságát a technológiai alosztály számára. Ennek az energiának egy része olyan emberek tranzakcióinak feldolgozására irányul, akiknek nincs bankszámlájuk vagy dokumentumaik, vagy akik nem akarják, hogy pénzügyi tevékenységüket a kormányok szigorúan ellenőrizzék. A bankok és a hitelkártyák meghaladhatják a bitcoin hasznosságát egy olyan helyen, mint az Egyesült Államok, de semmit sem tesznek egy bank nélküli dubaji vendégmunkás vagy egy ENSZ-szankciók alatt élő iráni számára.

Energiafelhasználás és technológiai innováció

A bitcoin egy jelentős technikai újítás, amely lehetővé teszi a könyvben felvázolt sok olyan dolgot, amire a jelenlegi monetáris rendszer nem képes. Történelmileg az új technológiák több energiát használnak, mint az általuk kiszorított régi

rendszerek. Gondoljunk például arra, hogy a lovat felváltotta az autó, a tábori sátrat a modern kórház, a kézi mosást a mosógép, a jégszekrényt a hűtőszekrény, az olajlámpát pedig az elektromos lámpa. A műszaki innováció villamosenergia-költségét ellensúlyozza az általa lehetővé tett jobb életminőség. A civilizáció fejlődésével egyre több energia jut egy emberre. Az innováció megerősíti a társadalmat, és nincs olyan innováció, amelyet ne fogadnánk el bizonyos kompromisszumok nélkül. A bitcoin esetén a kompromisszum a villamosenergia-felhasználás, cserébe egy tisztességes, kényelmes és biztonságos pénzrendszerért. A bitcoin sok energiát használ, de a megújuló energiaforrások innovációjának motorja. A bitcoin óriási értéket képvisel, különösen a szegények és elnyomottak számára, és egy hibás, régebbi rendszert vált fel, amely még több energiát használ.

Mi van, ha valaki egy szuperszámítógéppel vagy kvantumszámítógéppel feltöri a bitcoin hálózatot?

Elméletileg a bitcoin hálózatot egy elég nagy számítási kapacitással rendelkező támadó feltörhetné. A gyakorlatban ez azonban nagyon nehezen kivitelezhető.

Egy jelenlegi hardvert használva egy támadónak több mint 1 milliárd dolláros költséggel kellene számolnia, meg kellene építenie és üzemeltetnie egy bányászati létesítményt, majd találnia egy olyan energiaszolgáltatót, amelynek a teljesítménye 8 Hoover-gátének felel meg. Ugyanezeket az erőforrásokat becsületesen bányászatra fordítva rendkívül jövedelmező vállalkozása lenne. Egy ilyen támadás tehát gazdaságilag irracionális.

E sorok írásakor ezek a dolgok igazak a kvantumszámítástechnikára:

1. A kvantumszámítógépek a hagyományos számítógépekhez képest nagyságrendekkel lassabbak.

2. A kvantumszámítógépek megépítése rendkívül drága, és még jó ideig nem is lesz költséghatékony.

3. A legismertebb kvantumalgoritmusok jelentős előrelépést jelentenek, de a bitcoinhoz használt kriptográfia feltöréséhez még mindig sok milliárd, évmilliárdokig működő számítógépre lenne szükség.

Még ha a tudósok olyan új kvantumalgoritmusokat fedeznének is fel, amelyek képesek lennének feltörni a modern kriptográfiát, a kvantumbiztonságos kriptográfia akkor is beépülne a bitcoinba.

Más szóval élve a bitcoin felhasználói és fejlesztői közössége egy lépéssel a kvantumtámadók előtt járhatna. Bár a bitcoin közösségnek ébernek kell lennie a nagyszabású támadási lehetőségekkel szemben, az átlagos bitcoin felhasználónak nem kell aggódnia.

Hogyan maradhat a bitcoin decentralizált?

A bitcoin egyik legfontosabb tulajdonsága, hogy a világon bárki letöltheti a teljes bitcoin főkönyv másolatát – a hálózaton valaha végrehajtott minden egyes tranzakciót –, és saját maga ellenőrizheti, hogy a történelmi nyilvántartások helyesek.

A 2. fejezetben leírtak szerint ezt a gyakorlatot egy teljes csomópont futtatásának nevezzük. A teljes csomópont működtetésének egyszerűsége kritikus fontosságú a bitcoin hálózat általános cenzúrával szembeni ellenállása szempontjából. Ha a bitcoin hálózat egy maroknyi vállalatra vagy gazdag emberek egy kis csoportjára támaszkodna a teljes csomópontok működtetésében, akkor ezek összejátszhatnának, és szerkeszthetnék a nyilvántartásokat, vagy ellophatnák az érméket. Minden felhasználó egy teljes csomópont futtatásával mindent ellenőrizhet, és nem kell megbíznia senkiben. Ha egy teljes csomópont működtetéséhez drága szervereszközökre vagy gyors internet kapcsolatra lenne szükség, az arra kényszerítené a szegényebb embereket, hogy megbízzanak másokban. A hálózat természetesen a fejlett világban lévő helyszínek és a csúcstechnológiai vállalkozások köré összpontosulna.

Szerencsére mivel egy teljes csomópont futtatásához nagyon alacsonyak a követelmények, sok ezer, egymás számára teljesen ismeretlen felhasználó különböző kontinenseken folyamatosan ellenőrzi a bitcoin blokkláncát. Ráadásul mivel egyre több felhasználóbarát hardveres teljes csomópont áll rendelkezésre a piacon, egy teljes csomópont otthoni üzemeltetése a nem technológiai felhasználók számára is elérhetővé válik. Jelenleg több tudós olyan intézményekben, mint az MIT és a Stanford, segít olyan módszereket kidolgozni, amelyekkel a jövőben bárki teljes csomópontot futtathat a mobiltelefonján, ami tovább javítaná a bitcoin hálózat decentralizációját.

Milyen a bitcoin adatvédelme?

Népszerű tévhit, hogy a bitcoin anonim. A bitcoin pszeudonim, elegendő nyomozói munkával és törvényszéki elemzéssel összekapcsolhatók a felhasználó tranzakciói és

a személyazonossága. Megfelelő működési biztonság mellett egy hozzáértő bitcoin felhasználó olyan mértékben álcázhatja a tranzakciókat, hogy megnehezítse a megfigyelést. Elegendő idővel vagy erőforrásokkal azonban egy motivált nemzetállam vagy vállalat továbbra is nyomon követheti az illetőt.

Ennek ellenére a bitcoin sokkal jobb adatvédelmet biztosít a tranzakciók számára, mint a meglévő fizetési rendszerek. A bitcoinnal történő online vásárlás megvalósítható anélkül, hogy felfedné a személyes adatokat, például valaki nevét, bankszámláját vagy címét. Ez előrelépés a jelenlegi bankrendszerhez képest, ahol a kormányok, vállalatok és kereskedők naponta kérik, majd megosztják, eladják vagy kiszivárogtatják a személyes adatokat.

A bitcoin folyamatban lévő és tervezett fejlesztései, mint például a Lightning Network, a Taproot, a Graftroot és a Schnorr Signatures együttesen olcsóbbá és egyszerűbbé teszik a privát bitcoin tranzakciókat. A bitcoin kiváló adatvédelmi technológia lehet, amely rendkívüli mértékben megnehezíti a tömeges pénzügyi felügyeletet.

Az internet egykor teljesen nyitott és nyilvános volt. Mivel a felhasználók és a vállalkozások több privát tranzakciót igényeltek, a mérnökök az eredeti internetre építve több adatvédelmi réteget adtak hozzá. A privát kommunikáció most már lehetséges olyan alkalmazásokkal, amelyek automatikusan titkosított üzeneteket küldenek. A bitcoin hasonló utat követ.

Hogyan tudja a bitcoin kielégíteni 7 milliárd ember igényét?

1989-ben, amikor a szakemberek feltalálták a World Wide Web-et, hogy az az interneten futhasson, technikailag lehetetlennek tűnt az a gondolat, hogy a felhasználók egy nap fényképeket, sőt videókat cserélhessenek egymással. A technológia fejlődésével és kibontakozásával az internet olyan, egykor elképzelhetetlen, erőforrás-igényes alkalmazásokhoz igazodott, mint a videomegosztás és a konferencia. Percenként 300 órányi videót töltenek fel az emberek a YouTube-ra, és naponta 5 milliárd videót néznek meg. Csakúgy, mint az internet, a bitcoin skálázásának is számos módja van.

Amint azt a 4. fejezetben tárgyaltuk, a bitcoin kapacitását jelenleg a Lightning hálózaton keresztül bővítik. Továbbá a tranzakciók adatvédelmének fokozása érdekében a Lightning a bitcoin hálózatot is skálázza.

A Lightning másodpercenként több millió bitcoin tranzakciót képes kezelni. A bitcoin jó úton halad az exponenciális skálázás felé, míg a hagyományos fizetési hálózatok, mint például a Visa, lineárisan skáláznak egyre több szerver hozzáadásával. A bitcoin forradalmasíthatja a pénzt, és teljesen új megoldást tesz lehetővé olyan mikrofizetésekkel, amelyek egyszerre csak egy-egy ezreléknyi (1/1000) satoshit használnak.

Az óvatos, lassú, ultra-biztonságos és cenzúrának ellenálló alkalmi, láncon belüli tranzakciók, valamint a Lightningon történő azonnali és olcsó tranzakciók kombinációjával a bitcoin teljes körű globális fizetési rendszerré válhat. Ezt az elképzelést érdemes követni, mivel ez még inkább kivenné a kormányok és a vállalatok kezéből a pénzügyek feletti hatalmat, és visszahelyezné azt az emberek kezébe.

Bár ma még nehéz elképzelni, hogy a bitcoin több milliárd ember igényeit kielégítse, ez nem kevésbé elrugaszkodott elképzelés, mint egykor az interneten a több milliárd nézőnek közvetített videostreaming.

Létezik-e rendkívüli vagyoni egyenlőtlenség a bitcoin esetében?

Azoknak az embereknek, akik a korai szakaszban léptek be a térbe, lehetőségük volt sok bitcoin felhalmozására. A blokklánc azonban azt mutatja, hogy sok korai felhasználó 2009 és 2012 között el is adta a bitcoint ugyanebben az időszakban.

Sok vásárló 2011-ben 1 dollárért vette, néhány hónappal később 4 dollárért, vagy pár hónappal azután 30 dollárért eladta. Sok korai felhasználónak nem volt elég türelme ahhoz, hogy átvészelje a kezdeti idők szélsőséges volatilitását és bizonytalanságát, vagy elvesztette a privát kulcsát, így a bitcoinjai végleg elvesztek. Azok, akik kitartottak, már a kezdetektől fogva támogatták az ökoszisztémát, és valóban hisznek abban, hogy a bitcoin megváltoztathatja a világot. Ma néhány ezer cím tárolja a bitcoin nagy részét. Néhányan olyan magánszemélyek, akik most rendkívül gazdagok. A legtöbb olyan vállalat, amely ezeken a címeken ügyfelei tízezreinek vagyonát tárolja (pl. Coinbase, Binance). Mivel a címek és a felhasználók között nincs egy az egyben összefüggés, nehéz megmondani, hogy pontosan milyen lehet a vagyoni eloszlás.

A bitcoin nem fogja megoldani a gazdasági egyenlőtlenségeket. Aki ezt mondja, hazudik. Mivel azonban a bitcoin egy mindenki számára hozzáférhető értéktároló, amelyet a kormányok nem értékelhetnek le, a jelenlegi monetáris rendszerrel ellentétben a megtakarítóknak tisztességes esélyt ad arra, hogy idősebb korukban is megtarthassák, amit megkerestek.

Ha csak 21 millió bitcoin van, hogyan használhatja azt az egész világ?

A hagyományos fiat valutaegységeket általában 100 alegységre osztják, amelyeket fillérnek vagy centnek neveznek. Az USA dollár és az euró 100 centre, a kínai jüan 10 jiao-ra vagy 100 fen-re, a cseh korona pedig 100 halerre osztható.

A bitcoinok viszont 100 000 000 (százmillió) kisebb egységre oszthatók. A bitcoin atomegységét satoshinak (vagy röviden sat-nak) hívják a bitcoin feltalálója után.

Így a bitcoin teljes kínálata 2 100 000 000 000 000 satoshi. Összehasonlításképpen, ez jobban osztható, mint az amerikai dollár, amelynek M2 pénzkínálata 1 500 000 000 000 000 000 cent e sorok írásakor. A bitcoin oszthatósága egyenlő vagy jobb, mint az USA dolláré.

Ha az összes létező satoshit elosztjuk 7 milliárd ember között, akkor fejenként 300 000 satot kapunk. Ez elég oszthatónak tűnik ahhoz, hogy kielégítse az egyes emberek gazdasági tevékenységét, ha a bitcoin a világ uralkodó pénzévé válik.

Hogyan engedhetem meg magamnak a bitcoint? Olyan drága egy bitcoin!

A bitcoin osztható, így egy bitcoin kis töredékét is meg lehet vásárolni – 5 vagy 25 dollár értékű bitcoin jelenleg 0,00044 bitcoinnak, illetve 0,0022 bitcoinnak felel meg.

Hogyan juthatok bitcoinhoz?

A bitcoin beszerzésének elsődleges módjai a következők:

1. Bányászat
2. Vásárlás
3. Pénzkeresés

Bányászat

A bitcoin történetében a bitcoin bányászat nagyon alacsony árrést biztosító üzlet. Az aranybányászathoz hasonlóan a nyereséges bányászathoz szükséges berendezések, ipari kapcsolatok és speciális ismeretek több éves tapasztalatot és több millió dollárnyi tőkét igényelnek. A bányászat így a jelentős erőforrásokkal és szaktudással rendelkező vállalkozások és szervezetek birodalmává vált, és a tapasztalatlan egyének számára lehetetlen nyereségesen bányászni. Az új felhasználók számára a bitcoint olcsóbb vásárlással vagy pénzkereséssel beszerezni, mint bányászattal.

Vásárlás

A bitcoin megvásárlásának számos módja van, némelyik privátabb, mint a többi. A bitcoin ATM-ek és a peer-to-peer kereskedés gyors és viszonylag privát. A befektetők feliratkozhatnak online tőzsdékre, amelyek közül többet a *További források* között talál. Az új ügyfeleknek el kell küldeniük személyes adataikat, és a jóváhagyási folyamat néhány perctől akár néhány napig is eltarthat. Ezek a vállalatok bankként működnek, és ügyfeleik bitcoinjait, illetve fiat-pénzét őrzik. Használatuk tehát a magánélet némi feladásával jár, de az ügyfelek biztosíthatják bitcoinjaik tulajdonjogát, ha ezekből a szolgáltatásokból személyes tárcájukba hívják le a pénzt.

Pénzkeresés

Egy bitcoin vagy Lightning tárca használatával bárki közvetlenül fogadhat bitcoint áruk vagy szolgáltatások ellenértékeként. A munkavállalók bitcoin bérszámfejtési szolgáltatásokat vehetnek igénybe, hogy bérük egy részét fiat helyett bitcoinban kapják meg.

Hogyan kell bitcoin tárcát használni?

Számos különböző típusú bitcoin tárca létezik, beleértve a hardvertárcákat, az asztali, a mobil és az online tárcákat. Mindegyiknek különböző biztonsági, kényelmi és adatvédelmi kompromisszumai vannak, amelyeket a felhasználóknak érdemes tanulmányozniuk.

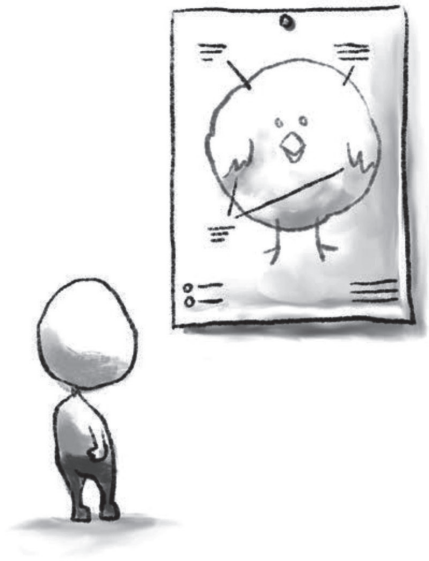
A bitcoin tárolásának ésszerűen biztonságos módja egy letétkezelő nélküli tárca, melyek közül néhányat a *További források* alatt *Hardver tárca* megnevezéssel sorolunk fel. Ugyanakkor az elindulás legkényelmesebb módja egy ingyenes mobiltárca letöltése, amelyek közül néhány a *További források* alatt *Tárcák* néven található.

A letöltés után a bitcoin tárca beállításának első lépése egy biztonsági mentés létrehozása. Ezt a biztonsági mentést *jelszómondatnak* vagy angolul *seed phrase-nek* nevezik, és arra használják, hogy ha a tárca elveszne, újból elérjék azt. A jelszómondat olyan szavak listája, amelyeket általában egy darab papírra írnak. Mivel a tárca újbóli eléréséhez a jelszómondat használható, gondosan kell őrizni. Gondoljon erre a kifejezésre ugyanúgy, mint egy aranyrúdra vagy egy gyémántra. A seed phrase vagy jelszómondat jelentős értéket képvisel, és ennek megfelelően kell védett helyen őrizni. Az ökoszisztéma növekedésével az új tárcák a

komplexitás csökkentésére összpontosítanak, miközben javítják a használhatóságot, a biztonságot és az adatvédelmet.

A tárca beállítása után egyedi címeket generálhat minden új fizetéshez. Ez eltér a szokásos banki fizetések működésétől, ahol az ügyfélnek általában csak egy számlaszámot biztosítanak. A bitcoin jobb pénzügyi adatvédelmet biztosít egyedi címek kiadásával, amelyek mindegyike ugyanahhoz a bitcoin tárcához tartozik.

Amint azt a *Miért ért olyan sok tőzsdét hackertámadás?* részben említettük, a letétkezelési szolgáltatásokat igénybe vevő befektetők a tőzsdei hackertámadások kockázatának vannak kitéve. A vásárlás után a pénzeszközök személyes tárcákba történő lehívása enyhíti ezt a kockázatot.



További Források

A Bitcoin tanulmány

Satoshi Nakamoto *Bitcoin: Egy peer-to-peer elektronikus készpénzrendszer* című tanulmánya az eredeti mestermű, ami elindította ezt a pénzügyi innovációt, immár több mint egy évtizede.

Forráskód

A *Bitcoin Core* a bitcoin csomópont szoftver referencia implementációja. A kezdetekben Satoshi Nakamoto hozta létre, de azóta több mint 500 fejlesztő dolgozott rajta szerte a világból. (Megjegyzés: magyar fordításban is elérhető.)

Könyvek

Andreas M. Antonopoulos *The Internet of Money (Vol 1 & 2)* könyvében gyűjtött össze több esszét és előadást, és egy sor ‹miért› kérdésbe merül bele a bitcoin kapcsán.

Jimmy Song *Programming Bitcoin* könyve egy gyakorlatias technikai anyag a bitcoin programozás meghatározó tanítójától, azoknak a fejlesztőknek, akik a bitcoinra szeretnének építeni vagy továbbfejleszteni.

Saifedean Ammous *Bitcoin Standard – A központi bankok decentralizált alternatívája* a pénz gazdaságtani történetét mutatja be, és elmagyarázza hogy a bitcoin miképpen alternatívája a központi bankoknak. (Megjegyzés: magyar fordításban is elérhető.)

Yan Pritzker: *Inventing Bitcoin:* lépésről lépésre mutatja be a bitcoin működését, oly módon, hogy iskolai szintű matematika tudásnál nem vár el többet az olvasótól.

Kalle Rosenbaum: *Grokking Bitcoin:* egy gazdagon illusztrált bevezető a bitcoin működésébe.

Bitcoin Money: A Tale of Bitville Discovering Good Money by The Bitcoin Rabbi: egy gyerekkönyv, színes szereplőkkel mesél a bitcoinról kicsiknek.

Andreas M. Antonopoulos: *Mastering Bitcoin: Programming the Open Blockchain:* egy komplett áttekintése a bitcoin- és bitcoinnal való programozásnak.

Weboldalak és kiadványok

Bitcoin.org weboldal: hasznos induló információk gyűjtőhelye, dokumentációkkal és linkekkel. A Bitcoin.com nem ajánlott, mivel ez az oldal szándékosan összemossa a bitcoint egyéb kriptovalutákkal, hogy az embereket ez utóbbiak irányába terelje.

A *Bitcoin.page* oldal egy valódi kincsesbánya, bitcoin oktató anyagok és információk hasznos gyűjteménye, Jameson Lopp gondozásában.

A *Bitcoin Wiki* egy nyilvános gyűjtemény a bitcoin közösség, fejlesztők, cégek és minden érdeklődő számára.

A *Coin Center* egy USA-beli nonprofit szervezet, ami a bitcoint és egyéb kriptovalutákat érintő szabályozási kérdésekkel foglalkozik. Rendszeresen tesznek közzé tartalmas, köznyelven megfogalmazott magyarázó anyagokat.

Bitcoinmining.com a bitcoin bányászattal kapcsolatos anyagokat tartalmaz: hogyan működik, hogyan érdemes belekezdeni, hardver infók.

Global Coin Research: kriptovaluta trendekkel foglalkozik, USA és Ázsia fókusszal.

Podcastok

Tales from the Crypt: Marty Bent podcastja, amiben érdekes emberekkel beszélget a bitcoinról.

What Bitcoin Did: Peter McCormack rendszeres műsora, melyben a bitcoin közösség vezető és ismert egyéniségeit kérdezi ki.

A *Stephan Livera Podcast* interjúiból és vitáiból a bitcoin gazdaságról és technológiáról lehet tanulni.

A Michael Goldstein and Pierre Rochard által hosztolt *Noded* a bitcoin technical újdonságaira fókuszál.

Anthony Pompliano *Off the Chain* podcastjában főleg befektetőket szólaltat meg a 'régi' és az 'új' pénzügyi rendszerből bemutatva, hogy hogyan gondolkodnak a bitcoinról és más hasonló eszközökről.

Unchained és *Unconfirmed:* Laura Shin heti műsora, melyben a kriptó világ neves szereplőit szólaltatja meg.

Let's Talk Bitcoin a kriptó világ ötleteit és arcait mutatja be a műsor házigazda-csapata.

The Bitcoin Knowledge Podcast: Trace Mayer a bitcoin iparág kiemelt szereplőit szólaltatja meg, hogy segítsen jobban megérteni a technológiát.

(Fordító megjegyzése: magyar nyelven a *Bitcoin Kebab* podcastot ajánljuk, melyben Stier Kata beszélget vendégeivel főként bitcoinról.)

Online váltók

Jogi nyilatkozat: Ugyan ez a rész konkrét bitcoinnal foglalkozó weboldalakat, applikációkat és szolgáltatásokat sorol fel, ez nem tekintendő ajánlásnak vagy befektetési tanácsnak. Mint a könyv egészével kapcsolatban, itt is mindenkit arra biztatunk, hogy végezzen saját körültekintő elemzést.

Fiat-kriptó között:
Bitfinex – hongkongi központú váltó, 2014-ben indult
CashApp – A Square cég applikációja (iOS-re és Androidra), bitcoint lehet vásárolni bankkártyával (USA)
Kraken – USA és EU-ban működő váltó, 2014-ben indult

Kriptó-kriptó:
Binance – 2017-ben indult váltó, máltai központtal
BitMex – 2014-ben indult váltó, Seychelle-szigeti központtal
Bittrex – 2016-ban indult USA váltó

Peer-to-peer piacterek:
LocalBitcoins – Finn hátterű bitcoin piactér, 2012-es alapítással

Paxful – 2015-ben indult USA bitcoin piactér
Bisq – Egy titoktartásra fókuszáló piactér, 2014-ben indult

Tárcák

'Letétkezelői' ('custodial'; a használó nem rendelkezik a privát kulcsok felett):
Blockchain.info
CashApp
Coinbase

'Nem letétkezelői' ('non-custodial'; a használónál van a privát kulcs):
BreadWallet – iOS tárca
Bitcoin Core – Asztali gép tárca
Casa Keymaster – Android and iOS több-aláírásos tárca app, hardver tárca támogatással
Samourai – Android tárca
Wasabi – Asztali gép tárca

Hardver tárca (a használó egy dedikált, biztonságos eszközön tartja a privát kulcsokat)
ColdCard
Ledger
Trezor

Teljes csomópont megoldások

Casa Node – Tartalmaz egy előrecsomagolt Lightning és bitcoin node-ot
Nodl – Bitcoin és Lightning node

Szójegyzék

arany standard – az a világrend, amelyben a vezető nemzetek *fiat* pénzüket megfelelő mennyiségű arannyal fedezték, amit kincstári tartalékként őriztek. Lásd még: fiat standard.

bancor – az 1944-es Bretton Woods-i találkozón javasolt világpénz.

bányász – egy személy vagy csoport („mining pool"), akik cél-számítógépeket használnak a ritka munka-bizonyíték számok keresésére, hogy új blokkokat hozzanak létre, és megnyerjék a blokk jutalmat.

bányász jutalom / bányász díj – bitcoin összeg, ami a bányászok bevétele, a tranzakciók feldolgozásáért és a hálózat védelméért cserébe.

Bitcoin – egy decentralizált, digitális, szűkös pénz, amit Satoshi Nakamoto alkotott meg.

bitcoin – a Bitcoin hálózaton létező pénz egysége. Váltópénze a satoshi, egy bitcoin 100.000.000 satoshira osztható.

blokk – a bitcoin tranzakciók egy csoportosítása, egy hozzá-csatolt munka bizonyítékkal (ritka számmal) együtt. Egy blokk olyan, mint egy oldal a bitcoin főkönyvében. Nagyjából 10 percenként jön létre egy új blokk.

blokklánc – egy decentralizált könyvelési rendszer, amit a bitcoin használt először. A bitcoin blokklánc nyilvántartja, hogy mennyi bitcoin tartozik minden egyes címhez. A blokklánc alkotóelemei a blokkok.

blokklánc technológia – olyan rendszer, amely valamilyen mértékben használja a bitcoin innovatív blokklánc megoldását. A bitcoin és néhány más kriptovalután kívül nincs olyan blokklánc technológiát alkalmazó más rendszer, amely széles körben elterjedt volna.

BTC – a bitcoin szimbóluma tőzsdéken és kereskedőknél. Ritkábban az XBT is használatos.

cím – egy bitcoin cím egy bankszámlaszámhoz hasonlítható azonosító; egy címen lehet bitcoin fogadni. Minden címhez létezik egy hozzá tartozó privát kulcs, aminek a segítségével tudja a tulajdonosa elkölteni a bitcoint, egy digitális aláíráson keresztül.

decentralizált – olyan rendszer, amelyben nincs központi hibalehetőség (nincs olyan pont, amelynek meghibásodása az egész rendszert leállítja). Lásd még: központosított.

digitális aláírás – annak bizonyítéka, hogy a felhasználó, avagy aláíró birtokában van egy adott címhez tartozó privát kulcsnak. Ez fogalmilag hasonló egy banki átutalás nyomtatvány aláírásához, amivel az aláíró igazolja, hogy valóban a számla tulajdonosa indította az utalást, viszont a digitális esetben nincs szükség a kézírás (vagy egyéb privát információ) felfedésére. Amikor valaki bitcoint küld, aláírja a tranzakciót, így igazolva a bitcoin feletti rendelkezését, de mindezt a privát kulcs bemutatása nélkül.

dollár standard – az aktuális, USA dollár által uralt világkereskedelmi rendszer. Az 1944-es Bretton Woods-i egyezséggel indult, és 1971 óta a ‘petródollár’ rendszerrel folytatódott.

feleződés – egy négyévente bekövetkező esemény, amikor a bitcoin blokkjutalom a felére csökken.

fiat pénz – egy központi bank által kibocsátott pénz.

fiat-kriptó tőzsde – olyan tőzsde, ahol fiat pénzeket közvetlenül lehet kriptovalutákra váltani (és vissza).

FOMO – „Fear Of Missing Out”, „ki ne maradjak”, a piaci szereplők ‘csordaviselkedésére’ és irracionális vásárlási döntéseire utaló kifejezés.

központi autoritás – olyan szervezet vagy ügynökség, amely döntéseket hoz egy adott rendszerről.

központosított (centralizált) – olyan rendszer, amelynek van egy központi hibalehetősége (egy olyan pont, amelynek meghibásodása az egész rendszert leállítja). Ez lehet például egy olyan rendszer, amit egyetlen személy, alapítvány, cég vagy kormány irányít.

kriptó-kriptó tőzsde – olyan tőzsde, ami csak különböző kriptovaluták közötti kereskedést támogat (fiatot nem).

KYC – „Know Your Customer”, „ismerd az ügyfeleid”, az a kormányok által megkövetelt gyakorlat, amikor a bankok csak úgy nyújtanak szolgáltatásokat, ha ügyfeleik sok személyes információt osztanak meg velük. Különböző törvények és szabályok a kormányszerveknek hozzáférést adnak az ügyféladatokhoz.

Lightning hálózat – a bitcoin hálózatra épülő fizetési rendszer, amelynek célja a jobb skálázhatóság, akár másodpercenkénti milliós nagyságrendű tranzakcióig. Ez a fejlesztés privátabbá is teszi a tranzakciókat.

likviditás – az a mennyiség egy eszközből, amelyet könnyen adni-venni lehet egy adott időszakban.

munka bizonyíték – 'proof of work', az eljárás ami által a bányászok matematikailag igazolják, hogy energiát fektettek egy új, érvényes blokk megalkotásába, melyet hozzá lehet fűzni a blokklánchoz.

nyilvános blokklánc – olyan blokklánc, amit bárki letölthet, hozzáférhet és böngészhet.

Octopus kártya – Honkongban használatos elektronikus fizetési rendszer.

off-chain tranzakció – láncon kívüli; olyan tranzakció, amely nem kerül be a bitcoin blokkláncba. Ilyen például egy Lightning tranzakció.

on-chain tranzakció – láncban; olyan tranzakció, amely közvetlenül a bitcion blokkláncban kerül feldolgozásra.

peer-to-peer váltó – olyan váltó, ahol az ügyfelek közvetlenül egymással kereskednek, gyakran személyesen találkozva.

privát kulcs – egy banki jelszóhoz hasonlóan, egy privát kulcs teszi lehetővé egy tárcában tárolt bitcoin elküldését. A privát kulcs birtoklása egyenértékű a bitcoin birtoklásával.

sat / satoshi – a bitcoin váltópénze. 100.000.000 (százmillió) satoshi egy bitcoin.

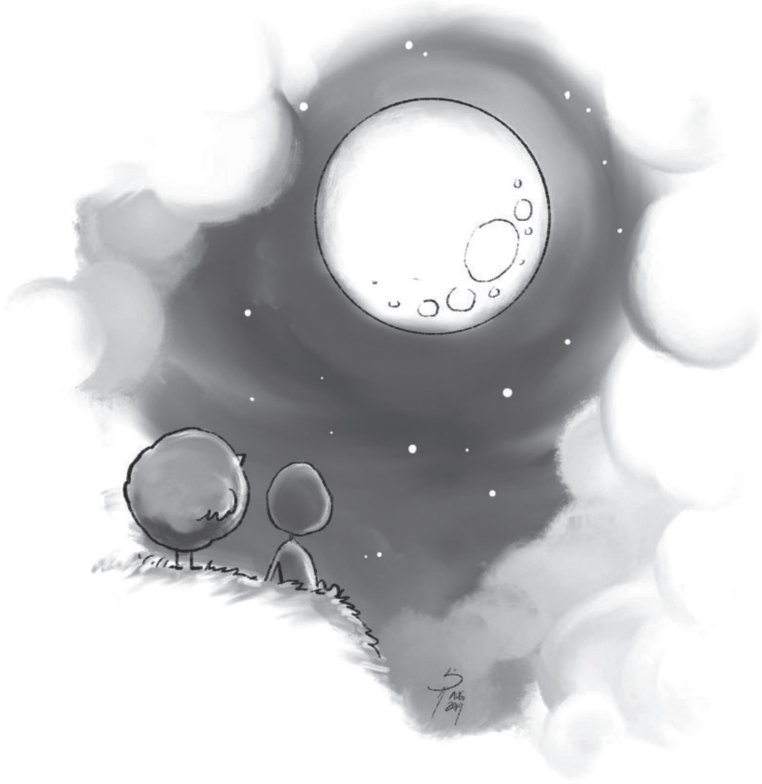
Satoshi Nakamoto – a bitcoin megalkotójának álneve.

tárca – egy applikáció vagy hardver eszköz, ami segítségével lehet bitcoint fogadni és küldeni.

teljes csomópont – olyan szoftver, ami ellenőrzi az összes tranzakciót és a blokklánc integritását.

tőkeáttételes tőzsde – olyan tőzsde, ahol lehetőség van a letéti összeg többszöröse – akár 100-szorosa – ellenében kereskedni. Így a lehetséges nyereség is, de a lehetséges veszteség is többszöröződik. (Az angol szakszó: 'leverage'.)

white paper – egy olyan szerzői, gyakran tudományos tanulmány, ami részletesen leír, meghatároz egy bizonyos témát. Ebben a formában mutatta be Satoshi Nakamoto a bitcoint és a technikai részleteit 2008 októberében.



Köszönetnyilvánítás

A szerzők köszönetüket fejezik ki az alábbi személyeknek, amiért idejükkel és tudásukkal segítették ezt a vállalkozást, ami nélkülük még nehezebb lett volna:

Leigh Cuen
Sam Corcos
Nick Foley
Irl Nathan
Jane Song Lee
June Park
Rodrigo Linares
Jan Čapek
Nick Neuman
Tomiwa Lasebikan

Az alábbi személyeknek is hálásak vagyunk, amiért támogattak a könyv írása során:

Bill Barhydt
Daniel Buchner
Cryptograffiti
Jill Carlson
Juan Gutiérrez
Han Hua
Ben Richman

Bill Tai
Mike Youssefmir
Sebastien Lhuilieri

Az alábbiak pedig informáltak és inspiráltak minket az évek során:

Nick Szabó
Andreas Antonopoulos
Jameson Lopp
Elizabeth Stark
Marek Palatinus
Pavol Rusnak
Michelle Lai

A következő szervezetek ösztönöztek minket a könyv megírására:

Blockchain Capital
BloomX
BuyCoins Africa
Casa
Human Rights Foundation
Open Money Initiative
University of Texas

Nagyon hálásak vagyunk Tim Changnak, aki megengedte, hogy a csodálatos házát használhassuk, és ami a legfontosabb, családjainknak és szeretteinknek, a sok biztatásért.

A magyar fordítás létrejöttében többen is közreműködtek (a fordítókon kívül), hálás köszönetünk nekik: balaxi (szervezés), Fazekas Csilla (borítóterv), Murányi Árpád (korrektúra), Stier Kata, Zsozsó.