

Lovász Ádám
(doktorandusz, Eötvös Loránd Tudományegyetem,
Filozófiatudományi Doktori Iskola)

Kriptoutópiák: A kriptovaluták politikai-ideológiai háttere

ÖSSZEFOGLALÓ

*A radikálisan decentralizált szerveződésű kriptovaluták sikerei a 2010-es években felkeltették a politikai szféra érdeklődését is. Jelen tanulmány keretei között azt tételezzük fel, hogy a kriptovaluta mint technológia egy eredendően politikai jellegű igényre való technopolitikai válaszkísérletként értelmezhető. A decentralizált, bármilyen központi monetáris hatóság jelenlétét nélkülöző privatizált pénzrendszer igénye megjelenik a libertárius politikai filozófiában évtizedekkel a kriptovaluták feltalálását megelőzően. Friedrich August Hayek a *Denationalisation of Money* című 1976-os tanulmányában a központi bankok szerepét háttérbeszorító, magánkibocsátású pénzformák mellett érvel. Méltán nevezhetjük a korai huszonegyedik századi kriptovaluták egyik legkorábbi elméleti előzményeként. Az 1990-es évek információs forradalma új lendületet adott a libertárius és anarchista elgondolásoknak, ekkor jelentek meg a „kriptoanarchisták.” Ezen irányzatok képviselői szerint a kibernetika, különösen robbanékony politikai lehetőséget kínál a radikális mozgalmak hívei számára. 2008-ban dolgozta ki egy Satoshi Nakamoto álnevű programozó a Bitcoin elméleti alapjait egy tanulmányban, majd ugyanebben az évben tette közzé a Bitcoin szoftver forráskódját. Ezt követően robbanásszerű fejlődésnek indultak a kriptovaluták. Fontos elem a kriptovaluták esetében a titkosított jelleg, a harmadik felek és központi hatalmi szereplők lehetőség szerinti kizárása a rendszerből a közvetlen kereskedelem megvalósítása révén. „Kriptoutópikus”-nak is jellemezhetjük a kibernetikai termelési módba mint emancipációs tényezőbe vetett anarchista ideológiai bizalmat, tanulmányunkban pedig igyekszünk felvázolni ezen szerteágazó irányzatnak egy lehetséges genealógiáját.*

Kulcsszavak: anarchizmus, kriptovaluta, libertarizmus, technopolitika, utópia

Ádám Lovász

(PhD student, Eötvös Loránd University,
Doctoral School of Philosophy)

Crypto-Utopias: The Ideological Background of Cryptocurrencies

ABSTRACT

*The success of radically decentralized cryptocurrencies in the second decade of the 21st century has increased the spotlight on the political ramifications of this major shift. In this article, we propose that cryptocurrencies as a technology compose a technopolitically inspired, essentially ideologically driven attempt to address political concerns. The idea of a completely decentralized and privatized monetary system lacking any central monetary authority was proposed by Friedrich August Hayek in his 1976 essay, *Denationalisation of Money*. This book is arguably one of the ideological inspirations for the entire crypto movement. The Information Revolution of the 1990s gave new impetus to various libertarian and anarchist strands, and it was during the early Nineties that the crypto-anarchists emerged. According to the view of these groups, information technology has the potential to radically change the social structure of society and undo any centralization of power. In 2008, programmer Satoshi Nakamoto published a white paper detailing the outlines of a new currency, and went on to release the sourcecode of Bitcoin. Since then, the popularity of cryptocurrencies has grown exponentially. In the case of cryptocurrencies, anonymity is key: trusted third parties and power centers are excluded from the system, in favour of direct peer-to-peer trading. We may in summary identify movements such as the crypto-anarchists and cypher-punks that believe in the emancipative, decentralizing potential of cybernetics as „crypto-utopians”, and hope to provide a genealogy of this heterogeneous movement.*

Keywords: anarchism, cryptocurrency, libertarianism, techno-politics, utopia

Bevezetés

A radikálisan decentralizált szerveződésű kriptovaluták sikerei a 2010-es években felkeltették azok érdeklődését is, akik valamilyen világnézeti háttérrel, politikai filozófiai alapot kívánnak találni ennek az újszerű monetáris konstrukciónak. Minden új termelési mód életre hív politikai változásokat, valamint értelmezési kísérleteket. Első látásra úgy tűnhet, mintha az alternatív monetáris rendszerek népszerűsége megteremtett volna utólag egy világnézetbeli mozgást. Azonban jelen tanulmány keretei között ennek fordítottját tételezzük fel, nevezetesen azt, hogy a kriptovaluta mint technológia egy eredendően politikai jellegű igényre való technológiai, sőt, technopolitikai válaszadási kísérletként értelmezhető. Tézisünk szerint a decentralizált, bármilyen központi monetáris hatóság jelenlétét nélkülöző, teljes mértékben privatizált pénzrendszer igénye megjelenik évtizedekkel a kriptovaluták feltalálását megelőzően a libertárius politikai filozófiában. Friedrich August Hayek a *Denationalisation of Money* című híres 1976-os tanulmányában már a központi bankok szerepét háttérbeszorító, magánkibocsátású pénzformák mellett érvel. Érvelése elsősorban utilitárius jellegű. Tézise szerint a szabadversenyen alapuló magánpénzrendszerek közül mintegy kiválogatódnának az értékálló formák, amelyek használata világszerte elterjedne, a túlságosan változékony árfolyamú valuták pedig spontán módon kiiktatódnának a gazdasági rendszer vérkeringéséből. Ebben a tekintetben méltán nevezhetjük a korai huszonegyedik századi kriptovaluták egyik legkorábbi elméleti előzményeként Hayek munkáját, dacára annak hogy saját modellje még pénzintézetekkel és nem teljes mértékben decentralizált hálózatokkal operál.

Az 1990-es évek információs forradalma új lendületet adott a libertárius és anarchista elgondolásoknak, ekkor jelentek meg a „kriptoanarchisták”. Az olyan kiáltványok, mint a *The Crypto-Anarchist Manifesto* vagy az *A Declaration of the Independence of Cyberspace* előrevetítik egy, a központi ellenőrzés és monopólium valamennyi formája alól teljes mértékben felszabaduló, laza összekapcsoltságú társadalom utópiáját. Különösen az ellenőrizhetetlen, titkosítással működő digitális fekete piacokban látnak a kriptoanarchisták egy olyan szerveződési módot, amely megkerüli és aláássa a domináns hatalmi struktúrákat. Ezen irányzatok képviselői szerint a kibernetika, kiváltképpen a titkosítás technológiája, robbanékony politikai lehetőséget kínál a tekintélyellenes mozgalmak hívei számára. Ugyanakkor, mint látni fogjuk, érveléseik már inkább az anonimitás értéke és a digitálisan szavatolt individuum szabadságjogai köré szerveződnek. 2008-ban dolgozta ki egy Satoshi Nakamoto álnévű programozó a Bitcoin elméleti alapjait egy tanulmányban, amely lényegét tekintve a kriptovaluták alapító dokumentumának tekinthető. Nakamoto ugyanebben az évben tette közzé a Bitcoin szoftver forráskódját, ezt követően pedig robbanásszerű fejlődésnek indultak a kriptovaluták. Mára sokezer kriptovaluta-rendszer működik. Fontos elem a kriptovaluták esetében a titkosított jelleg, a harmadik felek és központi hatalmi szereplők lehetőség szerinti kizárása a rendszerből. Mint látni fogjuk, Nakamoto koncepciója még radikálisabb Hayekénál, mivel még a magántulajdonú pénzintézetek szerepét is megkérdőjelezi a közvetlen (peer-to-peer) fizetési mechanizmus révén.

A titkosítás, nézetünk szerint, itt egy közös összekötő kapocsként funkcionál a kriptoanarchisták és Nakamoto vonatkozásában, amelynek okán „kriptoutópikus”-ként is jellemez-

hetjük a kibernetikai termelési módba mint emancipációs tényezőbe vetett anarchista ideológiai bizalmat, tanulmányunkban pedig igyekszünk felvázolni ezen szerteágazó irányzat egy lehetséges genealógiáját. Fontos lesz vizsgálódásunk szempontjából megtekintenünk azt, hogy miként keveredtek, hibridizálódtak egymással az ideológiai fogalmak a végtelenül nyitott virtuális térben. Amellett kívánunk érvelni, hogy eredendő és alapvető módon összekapcsolódik a kriptovaluta mint önszerveződő fizetési rendszer ötlete a késő huszadik századi libertárius és kriptanarchista irányzatokkal. Az anonimitás igénye mögött pedig egy felforgató töltettel bíró, radikális politikai törekvést találunk, amely igencsak nehezen egyeztethető össze bármilyen létező hatalmi formával.

A MONETÁRIS DECENTRALIZÁCIÓ LIBERTÁRIUS UTÓPIÁJA

A kriptovaluták, kiváltképpen a Bitcoin, számottevő médiafigyelemben részesedtek. Ismeretlen fogalomból rövid idő alatt széleskörűen elterjedt kifejezéssé vált. A figyelem növekedése nem elvonatkoztatható a kriptovaluták egyre elterjedő használatától. Egy népszerű információs oldal adatait böngészve az írás idején 2102 féle kriptovalutát találunk, melyek összértéke közelíti a 200 milliárd dollárt.¹ Ennek a piaci kapitalizációnak csaknem felét egyedül egy valuta, a Bitcoin teszi ki, amely a kriptovaluták közül a legismertebb és legsikeresebb fizetőeszköznek számít. Noha a kripto-fizetőeszközök értéke a világ összpénzforgalmának csupán egy töredékét teszi ki, a kriptovaluták, már szerkezeti sajátosságaiknál fogva is, „kihívást jelentenek a fennálló társadalmi berendezkedéssel szemben” (Karlstrøm, 2014: 24.). A kriptovaluta lényegét tekintve a decentralizált pénznemek közé sorolható. Hívei szerint aláásni látszik minden központi hatalmi intézményt, tanulmányunkban pedig amellett kívánunk érvelni, hogy az anarchista eszmeiséghez szorosan kapcsolódik már eredeténél fogva (Chohan, 2017: 1–9.). Nem létezik semmilyen azonosítható kibocsátó hatóság vagy központi bank, amely szavatolná a kriptovalutákat. Ez a decentralizált jelleg nem a véletlen műve. Továbbá, a titkosításra való utalás (crypto) is eredendően szubverzív politikai töltettel rendelkező igényként kódolódik a kriptovaluták fejlődését megelőlegező, jelen tanulmányban tárgyalásra kerülő írásokban. A kriptovaluta mint intézmény politikai ideológiai származású gazdasági konstrukció. Annak érdekében hogy megérthessük ezen intézményt, fel kell állítanunk a monetáris decentralizáció libertárius és anarchista eredetű genealógiáját.² Az első részben arra az utilitarista érvekkel dolgozó libertárius felfogásra összpontosítunk, amelyet Friedrich August von Hayek és nyomában Lawrence White fejtenek ki a monetáris decentralizációt tárgyaló munkáikban. Ezt követően áttérünk a „kriptanarchis-

¹ <https://coinmarketcap.com/all/views/all/>

² Hangsúlyozandó, hogy a libertarizmust a magunk részéről távolról sem kívánjuk azonosítani az állam maradtalan megszüntetését követelő anarchizmussal. Az sem lényegtelen, milyen jellegű libertarizmussal és anarchizmussal van dolgunk, így ezen fogalmak tartalmát is meg kell vizsgálnunk. Viszont ezzel egyetemben az is megjegyzendő, hogy a szóbanforgó diszkurzusokban a két kifejezés hajlamos nagymértékű keveredésre. A kriptovaluták lehetőségeit vizsgáló 1990-es évekbeli kriptanarchista szövegek amelyek a második részben elemzés tárgyai lesznek, egymás szinonimáiként, csaknem felváltható fogalmakként alkalmazzák a libertarizmust és anarchizmust.

ta” irányzat tárgyalására. Különösen a monetáris decentralizáció és az anononimitás összekötését tekintjük ez utóbbi irányzat fontos eszmetörténeti innovációjának. Tanulmányunk végén pedig a kriptovaluták „alapító atyjának”, a Satoshi Nakamoto álnevű, máig azonosítatlan szerzőtől származó klasszikus white papert értelmezzük, különös tekintettel arra, hogy miképpen jelennek meg a libertárius és kriptooanarchista politikai filozófiák ideológiai szempontjai a Bitcoin alapító dokumentumában.³

A monetáris decentralizáció politikai filozófiai tétjének értelmezése nem hagyhatja figyelmen kívül az első komoly elméleti munkát, amely ezen lehetőséget tárgyalja. Hayek *The Denationalisation of Money* című esszéjében egy radikális felvetéssel él: a történelem során tapasztalható valamennyi pénzromlás oka a monetáris monopóliumban mint intézményben keresendő. Az infláció felszámolásának egyetlen tartós garanciája a központi monetáris szabályozásért felelő hatóságok eltörlése volna, hiszen ezek törvényszerűen a piaci spontán folyamatoknál kevésbé hatékony módon látják el a pénzforgalom koordinációjának feladatát. Az eszmetörténeti kontextus egyáltalán nem lényegtelen, ugyanis Hayek az esszé első verzióját 1976-ban adja ki, nem sokkal a Bretton Woods-i devizaárfolyamszabályozási rendszer lebontását követően, míg az esszé harmadik, bővített kiadását az Euro bevezetését előkészítő tárgyalássorozatok kellős közepére, 1990-re időzítette. A már megkezdett pénzügyi liberalizációk folytatásaként konceptualizálja saját programját. Ahogyan Hayek fogalmaz, felmerül a kérdés, ha a nemzeti valuták átválthatósága is nagymértékben erodálja a nemzeti monetáris monopóliumot, akkor „vajon nem volna-e ugyanolyan üdvös teljesen eltörölni a pénzkibocsátás állami monopóliumát és megengedni a magánvállalkozásoknak hogy eltérő médiumokkal láthassak el a publikumot?” (Hayek, 1990: 27.). A monetáris monopólium Hayek számára eredendően politikai kérdés. Elképzelhetetlen ugyanis az a nagyfokú állami központosítás, amelyet a libertáriusok hagyományosan sérelmeznek, a pénzügyi folyamatok feletti monopóliumok híján. Mivel az állam olyan kényszerítő jogi eszközökkel rendelkezik, amelyek a magánvállalkozások számára elérhetetlenek, képes erőszakkal elfogadtatni a hatásköre alá tartozó területen belül még a legpocsékabb, legkevésbé értékálló pénznemek használatát is. Ilyen jogi kényszert alkotnak egyebek mellett a „törvényes fizetőeszközöket” definiáló és szabályozó törvények. Tautologikus módon, az a törvényes és legitim fizetőeszköz, amelyet az állam akként jelöl meg. Semmilyen legitimitással nem bír az ilyen típusú korlátozás. Hayektól nem idegen a libertarizmus klasszikus hagyományának az individuum jogaira való, kantianusnak nevezhető hivatkozás – számára is az egyén jogainak tisztelete fontos, sőt, nélkülözhetetlen mozzanata egy szabad társadalomnak –, de az egyének szabad döntései a hayekiánus koncepcióban a változatosabb társadalmi evolúció végett szükségeltetnek. Hayek számára a kulturális szelekció egysége a szokások és intézmények összességként értett *csoport* és nem az individuum.⁴ Akarva-akaratlanul becsempész tehát utilitá-

³ Itt értelemszerűen a Nakamoto által jegyzett *Bitcoin: A Peer-to-Peer Electronic Cash System* című white paperre gondolunk, amely a Bitcoin elméleti alapjait mutatja be a laikus olvasók számára, és nem magára a forráskódot tartalmazó dokumentumra.

⁴ Ennyiben valóban ellentmond Hayek a libertarizmus racionalista ága egyik legfontosabb módszertani kitételének, nevezetesen a módszertani individualizmusnak. Hayek ugyanis határozottan módszertani kollektivistá. A hayekiánus normatív libertarizmus és a kulturális szelekció elmélete közötti ellentétről két racionalista libertárius kritikáért ld. Steele, 1987: 171–195. és Hoppe, 1994: 67–93. David Miller pedig egyenesen

rius megfontolásokat gondolatmenetébe, a gazdasági következmények felől ítéli meg a pénzrendszerek működését. A pénzkibocsátás monopóliuma felruházódott a magától értetődőség látszatával, anélkül hogy rendelkezne a legitimitás látszatával. Hosszú időn át még csak el sem tudták képzelni a gazdasági írók és tudósok, Adam Smith fellépéséig bezárólag, hogy lehetséges alternatív, decentralizált pénzrendszer. Márpedig fontos látni, hogy a monetáris központosítás „alapvető módon járult hozzá az állam hatalmának általános növekedéséhez” (Hayek, 1990: 32.). A szabad társadalom melletti elköteleződés Hayek számára egyenértékű a versenyen alapuló, magánkibocsátású szabad pénz eszméjével, sőt, az előbbi szerinte elkerülhetetlenné teszi az utóbbi melletti kiállást.

Nem túlzás Hayek szerint a történelmet az infláció(k) történeteként értelmezni. Körülbelül azóta van pénzromlás, amióta az államra bízta az emberiség a pénz minőségének ellenőrzését. Az állam mindig is érdekelt abban, hogy mindennemű politikai cél teljesítése, valamint különböző érdekcsoportok kielégítése végett, visszaéljen az általa bitorolt monetáris előjogokkal. Illegitim minden hatalom, amely nem az egyének önkéntes hozzájárulásán alapul. Legyen szó még a legügyesebben szabályozott, a látszólag legnagyobb függetlenséggel bíró központi bankról, ezutóbbi mindig ki lesz téve az állam felől érkező politikai nyomásnak. Ahelyett hogy csökkentené a pénzkibocsátás monopóliuma a bizonytalanságot, Hayek nézetében az ellenkezőjéről beszélhetünk: a gazdaságon kívüli szempontok önkényes módon állandóan átfertőzik, eltorzítják a monetáris politikát, és ez a sajnálatos tendencia okolható a gazdaságot egyre kaotikusabbá és kiszámíthatatlanabbá tevő üzleti ciklusokért. Nem a hatékonyság szülte az állam monetáris monopóliumát, hanem az „önkény” (Hayek, 1990: 39.). Hayek számára a piac önszerveződése önmagát szervező rend, de ez a rend igencsak törékeny, mert a hibás beavatkozások okán átcsúszhat az irányíthatatlanság, az önszerveződő káosz állapotába is. A pénzkibocsátási monopólium kiterjesztése, esetleg nemzetközi méretűvé duzzasztása, még elfogadhatatlanabb Hayek számára, mint a meglévő nemzeti monopóliumok megtartása⁵ (Hayek, 1990: 24.). Miért törvényszerű az, hogy jobb, vagy legalábbis értékálló, legfeljebb a defláció veszélye által fenyegetett pénzt eredményezne a pénzkibocsátásra kiterjesztett szabadverseny? Hayek a pénzkibocsátás privatizációja melletti legnyomósabb érvként mindenekelőtt a hitelességet tekinti. Egy hiteltelen, szerződéseit sorozatosan megszegő magánvállalkozás reputációja gyors zuhanásnak indulna, ügyfélkörét elveszítené, ez pedig „sokkal erősebb biztosíték volna mint bármi, amit kitalálhatunk egy állami monopólium keretén belül” (Hayek, 1990: 48.). Libertáriusként, Hayek finoman szólva nem bízik az állam azon ígéreteiben, amelyek szerint önmérséklő magatartást fog tanúsítani. Az állam hajlamos az önmagára vonatkoztatott szabályok rugalmas in-

fatalizmussal vádolja Hayeket a kulturális szelekció elméletének kollektivista voltából adódóan. Eszerint az igazi libertárius nem lehetne módszertani kollektivista (Miller, 1989: 310–323.).

⁵ A pénzügytörténet kielégítően bebizonyította az Euro bevezetését illető általános szkepszist a libertárius közgazdászok részéről. Az állam monetáris inkompetenciáját és inkontinenciáját csupán még inkább felfokozza a nemzeti monetáris hatóságoknak egy bürokratikus, központi tervezésen alapuló monetáris centrummal való felváltása. Az Euronak mint fizetőeszköznek az Európai Központi Bank általi tragikusan inkompetens, a magországok adófizetői számára botránnyosan hatalmas veszteségekbe kerülő, minden áron való, az összes közgazdasági realitással szembeni fenntartása komoly tanulság az erőltetett központosítás eleve kudarcra ítélt voltát illetően. Hayek jóslata, mely szerint törvényszerűen rosszul lesz kezelve az Euro, teljes mértékben bevált.

terpretációjára, ha egyáltalán hajlandó még formailag is korlátozni önmaga működését. Szemben a monopóliummal, az egymással párhuzamosan használható, egymással versengő magánpénzek sokaságait vizionálja Hayek, amelyek megvalósítják a kölcsönös hitelesítést. Bevallottan kevés történeti esetet sorol fel, amelyek ténylegesen megvalósították volna a fizetőeszközök párhuzamosságát (Hayek, 1990: 43–44.). Ennyiben a hayekiánus pénzprivatizációt joggal tekinthetjük egyfajta utópizmusnak. A valóságban általánosan elterjedt az állam monopóliuma a pénzkibocsátás felett. A huszadik század nem ismert ilyen példát, olyan teljeskörűnek látszott az államhatalom. Mint látni fogjuk, mégsem egészen előzmények nélküli azonban a pénzkibocsátási monopóliumot nélkülöző pénzrendszer.

Technikai részletessége dacára, Hayek esszében végigvonul a politikai filozófiai tartalom. Egyáltalán nem ördögtől való gondolat az itt felvázolt libertárius perspektívában az állami pénz teljes kiiktatása a pénzforgalomból, ez sokkal inkább előzetes lépés az állam hatásköreinek átfogó visszafogásában, visszanyesésében. A verseny a központi hatalom minden formájával szembenálló szubverzív erőként tételeződik a libertárius keretben. Alapvető követelmény a fogyasztók részéről az értékállóság mellett a kiszámíthatóság is. Mivel az állam nem magánvállalkozás, a profitorientáltabb pénzügyi szolgáltatók rövid idő alatt feltehetően kiszorítanak az állam által kibocsátott fizetőeszközöket. Az állami pénz így akár el is tűnhetne, sőt, ezen fejlemény Hayek interpretációja alapján kifejezetten üdvös volna: „Az új fizetőeszközök megjelenése és egyre fokozódó használatuk természetesen csökkentené a létező nemzeti valuták iránti keresletet és mennyiségük radikális csökkentése híján, ezek értéke csökkenésnek indulna. Ezen a folyamaton keresztül a megbízhatatlan valuták egy idő múlva mind eltűnnének. Egyetlen módon lenne elkerülhető az állami pénz szerepének összezsugorodása: ha az állam megreformálná a pénzét és a kibocsátást olyan elvek mentén szervezné át, amelyeket a magánkibocsátók követnének. Az utóbbi lépés sikere nem túlságosan valószínű...” (Hayek, 1990: 53.). Érdekellentét áll fenn az államhatalom és a magánkibocsátók között, amely hosszútávon, egy valódi versenyen alapuló pénzrendszeren belül Hayek szerint kizárólag az állami pénz eltűnésével és így az állam hatásköreinek csökkenésével végződhet. Egyenesen következik egy libertárius politikai fordulat igénye a pénzkibocsátás privatizációjából, sőt, a két folyamat Hayeknél egymást feltételezi. A haszonelvűség nem zárja ki a politikai normativitást: a piaci rend előnyösebb a szervezett, központosított rendnél, jobban működik, ám mivel jobban működik (pontosabban szólva: működhét), politikai értelemben is kívánatosabb a központi monetáris hatóságnál. Az a lényeges, hogy nagyobb mennyiségű döntési lehetőséggel találkozzanak a fogyasztók a folyamat végén, mint annak kezdetén. Ehhez eleve megfelelő politikai keret is szükségeltetik, viszont Hayek számára az is evidencia, hogy a monetáris verseny olyan dinamizmust hordoz magában, amely önmagában is hozzájárulhat az állam és tágabban, minden centrális hatalmi intézmény erodálódásához. Világosan fogalmaz Hayek, amikor azt fejtegeti, hogy „az a fajta monetáris rendszer, amelyet javaslok, kizárólag egy oly mértékben korlátozott állam megléte mellett képzelhető el, amilyennel jelen pillanatban még nem rendelkezünk” (Hayek, 1990: 84.). Általános ismérve az utópikus gondolkodásnak, hogy zárójelezi az adottból való kiindulás igényét. Ugyanakkor Frederic Jameson nyomán az utópiának két formáját különböztethetjük meg: a forradalmi projektként értendő, az átfogó társadalomátalakítás igényét szimbolizáló utópia mellett található egy homályosabb és kétarcúbb utópizmus, amelyben a fennálló el-

fogadásaként értett realizmus álcázódik utópiaként, miközben valójában az autentikus utópizmus és az alternatív jövőképek tagadását képezi (Jameson, 2005: 3.). Ez utóbbinak volna megfeleltethető Jameson nézete szerint a libertárius utópia, a klasszikus liberalizmus minimális államának késő tizenkilencedik századi ideális állapotához való visszatérés követelménye. Míg Jameson számára a liberális utópia merő hazugság, a kapitalista rendszer álcája, számunkra itt az utópikus libertarizmus paradoxikusan realista volta az érdekesítőbb mozzanat. A monetáris rend megváltoztatásától a politikai rend módosítása, sőt, a társadalom egészének az átalakítása nem elvonatkoztathatók egymástól. Minden politikai átalakulásnak gazdasági alapfeltételei is vannak, de a pénzügyi infrastruktúra módosulása is érdemben képes, akár radikális mértékben, módosítani a politikai felépítményt. A pénzkibocsátás rendszerének messzemenő privatizációja és liberalizációja egy tágabb politikai reformprojekt egyik állomásának tekintendő, a szabad társadalom alapjainak lefektetésében. Ennyiben tehát Hayek egyáltalán nem csinál titkot abból, hogy az általa vizionált monetáris reform, a pénz új alapokra helyezése, távolról sem értékmentes, tisztán technikai cél. Nagyon is politikai, amennyiben szubvertál minden fennálló államhatalmat, de még a monetáris hatóságok szerepét is lefokozza. Sőt, Hayek egyenesen a monetáris politikának mint olyanak a megszüntetése, így mindennemű monetáris hatóság, megszüntetése mellett érvel⁶ (Hayek, 1990: 100–102.). Ebben az értelemben mondhatjuk azt, hogy Hayek jóval radikálisabban piacpárti az olyan neoklasszikus közgazdászokhoz képest, mint Milton Friedman, akik fenntartják az államtól ugyan formailag autonóm, de mégiscsak központilag szabályozott monetáris politika fontosságát. (A Hayek és Friedman közötti számottevő különbségeket illetően ld. Garrison, 2014: 1–11.). Az értékálló pénz olyan politikai töltetű igény, amely még a demokrácia megszokott keretrendszerén is túlmutat.

A pénzforgalom depolitizációja egyáltalán nem jelent Hayeknél egyben demokratizációt is. Mint írja, „egy jó pénz, akárcsak egy jó törvény, kizárólag annyiban működhet, amennyiben a kibocsátónak nem szükséges tekintettel lennie egyes csoportok vagy egyének különleges érdekeire” (Hayek, 1990: 117.). Mit jelent ez a depolitizációs igény a monetáris decentralizációra nézve? A libertárius utópiában a pénz privatizálódik, megszűnik az állam vagy annak intézményeinek politikai játékszere lenni. Emögött az a mélyebb, és kifejezetten klasszikus liberális politikai igény húzódik meg, amely az állam szerepének a csökkentésére irányul.⁷ Mielőtt továbblépnünk, a hayekiánus javaslatnak egy sarokkövére hívnánk fel a figyelmet, nevezetesen arra, hogy saját rendszere a valuták átfogó privatizációjára vonatkozik. Ennyiben még radikálisabb az úgynevezett „szabad banki” (*free banking*) mozgalomnál is, amely elsősorban a 19. századi Angliában ténykedő szabadpiaci közgazdászok és politikusok szer-teágazó csoportosulásait jelöli (Hayek, 1990: 32.). Annak érdekében hogy megérthessük a

⁶ Felvethető természetesen, hogy vajon nem túloz-e Hayek az összes eddigi monetáris hatóság hatékonytalanságának feltételezésében. Elvégre ismer a világgazdaság jelenleg is stabil valutákkal bíró, központi bankok által szavatolt pénzkibocsátó országokat. Sőt, a krónikus defláció is nem egy országot jellemez jelen pillanatban, ami legalább akkora részben a saját monetáris hatóságaik érdeme, mint a gyengébb valutákat kibocsátó országok bűneinek mellékterméke (a tőkeáramlások értelemszerűen, liberalizált gazdasági szerkezetben, a kevésbé értékálló valuták felől az értékállóbb valuták felé mozognak). Itt is, mint másutt, az utópizmus igénye ambivalens módon keveredni látszik az empíriával.

⁷ Emögött nem is annyira látens demokrácia-kritikusság is felfedezhető.

két pozíció közötti elméleti és gyakorlati különbséget, érdemesnek tartjuk röviden kitérni arra a történeti példára, amelyet Lawrence White hayekiánus közgazdász és gazdaságtörténész elemez a *Free Banking in Britain* című munkájában. A szabadpiaci pozíció szerint, amelyet Hayekkel egyetértve White is erősít, a forgalomban lévő valuták értékállóbbak, amennyiben a verseny kényszereinek vannak alávetve (White, 1995: 7.). 1727 és 1844 között egy egészen különleges helyzet állt fenn: a skót bankrendszerben kezdetben kettő, majd három, majd több mint egy tucatnyi, pénzkibocsátási joggal rendelkező bank létezett. Az 1844-es törvénymódosítás idején, amely véget vetett ennek a különleges pénzügytörténeti kísérletnek, 19 darab különböző pénzkibocsátó bank létezett Skóciában (White, 1995: 30.). Ez az eset White nézete szerint kimerítően bizonyítja, hogy a pénzkibocsátás távolról sem tekinthető „természetes monopóliumnak.” Magyarul, nem magától értetődő a központi monetáris hatóság szükségessége. A szerző által vizsgált időszakban a skót bankrendszer hatékonyabban funkcionált a jóval központosítottabb angol bankrendszerénél: jóval kisebb gyakoriságúak voltak a gazdasági pánikok és bankcsődök, a skót gazdaság növekedése pedig megelőzte az angol gazdaság növekedési ütemét. Amennyiben egyáltalán előfordultak csődhullámok a skót bankrendszerben, ezek nagyrészt az angol gazdaság krónikus instabilitásából származtak, és jóval kisebb arányú tőkevesztéseket eredményeztek a befektetők számára, mint az angol központi bank monetáris politikai inkompetenciája által súlyosbított csődhullámok (White, 1995: 37.). White tézise szerint a skót „szabad bankrendszer” működése empirikus bizonyíték amellet, hogy igenis lehetséges egy akár szélsőségesen decentralizált pénzkibocsátási mechanizmus, sőt, egy ilyen típusú konstrukció akár nagyobb stabilitást is mutathat, mint egy rivális, pénzkibocsátási monopóliummal bíró központi monetáris hatósággal ellátott rendszer. Látnunk kell azonban a skót szabad banki rendszer és a hayekiánus koncepció közötti különbséget: a skót esetben egymással versenyző kibocsátókról beszélhetünk, amelyek egyetlen valuta kibocsátásában versenyeztek. Mindegyik kibocsátó intézmény az angol fontot bocsátotta ki, ellátva a kibocsátó intézmény jelével. Ebben az értelemben a skót példa nem tekinthető egy egészen monopóliummentes képződménynek. Szó sincs tehát ebben a vonatkozásban az egymással valóban versengő valuták sokaságairól. Márpedig Hayek elgondolása ezutóbbit foglalja magába. A skót szabad bankok történetük során végig erősen függő viszonyban álltak a Bank of Englanddel, mivel annak valutájától függtek.

TITKOSÍTOTT ANARCHIZMUS: A KRIPTOANARCHISTA FORDULAT ÉS A BITCOIN GENEZISE

A hayekiánus nézet értelmében az evolúció szelekciós folyamatainak kell igazgatniuk a fizetőeszközök piacát. Ez viszont a fizetőeszközökre vonatkozó mindennemű monopólium lebontását igényli. Evolúciós perspektívája ugyanakkor kollektivista módszertani alapelven nyugszik. Az egyéni döntések a komplexebb struktúra előállításához szükségeltetnek. Hayek kollektivista haszonelvűségéhez képest a következő hullámban jelentősen felértékelődnek a piaci folyamatba virtuális szubjektumként bekapcsolódó egyén jogai. Az 1990-es évek folyamán egy új igénnyel egészült ki a klasszikus libertárius monopólium-ellenesség: a titkosítással. Az információs technológiai forradalom korszakában előtérbe kerül az ano-

nimitás és a személyes adatokkal való visszaéléssel szembeni védekezés törekvése. Kialakul a késő huszadik századi modernitásban a személyes magánélet oltalmazására vonatkozó, erőteljesen individualista politikai akarat. Látnunk kell, hogy a titoktartásra vonatkozó követelések is eredendően politikai filozófiai értelemben rendelkeznek, eredendően átpolitizálódik a technológia. Az olyan személyek nyilvános fellépése mint Julian Assange vagy Edward Snowden felhívta a figyelmet arra, hogy a késő modernitásban a központi hatalom működését egy sajátos kétoldalúság jellemzi. Míg a polgároktól egyre nagyobb fokú átláthatóságot vár el az államhatalom és monopolisztikus magánhatalom, a gazdaság kifehérítésétől a terrorfenyegetettségre hivatkozó, az adatok titkosságát igencsak aláásó biztonsági törvények elfogadásáig, addig a hatalom egyre inkább igyekszik elfedni saját ténykedését. Ezen tendenciára való reakcióként értelmezi a „kiszivárogtató” (*whistle-blower*) jelenségét Giorel Curran és Morgan Gibson az Assange-ról szóló tanulmányukban. Assange számos szállal kapcsolódik az 1990-es éveknek egy, a kriptovaluták feltalálása előtt csaknem feledésbe merült irányzathoz, a „kriptoanarchizmus”-hoz (Curran–Gibson, 2013: 13.). Látnunk kell, hogy a kriptovaluta eredendően több mint pusztán pénzügytörténeti képződmény. Sokkal inkább politikai technológiának nevezhető. A kriptoanarchizmus szinoním a „cypherpunk” mozgalommal, olyannyira hogy a két irányzat egymással azonosnak tekinthető. A szemantikai egyértelműség kedvéért, jelen tanulmány keretén belül a továbbiakban „kriptoanarchizmusról” fogunk beszélni, mivel nézetünk szerint ezutóbbi fejezi ki legtalálébban ezen összetett politikai ideológia tétjét, továbbá a „kripto” előtag hermeneutikai értelemben is összekapcsolja a kriptoanarchia eszméjét a későbbi kriptovalutákkal.

Számos értelmezésbeli nehézség adódik. Az első az, hogy a szemantikai pontosság a legkevésbé sem jellemző a kriptoanarchista irányzat alapszövegeire. Egymással kibogozhatatlanul összekeverednek a kriptoanarchista diszkurzusban a libertárius és anarchista szempontok. Nem könnyű tehát politikaelméleti értelemben megközelíteni ezen áramlatot, sőt, a politikai filozófia bevett kategóriái kifejezetten alkalmatlannak tűnnek egy ilyen fokú hibriditást mutató képződmény értelmezésére. Második hermeneutikai nehézségünk a kanonikus szövegek formabontó jellegéből eredeztethető. Szemben számos egyéb politikai ideológiával, a John Gilmore, Timothy May és Eric Hughes nevei által fémjelvezhető kriptoanarchizmus nem hagyott maga után egyetlen kiadott, szerkesztett, lektorált szöveget sem. Három alapvető forrást találunk: a *Cyphernomicon* című nyilvános levelezőlistát, amelynek megalkotásában a három fenti szerző mellett számos anonim, döntőrészt informatikai háttérű felhasználó is közreműködött. Továbbá, rendelkezésünkre áll May *The Crypto-Anarchist Manifesto* című kiáltványa, valamint Hughes *A Cypherpunk's Manifesto* című írása, és John Perry Barlow *A Declaration of the Independence of Cyberspace* című kiáltványa. Figyelemre méltó, hogy egyetlen szerző sem tekintette önmagát sem filozófusnak vagy politikatudósnak. Maud Barret Bertelloni helytálló meghatározása szerint a kriptoanarchizmus kapcsán egyáltalán nem megalapozatlan egyfajta „technopolitikáról” beszélni (Bertelloni, 2017: 1.). Olyan politika ez, amely öntudatosan kíván a technológiai infrastruktúrára alapozni, saját állásfoglalásait mindig arra vonatkoztatja vissza. Az informatika mindenkori állapota determinálja a kriptoanarchista és cypherpunk politikák lehetőséghorizontját. Ezen irányzatok normatív kiindulópontja a kriptográfiai technológiák vélt szubverzív politikai töltetének a lehetőség szerinti legmesszebbmenő kiaknázása. A *Cyphernomicon*ban például a következőt

olvassuk ezzel kapcsolatban: „az erős kriptográfia bizonyos formái az államhatalom csökkenését fogják előidézni, sőt, potenciálisan annak hirtelen bekövetkező összeomlását”. Jól látható, hogy az anonim szerző szerint az állam meggyengítése és felszámolása között vékony határ van. A kriptográfia vagy meggyengítheti az állam befolyását, vagy egyenesen államnélküli társadalmat is teremthet rövid idő alatt. Az anarchia ebben a dokumentumban a „tisztá libertarizmusként” tételeződik (uo.). Mivel a kriptográfiai eljárások az állam számára sokkal átláthatatlanabbá tehetik a pénzügyi tranzakciók ellenőrzését, a technológia a kriptoanarchisták szerint nagymértékben megnehezítheti, sőt, elehetetlenítheti az adóbeajtást is az állami struktúrák részéről. Kifejezetten morális tétje is van a kriptoanarchiának: ugyanennél a szövegrésznél a kriptoanarchiát a szerző „a morálok és szerződések erodálásának megkerüléseként” is jellemzi. A kriptoanarchista ideológiában a technológia deleuziánus értelemben vett „szökésvonalként” tételeződik, egy olyan médiumként amelyen keresztül ágensek megszökhetnek bármilyen központi hatalmi intézmény ellenőrzése elől.⁸

Jelen vizsgálódásunk szempontjából a kriptoanarchista utópia pénzügyi vonatkozásai a legérdekfeszítőbbek. Míg Hayek libertárius víziójában továbbra is fenntartja, persze erőteljesen decentralizált formában, a bank mint közvetítő intézmény igényét, addig a kriptoanarchisták még radikálisabb típusú decentralizációban gondolkodnak. A döntőrészt 1992 és 1994 között íródott *Cyphernomicon*ban rendszeresen szóba kerülnek konkrét, praktikus problémák. Aligha meglepő módon, a monetáris rendszer radikális átalakításának igénye is megfogalmazódik. Az „erős kripto” (*strong crypto*) potenciálisan valamennyi állami funkció ellehetetlenülését eredményezheti. Nem riadnak vissza a kriptoanarchisták akár a társadalmi igazságosság vagy a társadalmi szolidaritás igényének a zárójelzésétől sem; a kibertérben felszabaduló ismeretlen ágensek megengedhetik maguknak a közösségből való kilépést. Mint olvasható a *Cyphernomicon* soraiban, „a libertáriusok és anarchokapitalisták számára különösen vonzó lehet a víziónk, ami a konvencionális liberálisok számára kényelmetlen konzekvenciákat is magába foglal (amikor ráébrednek, hogy az erős kripto olyan dolgokat is lehetővé tehet, amelyek ellentétesek a társadalmi jólét eszméjével, vagy az antidiszkriminációs törvényekkel...)” (uo.) Jól látható, hogy a libertarizmus itt az államellenességgel és erősen piacorientált anarchokapitalizmussal szinoním fogalomként van kezelve. Jó kérdés, mennyire kulturálisan specifikus a közösségről leválasztott anonim individuum eszméje, azaz, van-e realitása egy ilyen vízióknak az igencsak speciális angolszász szociokulturális környezetben kívül. Titkosított, mondhatni numenális szubjektivitás a kriptoszubjektum. Timothy May 1988-as kiáltványa egyértelművé teszi, hogy a teljes anarchia, az összes központosító jellegű intézmény alól való felszabadulás eszményi célja szorosan összefügg az anonimitással. „A számítógépes technológia – írja May – annak küszöbén áll hogy az egyének és csoportok számára lehetővé tegye az egymással való teljesen anonim interakciókat.” Az eszményi kantiánus szubjektum mentes minden külső meghatározottságtól, ebben az érte-

⁸ Az 1990-es évek technokultúrájának és kiberkultúrájának tágabb értelemben is jellemzője volt az ellenőrzés alól megszökő technológia toposza. Ez, a korszak számos elméleti tárgyú szövegében visszatérő mozzanat. Ennek a technológiát és kibernetikát középpontba állító, a radikális decentralizációt hangsúlyozó gondolkodói tendenciának egyik legrepresentatívabb képviselője volt a Cybernetic Culture Research Unit. Egy, a CCRU tevékenységét feldolgozó magyar nyelvű bevezetőért ld. Horváth, 2018: 229–309.

lemben mondható transzcendentálisnak. Semmilyen külső teleológiát nem követ az eszményi kantiánus; az egyetlen követendő teleológia az, amelyet önmaga számára jelöl ki az ágens. Ez a hatalom lefejezését vonja maga után. „Az anarchia vezető (fej) nélküliséget jelent” – szól a *Cyphernomicon* gazdag metaforikussággal bíró definíciója. Mint minden utópia, a kriptoa-narchizmus számottevő gazdasági változásokat is kilátásba helyez. A *Cyphernomicon* szerzőinek teljes anonimitáson alapuló víziójában a pénzügyi tranzakciók lekövethetetlenek. Emiatt a fizetőeszközök anonimitására is szükség van. Kizárólag az „anonim pénz” fogadható el a kriptoa-narchista utópia számára; olyan fizetőeszköz amely a fennálló hatalmi érdekek befolyása alól mentes (uo.). Az autentikusan „kripto”-valuta a kriptoa-narchisták nézete alapján lehetetlenné kell tegye a nyomkövetés minden formáját. Egy 1994-es bejegyzésben például azt olvassuk, hogy a kriptovalutákban kifejezett hitelkártyák „lehetővé tennék a felhasználók számára [...] a tranzakciókat, anélkül hogy bármilyen közvetítőt igénybe kelljen venniük” (uo.). Hughes kiáltványa is explicit formában megfogalmazza ezt a radikális individualista pozíciót, az összes közvetítő intézmény vagy harmadik fél alól való emancipáció igényét, amikor a következőt írja: „mivel magánéletre vágyunk, lehetővé kell tennünk, hogy egy tranzakcióban résztvevő mindkét fél kizárólag olyan tudással rendelkezzen, amely a tranzakció megvalósításához szükségeltetik” (Hughes, 1993).

Látható tehát, hogy az anonimitás elválaszthatatlan a kriptoa-narchizmus tágabb ideológiai kontextusától. A kriptoa-narchizmus középpontjában a minden közösségi és társadalmi kötődés alól felszabaduló, ugyanakkor kibernetikailag erőteljesen integrált internethasználó szubjektum áll. Kritikai művelet volna a kriptoa-narchia a szó kantiánus értelmében: a hatalom metafizikájának felszámolására törekvő politikai mozgás. A kriptovaluta immanens kritikát képez minden hatalmi központtal szemben, miközben a létező monetáris rendszeren belül jött létre. Az anonimitás a kriptoa-narchisták nézete szerint eredendően szembenáll a hierarchikus szerveződésekkel, szinte magától értetődő módon összekapcsolódik a decentralizációval (Bertelloni, 2017: 3.). Lehetővé teszi, hogy az ágensek alulról szerveződő módon megvalósíthassanak saját játszmákat, taktikákat, manővereket. A kriptoa-narchisták által képviselt pozíció, túl annak erősen individualista hangszerelésén, igencsak techno-determinista előfeltevéseken is alapul. May egyenesen úgy fogalmaz, hogy a kriptográfiai technológiák pontosan ugyanolyan radikális társadalmi változásokat és politikai decentralizációt eredményezhetnek, mint a könyvnyomtatás feltalálása a késő középkorban: „miképpen a nyomtatás technológiája módosította és aláásta a középkori céhek, valamint a társadalom egészének hatalmi struktúráit, úgy a kriptológiai módszerek elterjedése is alapvetően módosítani fogja a nagyvállalatok és az államok befolyását a gazdasági tranzakciók terén” (May, 1988). Ez feltételezi a történelem szinte egyirányú technológiai meghatározottságát. Minél fejlettebb a technológia, annál nagyobb tere nyílik az anonim egyén szabadságának, vélik a kriptoa-narchisták. Henrik Karlstrøm a későbbi kriptovaluták ideológiai gyökereit a kriptoa-narchizmusban véli azonosítani (Karlstrøm, 2014: 29–30.). Valóban elmondható, hogy egyértelmű kapcsolatot láthatunk a Bitcoin olyan úttörői között, mint Nick Szabo, Wei Dai, és a kriptoa-narchisták között, hiszen szövegeikben megtalálhatóak a kriptoa-narchista szerzőkre való hivatkozások, reflexiók. Sőt, tanulmányunk befejező részében szövegszerűen is kimutatható viszonyt tárunk fel a Bitcoin és a kriptoa-narchista pozíció között. Látnunk kell, hogy a Bitcoin egy hosszabb távú ideológiai mozgás végterméke, azaz, részünkről nem jo-

gosulatlan igény a kriptovalutát egy kifejezetten anarchista technopolitikai ideológiával rezonáló technológiai innovációként olvasni. A Bitcoin önmagában távolról sem tekinthető újdonságnak. Nick Szabo, aki kifejezetten rokonszenvezik a kriptanarchizmussal, saját állítása alapján 1998-ban már kidolgozott egy decentralizált online valutát, Bit Gold névvel. Erről a megvalósíthatatlan ötletéről egy 2005-ös blogbejegyzésben számol be az informatikus (Szabo, 2005). Ugyanebben az évben hozta nyilvánosságra egy hasonló jellegű kriptovaluta ötletét Wei Dai kriptográfus B-Money címszóval, azonban ez utóbbi is csupán megvalósíthatatlan tervezet maradt. A B-Money tervezetét bemutató írásának első soraiban utal Wei Dai a kriptanarchista politikára, sőt, motivációját az anarchista utópia elősegítésében jelöli meg: „Tim May kriptanarchiája számomra roppant érdekes. Az »anarchizmussal« hagyományosan összefüggésbe hozható egyéb közösségekkel szemben, a kriptanarchiában az állam nemcsak átmenetileg kerül megsemmisítésre, hanem egyszer és mindenkorra betiltásra kerül és szükségtelenné válik.” (Dai, 1998). Az aranyárban mérhető bitek látomása, az anyagi motivációkon túlmenően, morálisan is kielégítő. Hívei számára a kriptovaluta erkölcsi magasztosulást is implikál, a hatalommal szembeni lázadás disszidens formájaként.

A kriptovaluta végső formáját 2008-ban kapta meg. Ebben az évben, amely egyébként – az időzítés szempontjából aligha véletlen módon, egy súlyos nemzetközi pénzügyi válság ki-robbanásának éve – jeleníti meg világhírűvé vált *Bitcoin: A Peer-to-Peer Electronic Cash System* című tanulmányát a máig azonosíthatatlanul maradt Satoshi Nakamoto.⁹ Tanulmányunk hátralévő hányadában Nakamoto írásának értelmezésére vállalkoznánk, különösen tekintettel az anonimitás és decentralizáció kettősségére. Nakamoto kiindulópontja a teljes anonimitás. „Az elektronikus pénznek egy tisztán peer-to-peer verziója lehetővé tenné az online fizetés közvetlen átutalását egyik féltől a másikhoz, bármilyen közvetítő pénzügyi intézmény nélkül” (Nakamoto, 2008: 1.). Már Nakamoto korszakalkotó tanulmányának kezdőmondatában is visszaköszön a közvetítő hatalmi intézmények kizárására vonatkozó igény, amely jól felismerhető módon kapcsolódik a *Cyphernomicon* azon kitételéhez, amely szerint a bankokon és egyéb pénzügyi intézményeken keresztül futó, ezek által uralt digitális pénzek nem azonosíthatóak azokkal az autentikusan „kripto”-pénz nemekkel, amelyeket a kriptanarchisták javasolnak (*Cyphernomicon*). A peer-to-peer modell olyan technológiai megoldást kínál, amely a tranzakciókat valóban transzcendentálissá alakítja. Nincs hely, amely felől a blockchain felülbíráható. A teljes mértékben peer-to-peer rendszer, a harmadik fél megfigyelő és hitelesítő funkciójának kiiktatásával, a Bitcoin protokoll automatikusan kivonja önmagát minden külső ellenőrizhetőség alól. Nakamoto tanulmánya konkrét technológiai megoldást is kínál a transzcendentális szubjektum sebezhetőségre, valamint a kettősköltés (*double-spending*) dilemmájára. Javaslata alapján a pénzhamisítás és lopás egyaránt minimalizálhatóak, amennyiben minden Bitcoinban kifejezett tranzakció egy publikus főkönyvben rögzítődik, az átutalást végzők személyes adatainak megőrzése mellett. A Bitcoin egy teljesen decentralizált hálózat, amelyben nincsen szükség bármilyen harmadik félre, amely szavatolja a tranzakciók legitimitását, ennyiben a hitelesítés immanens marad. Olyan fize-

⁹ Egyes pletykák szerint Satoshi Nakamoto valójában Nick Szabo, de Szabo ezt máig vehemensen tagadja. Ez is jól tükrözi a kriptovaluta és önazonosság paradoxikus viszonyát. A kripto azt ígéri számunkra, hogy megőrizhetjük egyéni jogainkat, de ez csupán a személyes identitásunk zárójelezése útján érhető el (Reiff, 2018).

tési médium, amely „nélkülöz bármely megbízott harmadik félt” (Nakamoto, 2008: 1.). A Bitcoin szóösszetétel alapján nem nehéz kikövetkeztetni, hogy ez a szó olyan „érmét” jelent, amely bitekből, adatokból áll. Teljesen immanens virtualitása szavatolja az anonimitást. Nakamoto definíciója alapján „az elektronikus érmét digitális aláírások láncolataként azonosítjuk. Minden tulajdonos átadja az érmét a következőnek [egy tranzakció lebonyolítása során] azáltal, hogy digitálisan aláírja az előző tranzakció és a következő tulajdonos publikus kulcsát tartalmazó hash-et, és ezeket hozzáadja az érme végéhez. A fizető fél leellenőrizheti az aláírásokat a tulajdonlás láncolatának ellenőrzése végett.” (Nakamoto, 2008: 2.). Anélkül hogy túlságosan elmélyednénk a Bitcoin konkrét technikai részleteiben, vagy azon empirikus kérdés megválaszolásában, hogy mennyire is bizonyult sikeresnek a tranzakciók biztonságos lebonyolításában a Nakamoto által kidolgozott biztonsági protokoll, a kriptovaluta legradikálisabb újítása a korábbi pénzrendszerekkel szemben a titkosítás mellett a kibocsátás módjában érhető tetten.

Szemben a hagyományos fizetőeszközökkel, a Bitcoint decentralizált szervereken állítják elő számítógépek, matematikai problémák megoldásával. Úgynevezett „bányászok” termelik ki az új érméket, amelyek száma felső korláttal bír. A nemesfémekhez hasonlóan, a Bitcoin érmék mennyiségileg behatároltak, ami egyfajta beépített deflációs mechanizmusként értelmezhető¹⁰ (Karlstrøm, 2014: 30.). Az első tranzakció egyben egy „blokk” létrehozását is jelenti, amely a tranzakciók láncolatát jelenti. Mivel nincsen központi monetáris hatóság, egy decentralizált hálózat résztvevőinek kell előállítaniuk az érméket, méghozzá úgy, hogy

¹⁰ Itt és most az értékállóság empirikus kérdését is kénytelenek vagyunk zárójelezni. Vizsgálódásunknak nem tárgya annak megválaszolása, mennyiben bizonyult valóságosnak az értékállóság és stabilitás ígérete. Tanulmányunk tárgya a kriptovaluta politikai-ideológiai konstrukcióként való azonosítása, továbbá azon utópista áramlatoknak a feltárása, amelyek hozzájárultak eme konstrukció létrejöveteléhez. Így vizsgálódásunk csupán 2008-ig terjed ki. Sem a kriptovaluták empirikus története, sem a mellettük vagy ellenük való érvelés nem képezi tárgyát. Mindazonáltal megjegyzendő, hogy már Hayek is számol az állami kibocsátású valuták gyorsütemű leértékelődésével. Vegyük észre az érem másik oldalát: ez a magánkiadású, deflációra hajlamos pénzformák felértékelődésével egyenlő. A Bitcoin és az egyéb, szélesebb körben alkalmazott altcoinok esetében az árfolyamok máig óriási felértékelődést mutatnak a kezdeti állapotukhoz képest, tehát a Hayek által konstatált deflációs mechanizmus empirikus értelemben működni látszik több kriptovaluta esetében. Ennek vizsgálata azonban átfogó kvantitatív kutatást igényelne, aminek a hozam és kockázat viszonyát is tematizálnia kéne. Létezik stabil fogyasztói igény ezekre a korlátozott mennyiségű pénzformákra, még ha volatilitásuk nagyságrendekkel meg is haladja a hagyományos fizetőeszközökét. Érdekesség továbbá, hogy jelen tanulmány megírását követően állami szereplők részéről is mutatkozott igény valamilyen kriptovaluta létrehozására. Arra utaló jelek tapasztalhatóak ugyanis, melyek alapján a Kínai Népköztársaság, az amerikai Facebook nagyvállalat „Libra” elnevezésű, tervezés alatt álló kriptovalutájának ösztökélésére vagy, helyesebben, provokálására, saját államilag garantált kriptovalutát tervez létrehozni. Ezt kínai állami pénzügyi intézetek bocsátanak az arra jogosult felhasználók rendelkezésére. Azonban a nagyvállalati, illetve állami szereplők által kibocsátott pénznemek „kripto” jellegét mindig is nagymértékű szkepszis övezte a kriptoközösségen belül, mivel az ilyen jellegű instrumentumok titkosítási mechanizmusai erősen kérdésesek. Ugyanakkor érdekesítő politikaelméleti kérdés, vajon miképpen módosíthatja a kriptofizetőeszközök politikai tétjét a kormányzati szereplők bekapcsolódása ezen területre. Nehezen elképzelhető, miként tartható fenn a fizetési rendszerek decentralizált jellege abban az esetben, amikor elfoglalják ezt a területet centralizált monopolisztikus hatalmi szervezetek, intézmények.

a Bitcoin beépített algoritmusának köszönhetően egyre nagyobb processzorteljesítményt igényel az érmék előállítására. „Jelen esetben – írja Nakamoto a Bitcoin előállítására kapcsán – a processzoridő és az elektromosság az a két termelési tényező, ami elköltésre kerül.” (Nakamoto, 2008: 4.) A Bitcoin materialitása szorosan függ attól a kiterjedt nemzetközi elektromos, energetikai és kibernetikai hálózattól, amelynek a működésének köszönhető az új érmék előállítása.¹¹ Egy 2018-as tanulmány szerint olyan mértékű áramfogyasztást igényelhet a Bitcoin-bányászat, hogy egy pár évtized alatt egyedül ennek az iparágak a tetemes energiafogyasztása 2 Celsius-fokkal növelheti Földünk légkörének átlaghőmérsékletét (Mora et al., 2018). Nem minden alapot nélkülözőek azok az ökológiai aggodalmak tehát, amelyek a kriptovaluták termelését övezik. Karlstrøm rámutat azon paradoxonra is, hogy a libertárius és kriptóanarchista utópia, a minden emberi eredetű hatalmi monopólium alól való felszabadulás távolról sem egyenértékű a tökéletes, eszményi szabadsággal: a kriptovaluták használói mintegy felcserélik a bankrendszerrel és a monetáris hatóságoktól való függőséget az informatikai hálózatoktól való függőségre. A harmadik fél szerepét ugyanis átveszi a számítógép, mint poszthumán ágens (Karlstrøm, 2014: 31.). A kriptovalutáknak a digitális infrastruktúrától való függőségét illetően még nem állnak rendelkezésre kielégítő logisztikai megoldások vagy koherens politikai válaszok. Mindezzel együtt, a decentralizációnak egy, minden eddigi példát messze meghaladó fokát láthatjuk érvényesülni a kriptovaluták esetében. Ténylegesen nélkülözik a kriptovalutákban végrehajtott tranzakciók az ellenőrizhetőséget. Akár a *Cyphernomicon* soraiból is származhatna Nakamoto következő mondata: „a nyilvánosság láthatja, hogy valaki küldött egy összeget valaki másnak, de nem rendelkezik bármilyen információval, amely a tranzakciót bárkihez is kötheti” (Nakamoto, 2008: 6.). Túl a Bitcoin-tanulmány technikai részletein, a magánélethez való jog ilyen mértékű afirmációja egyenesen kizár bármilyen központosított hatalmi logikát a kriptovaluta-rendszer működéséből. Nincsen helye Nakamoto politikai ideológiájában bármilyen harmadik félnek. Sőt, politikai teológiai formára hozva a problémát, azt mondhatjuk, hogy Nakamoto politikája a tiszta immanencia politikáját is jelenti. Legyen szó államról, bankról vagy Istenről, a kriptóanarchizmus, annak anarchista voltából következően, mintegy hatályon kívül helyez bármilyen transzcendens garanciát. A Bitcoin a legszigorúbb értelemben vett kritikai eljárás, amely célkeresztbe veszi a *megbízott harmadik feleket*. A hatalom transzcendenciája helyébe a tisztán immanens kereskedelem határtalan szabadsága lép, amelyet immáron egyetlen privilegizált központi szereplő sem korlátozhat. Ha a kripto világot a politikum lefejezéseként értjük, akkor a kriptovalutát a fejnélküli intelligencia technopolitikai instrumentumának kell tekintenünk. Kiszabadulni látszik a korai huszonegyedik században a pénzforgalom a politikai befolyás minden formája alól. A kriptovaluta technopolitikája ennyiben a hatalom felszámolásának szubverzív, anarchista projektjének legújabb manifesztációjaként értendő.

¹¹ Különösen túlzóként hatnak, a kriptovaluták valóságos materiális beágyazottságának ismeretében, azok az immaterialitást sugalló megfogalmazások, amelyeket Barlow és May megengednek maguknak. Így Barlow: „virtuális énjeinket a ti szuverenitásokkal szemben immunisnak valljuk. [...] Világszerte szétterítjük magunkat, annak érdekében hogy senki se gátolhassa meg gondolatainkat. Létrehozzuk az Elme civilizációját a Kibertérben. Legyen ez humánusabb és igazságosabb bárminél, amit az államok ezen a világon létrehoztak.” (Barlow, 1996). És így May: „A keletkezőfélben lévő információs piacokkal együtt, a kriptóanarchia létrehoz egy likvid piacot minden olyan anyagra vonatkozóan, amely szavakba és képekbe önthető” (May, 1988).

IRODALOM

- Barlow, John Perry (1996): *A Declaration of the Independence of Cyberspace*. <https://www.eff.org/cyberspace-independence>, utolsó letöltés: 1996. 02. 08.
- Bertelloni, Maud Barret (2017): The Cypherpunk Vision of Techno-Politics. *St. Anne's Academic Review*, 7.1: 1–8.
- Chohan, Usman W. (2017): Cryptoanarchism and Cryptocurrencies. *Notes on the 21st Century Discussion Papers Series*, 1–9.
- Curran, Giorel–Morgan Gibson (2013): WikiLeaks, anarchism and technologies of dissent. *Antipode*, 45.2: 1–21.
- Cyphernomicon*, <https://nakamotoinstitute.org/static/docs/cyphernomicon.txt>, 0666. verzió, utolsó letöltés: 1994. 09. 10.
- Dai, Wei (1998): *B-Money*. <https://nakamotoinstitute.org/b-money/>, utolsó letöltés: 1998. 11. 01.
- Garrison, Roger W. (2014): Hayek and Friedman: Head to head. In: Roger W. Garrison és Norman Barry (szerk.): *Elgar companion to Hayekian economics*. Cheltenham és Northampton, Edward Elgar Publishing, 1–11.
- Hayek, Friedrich August von (1990): *Denationalisation of Money: The Argument Refined. An Analysis of the Theory and Practice of Concurrent Currencies*. London, The Institute of Economic Affairs.
- Hoppe, Hans-Hermann. (1994): FA Hayek on government and social evolution: a critique. *The Review of Austrian Economics*, 7.1: 67–93.
- Horváth Márk (2018): *A digitalitás paroxizmusa. Spektákulum, szimulákrum, kibernetikai állapot és a virtualitás hiperkaotikus okkultúrája*. Szombathely, Savaria University Press.
- Hughes, Eric (1993): *A Cypherpunk's Manifesto*. <https://www.activism.net/cypherpunk/manifesto.html>, utolsó letöltés: 1993. 03. 09.
- Jameson, Frederic (2005): *Archaeologies of the Future. The Desire Called Utopia and Other Science Fictions*. London–New York, Verso.
- Karlstrøm, Henrik (2014): Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: Scandinavian Journal of Social Theory*, 15.1: 23–36.
- May, Timothy C. (1988): *The Crypto-Anarchist Manifesto*. <https://www.activism.net/cypherpunk/crypto-anarchy.html>
- Miller, David (1989): The fatalistic conceit. *Critical review*, 3.2: 310–323.
- Mora, Camilo et al. (2018): Bitcoin emissions alone could push global warming above 2 C. *Nature Climate Change*.
- Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>, utolsó letöltés: 2008. 10. 31.
- Reiff, Nathan (2018): Who Is Nick Szabo, and Is He Satoshi Nakamoto? <https://www.investopedia.com/news/who-nick-szabo-and-he-satoshi-nakamoto/>, 2018. 04. 12.
- Steele, David Ramsay (1987): Hayek's theory of cultural group selection. *Journal of Libertarian Studies*, 8.2: 171–195.
- Szabo, Nick (2005): Bit-Gold. <https://nakamotoinstitute.org/bit-gold/>, utolsó letöltés: 2005. 12. 09.
- White, Lawrence H. (1995): *Free Banking in Britain. Theory, Experience and Debate, 1800–1845*. London, The Institute of Economic Affairs.