

## A királynő nélküli hangyaboly — blockchain

Az egyik kriptobefektetésekkel foglalkozó honlap<sup>1</sup> adatai szerint az általa jegyzett 1901 kriptovaluta összesített kapitalizációja meghaladja a 232 milliárd dollárt<sup>2</sup>. Ugyanezen forrás szerint az elmúlt egy hétben két tucat kriptóérme veszítette el értékének legalább a felét, még közel ennyinek megduplázódott az értéke. 210 fajtának haladta meg a napi forgalma az egymillió dollárt. A blockchain technológia legnagyobb és leginkább egyedinek tekinthető előnye a decentralizáltság, a külső hierarchiától való függetlenség. Miért adják oda az emberek mégis a pénzük feletti rendelkezés jogát egy szolgáltatónak?

A brit kormány Tudományos Hivatala kiadott egy jelentést a blockchain technológia várható hatásáról. A közigazgatási alkalmazásról szóló rész azzal kezdődik, hogy „a technológiának akár akkora hatása lehet a brit társadalomra, mint a Magna Carta megalkotásának”. Japánban tesztelik a technológia használatát a közbeszerzésben Svédország lehet az első, ahol a földhivatal blockchain alapon működik. Az orosz miniszterelnök elrendelte a blockchain technológia használatának vizsgálatát a közszférában.

Az első blockchain megoldás a Bitcoin volt. Megalkotójának az volt a célja, hogy egy olyan elektronikus pénzt teremtsen, melyet virtuális pénztárcákban tartanak tulajdonosaik, mindenki csak a saját pénztárcájából költhet, de adott „pénzért” nem költhet el érvényesen kétszer. Hasonló szolgáltatást a világ valamennyi interneten szolgáltatást nyújtó pénzintézete biztosít. A bank központi rendszere csak a tulajdonosnak engedi meg, hogy a számlájához hozzáférjen és adott pénz dupla elköltésének problémája fel sem merül egy centralizált rendszerben. Volt azonban még két követelmény, melyet viszont a bankok nem tudnak teljesíteni: a rendszernek ne legyen központi felügyelete és legyen anonim! A rendszert felügyelő számítógépek (melyeket hálózati csomópontoknak vagy node-oknak hívunk) alkossanak egyenrangú hálózatot! Bárki (!) névtelenül (!) legyen képes ilyen node-ot csatlakoztatni a hálózatra, de akár több rossz szándékú node se hitelesíthessen a siker reményében szabálytalan tranzakciót. Na ehhez kellett a blokklánc. A felhasználók egyébként a bitcoin pénztárca (mely egy helyi adatbázis) segítségével férnek hozzá „pénzükhöz”, azaz nem kell egyfolytában egy vagy több node-hoz csatlakozniuk. Ma már számos más megoldás is született blokklánc alapon. Szerződéseket, megállapodásokat lehet ilyen módon tárolni, hitelesíteni. Ilyenkor a megállapodás fogalmaira vonatkozó szabály- vagy feltételrendszert, be lehet programozni, mely ilyen módon, technikai értelemben kikerülhetetlen, azaz kényszerítő erővel bír (pl. kriptovaluta átutalása következik be a megadott feltételek teljesülésének függvényében). Ilyen „okosszerződéseket” kezel pl. az Ethereum blokklánc rendszer, saját kriptovalutáját, az ether-t használva.

A blokklánc tehát olyan informatikai technikai megoldás, mely külső tekintély (felügyelet) nélkül, egyenrangú szereplők között képes, az adatok hiteleségéről és a tranzakciók sorrendjéről konszenzust létrehozni. A külső közreműködő hiánya, a közigazgatás szempontjából azt jelenti, hogy se hatósági felügyeletnek, se külső döntéshozónak (pl. kamara, bíróság) nincs helye a rendszerben. A belső konszenzus

---

<sup>1</sup> coinmarketcap.com

<sup>2</sup> 2018. augusztus 29-i adat (több, mint fele a Bitcoin-é)

függhet bizonyos, a rendszerbe programozott feltételek teljesülésétől, sőt ezektől függően akár ténylegesen végrehajthat érték átruházást is (pl. közvetlenül kriptovalutában vagy értékek (pl. gyémánt) nemzetközileg elfogadott követő-nyilvántartó rendszerében).

A blockchain tartalma lehet bármi, ami digitális formában rögzíthető: nyilatkozat, egy (IoT) mérőeszköz mérésének eredménye, digitálisan reprezentált fénykép, hang stb. vagy ezek lenyomata, természetesen minden a feltöltést végző felhasználó által elektronikusan aláírva. Lehet programkód is, melyet a tranzakciókat a következő blokkba foglaló node-ok futtatnak. Így eljutottunk az okosszerződések, sőt az ezek által megvalósított decentralizált virtuális szervezetek világába.

Látszik, hogy a technológia sok mindenre jó és hogy néhány dologra bizonyosan ez a legjobb megoldás. Az is látszik, hogy a potenciális felhasználóknak nem feltétlenül azokra az előnyökre van szükségük, melyekre az alkotók koncentráltak. Bizonyos pénzügyi műveletekben éppen a korábban kiváltani szándékolt bankok kezdik meg a technológia hasznosítását. A tokenizáción keresztül értékek globális nyilvántartására és az azokkal végzett műveletek szabályosságának kikényszerítésére használják. A technológiára épülő fizetős szolgáltatások új árufedezetet teremtenek a kriptopénznek, létrehozva a tiszta kriptogazdaságot. Az itt végzett gazdasági tevékenység után ki, kinek és mi alapján adózik? Az ilyen szolgáltatást nyújtó virtuális szervezetekbe hogyan fektessünk be, és milyen szabályok alapján?