A blockchain és annak specifikus biztonsági kérdései

SÍK ZOLTÁN NÁNDOR
Nemzeti Hírközlési és Informatikai Tanács
sikzoltan@gmail.com

Kulcsszavak: Blokk-lánc, blockchain, Bitcoin, kriptopénz, kriptográfia

A cikk bevezetés a blockchain, mint decentralizált rendszer világába, elsősorban a Bitcoinon, mint az első blockchain alapú rendszeren keresztül. Megkülönbözteti a blockchaint, azaz az értékek internetét, mint platformot a kriptopénzektől, valamint tárgyalja a különböző konszenzus-mechanizmusokat. Végül rátér egyes biztonsági kérdésekre, amelyek alapvetően a blockchain centralizált környezeti elemeinek bennfoglalt sérülékenységeiből, valamint a blockchain protokollbeli hibákból adódó sérülékenységeinek kihasználásából adódnak.

A *blockchain,* magyarul a blokklánc egy kb. tízéves technológia neve. Mivel a magyar fordítás nem terjedt még el, ezért a továbbiakban a blockchain kifejezést használjuk. De mielőtt erre rátérnénk, érdemes egy kissé távolabbról kezdeni. Egészen pontosan az elosztott főkönyvi technológiától *(Distributed Ledger Technology, 1. ábra*).

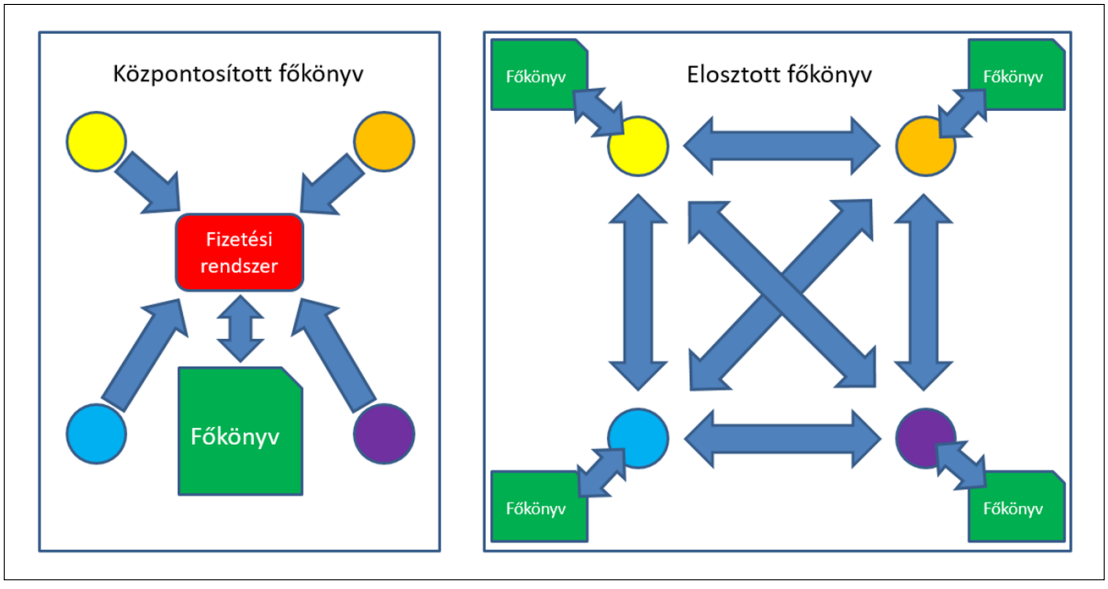
A DLT olyan decentralizált adatbázis, amelyet a különböző résztvevők kezelnek és nincs olyan központi hatóság, mely bíróként, vagy megfigyelőként közreműködne. Példa a jól ismert „torrent" protokoll (igaz, ott a torrent keresőknek kitüntetett funkciójuk van, de ez nem bírói vagy megfigyelői funkció).

A blockchain olyan infokommunikációs rendszer, amely központ nélküli (decentralizált), adatbázisaként láncba rendezett adatblokkokat kezel, működése egyenrangú felek konszenzuskényszerére, valamint kriptográfiai algoritmusok használatára alapul. A blockchain tehát a DLT-nek további feltételekkel rendelkező változataként fogható fel.

Ezek a feltételek így a következők:
– láncba rendezett adatblokkok,
– egyenrangú felek,
– konszenzuskényszer,
– kriptográfiai algoritmusok.

A blockchaint más néven az „értékek internetének" is nevezik, mivel a fenti plusz feltételek alkalmazásával egy-egy, benne tárolt adathoz egyértelműen egy tulajdonos tartozik. Az adat „tulajdonjogát" pedig a decentralizált rendszer egyes, akár egymásban nem bízó szereplőinek a blockchain szabályrendszerén (protokollján) alapuló konszenzuskényszere biztosítja. A legelső, és máig a legismertebb blockchain: a *Bitcoin-rendszer*.

Mindamellett léteznek a blockchain mellett más DLT típusú rendszerek is, csak említésként a tangle, az IPFS (Inter Planetary File System), a hashgraph, amelyekkel a továbbiakban nem foglalkozunk. Ugyanúgy nem foglalkozunk a blockchain egy olyan speciális funkciójával, hogy olyan adatok is tárolhatók benne, amelyek végrehajtható programkódot tartalmaznak és a blockchain,



1. ábra Központosított és elosztott főkönyv közötti különbség

mint rendszer végre is hajtja azokat. Ezek az ún. okos szerződések (*smart contract* – lásd például az Ethereum blockchain rendszert).

A blockchain ötlete annak a problémának a megoldásaként merült fel, hogy központi elem, azaz megbízható harmadik fél részvétele nélkül működve mégis értékeket (kvázi virtuális pénzt) lehessen közvetíteni, azaz tranzakciókat lehessen végrehajtani a blockchain felhasználói, mint szereplők között. Ez az igény abból fakadt, hogy a 2008-as bankválság után sokan úgy gondolták – nem minden alap nélkül –, hogy a mindenki által megbízhatónak hitt bankok mégsem megbízhatóak, ezért őket „ki kell kapcsolni" a rendszerből és központ nélküli, mégis funkcióiban hasonló rendszert kell létrehozni.

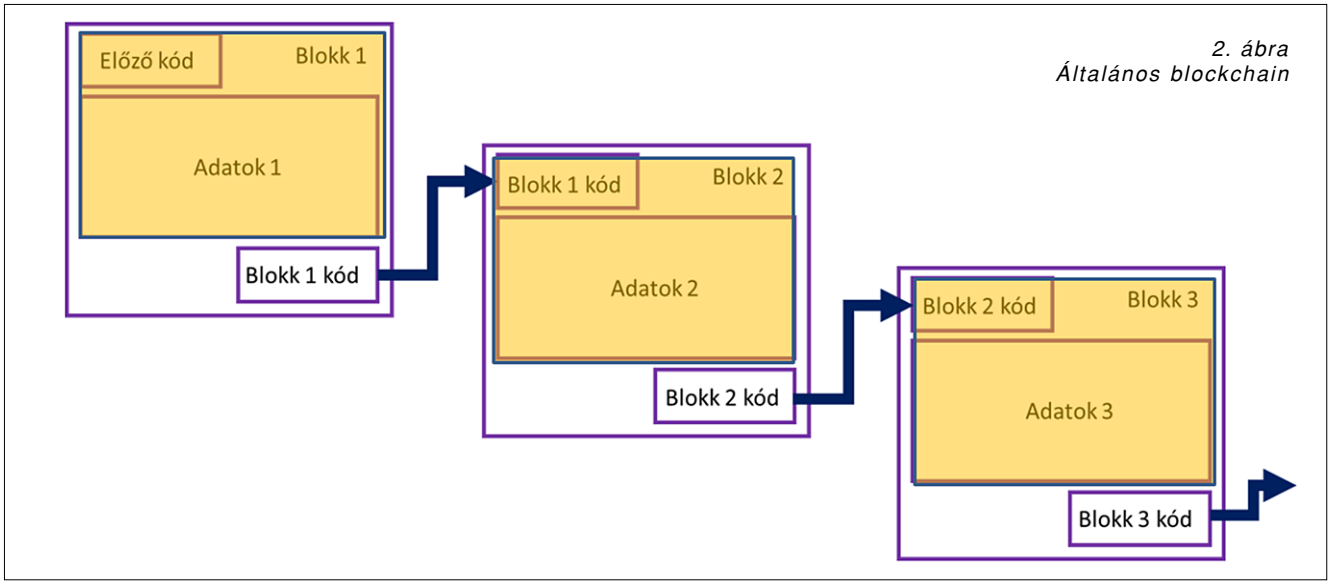
A blockchainben különböző adatokat, azaz a blockchainben tárolt elemeket ún. blokkokba foglaljuk. Mivel egy blokkba maximált mennyiségű adat tehető be – hiszen azért adatblokk –, ezért az így blokkokba foglalt, azaz „blokkosított" adatokból a legtöbb blockchain esetén egy, csak erre az adathalmazra jellemző, de a teljes befoglalt adatnál lényegesen rövidebb, az adatmennyiségtől függetlenül fix hosszúságú ellenőrző kódot, ún. *hash*-t (magyarul kivonatot, lenyomatot, zanzát) képeznek. Ezzel azonosítják az az adathalmazt és a hash tulajdonságai miatt annak változatlanságát. Ez a hash kód kerül az adott blokk ún. fejlécébe. Ezek után a következő blokk elejére ezt a kódot építik be, majd csak utána jön a következő blokkba teendő többi adat, illetve az arra a halmazra jellemző hash kód, és így tovább *(2. ábra)*.

Így végül a blokkoknak egy adott láncolata keletkezik, amelyeket ezek a hash kódok kötnek össze, gyakorlatilag megszakíthatatlanul, hiszen az előző blokk adatainak hash kódja beépül a következő blokkba. A hash kód pedig, bár egyedi módon jellemző az adott adathalmazra, ebből a kódból az adathalmaz mégsem található ki, azaz visszafelé nem működik az algoritmus.

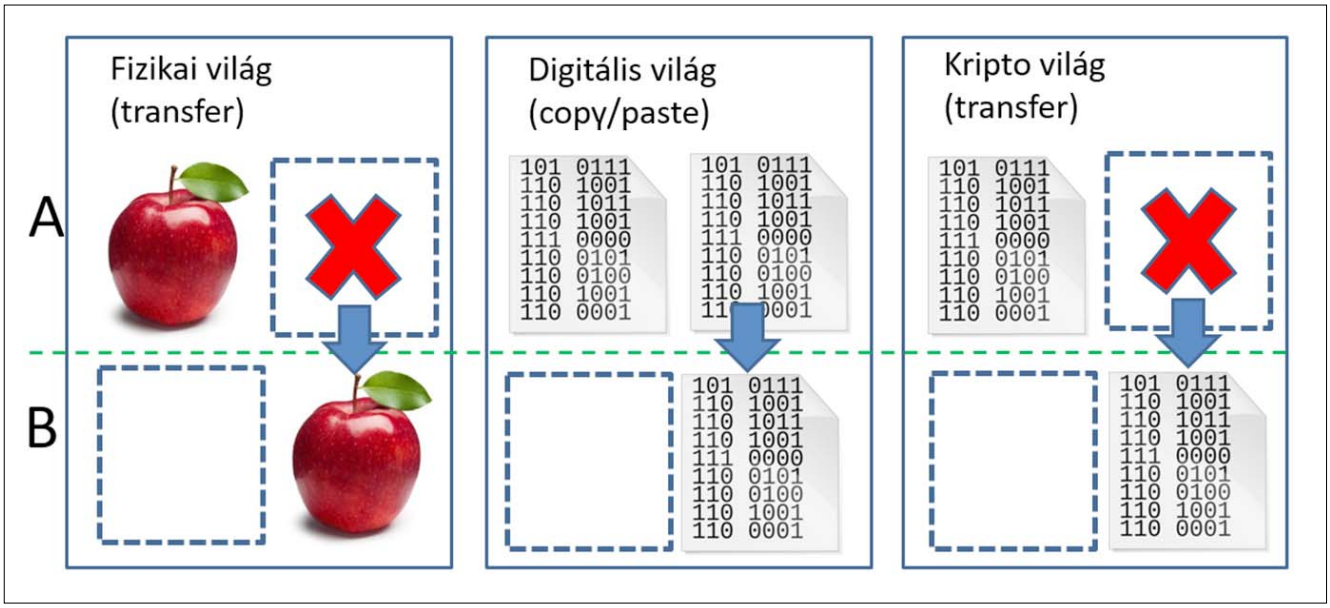
A hash kód ugyanis egy olyan, igen bonyolult algoritmus alapján számolt, megfelelően hosszú számsorból álló ellenőrző összeg, amely gyakorlatilag megjósolhatatlan módon megváltozik, amennyiben azokban az adatokban, amelyekből ez a lenyomat, a hash készült, csak egyetlen egy bitben is megváltozna. Ezért mindazon adat, ami a blockchain blokkjaiban szerepel, a gyakorlatban nem változtatható meg visszamenőleg, sem szándékosan, sem véletlenül, mivel ez esetben a blokkok nem „követik" egymást, így a blockchain megszakad és ez minden résztvevő számára nyilvánvalóvá válik. A blockchainben tehát minden adat, amely a fentiekben leírt láncolatba bekerül, valamilyen módon „le van könyvelve" és így hitelesnek tekinthető és tekintendő. A hitelességet a blockchain rendszer tehát informatikai megoldással kínálja úgy, hogy ez nem egy „egyszerű" adatbázis.

A blockchain, mint technológia a fentiek szerint biztosítja azt, hogy minden szereplő egyszersmind főkönyvelővé (blokk-lezáróvá), sőt revizorrá (validátorrá) is válik azzal, hogy mindenki ellenőrzi mindenki adatait. Ezzel lehet biztosítani, hogy a rendszerben ne kelljen központ, azaz megbízható harmadik fél. A lekönyvelt adatok, mint a felek közti adatáramlást, adatcserét (tranzakciót) bizonyító adatok (ezeket több esetben *token*eknek nevezik) kerülnek a blockchainbe, amivel el lehet kerülni, hogy valamelyik szereplő a saját tulajdonában lévő, immár kvázi pénzként funkcionáló egyedi adatot kétszer tudja felhasználni, azaz „elkölteni" *(double spending)*. Így egy-egy specifikus adatnak értéke lesz, hiszen egyszerre csak egy tulajdonosnál szerepel (és nincs „copy-paste", vagyis az információ, az adatsor nem tud duplázódni).

Végeredményben maga a blockchain szabályrendszere (a *protokoll*) biztosítja azt, hogy az internet világában is létezhessen a fizikai világban megszokott pénzhez hasonló fizetési eszköz. Mivel kriptográfiai algoritmusok használatával érik el azt, hogy a blockchainben szereplő adatok egyediek és a fenti módon láncba rendezettek legyenek, ezért ezt a világot ma már kriptovilágnak, a fenti, pénzhez hasonló adatokat *kriptopénznek* nevezik, mindezt úgy, hogy a kriptovilág kriptopénze a fizikai világban nem létezik *(3. ábra)*.



2. ábra
Általános blockchain



3. ábra A „dolgok” közvetítése fizikai, digitális és kripto-világban

A blockchain a fentiek szerint központ nélküli rendszer, amely minden szereplőt egyedileg azonosít (ezeket nevezzük *wallet*-eknek, virtuális pénztárcáknak, amelyeket nyílt kulcsú rejtjelezési technikával állítanak elő). A pénztárcák tulajdonosait azonban senki más nem tudja azonosítani, mint maga a pénztárca tulajdonosa (illetve a tranzakcióban szereplő két fél, amelyek a tranzakciókat szintén a nyílt kulcsú rejtjelezési technikán alapuló elektronikus aláírással „jegyzik”). A saját pénztárcáját minden szereplő maga állítja elő (generálja) ún. nyílt kulcsú rejtjelezési technológiával.

Mindemellett a központ nélküli működés esetén is egyetlen főkönyvet kell vezetni, amely minden szereplőnél azonos (ez maga a blockchain). Ahhoz, hogy ez megvalósuljon, a szereplők, akik általában nem is ismerik egymást, nem is bíznak egymásban *(trustless system)*, mindemellett egyenrangúak. Ezért valamilyen módon konszenzusra kell jutniuk abban, hogy mi van a főkönyvben, azaz milyen blokkokból áll a blockchain. Ennek keretén belül azt is biztosítani kell, hogy egy-egy tranzakció egyszer, és csak is egyszer legyen lekönyvelve.

Ezért a konszenzus lényege az egyetlen főkönyv kialakításában az, hogy az egyes szereplők (ún. csomópontok, *node*-ok) közül ki az, aki megmondja, hogy melyik a következő főkönyvi lap (azaz blokk). Ahhoz pedig, hogy a csalás, „összebeszélés” lehetősége a gyakorlatban ki legyen zárva, az kell, hogy véletlenszerűen alakuljon ki, hogy ki lesz a következő blokk lezárója.

A konszenzus azonban kényszerű, hiszen az a szereplő, amelyik nem tartja be, a rendszerből automatikusan kizárásra kerül, a többi szereplő zárja ki (ez a blockchain protokolljának, végső soron programkódjának része). A konszenzus kialakításának sokféle módja lehet, ezek közül ma a két legelterjedtebb a munkabizonyíték *(Proof of Work, PoW)*, illetve az érdekeltség alapon való konszenzuskényszer egyes fajtái *(Proof of Stake, PoS)*.

A PoW alkalmazása egy nagyon bonyolult matematikai feladat próbálkozások alapján történő megoldását jelenti (ezt használja a Bitcoin rendszer mellett például az Ethereum, a Litecoin, a Zcash, vagy a Monero). Ahhoz, hogy valaki előállíthassa (lezárhassa) a következő – az előző blokkokhoz a fentiekben leírt módon illeszkedő – blokkot, elsőnek kell megoldania ezt a feladatot. Ezután minden szereplő ezt a blokkot fogadja el hivatalosnak (azaz kialakult a konszenzus), egyes szereplők (a node-ok) pedig validálják is. A feladat olyan nehézségű, hogy véletlenszerűen alakul ki, ki lesz a következő blokk lezárója.

A megoldandó feladat az adott összeállítandó – tehát még készítés alatt lévő – blokkhoz, a benne lévő adatokon, valamint az előző blokk hash kódján kívül hozzá kell tenni még egy számot (ezt nevezik *nonce*-nak), melynek a blokkba való beillesztésével, valamint a blokkon ezzel a számmal együtt képzett hash kóddal a teljes készülő blokk hash kódja speciális értéket vesz fel (pl. adott számnál kisebbnek kell lennie). Ez, a fentiek szerint algoritmussal nem, csak igen sok próbálgatással megoldható feladat, amelyhez igen nagy számítási kapacitásra van szükség (ez a bányászat, a *mining*). A befektetett számítási kapacitás azonban megéri, hiszen a nyertes node (a tranzakciókba foglalt kis könyvelési díjon felül) a semmiből „teremthet”, azaz – központi bank híján – bocsáthat ki pénzt, amelyet a saját pénztárcájában írhat jóvá (ún. *coinbase* tranzakció).

A fenti megoldás azonban igen nagy áramfogyasztást jelent. Ezért kezdtek elterjedni más konszenzust kialakító megoldások, amelyek közül a leginkább használatos az érdekeltség alapú (PoS) *konszenzuskényszer*. Ennek keretén belül azok a csomópontok zárhatnak le egy adott blokkot, amelyek minden egyes körben befizetnek egy bizonyos – nem kicsi – kriptopénzben lévő összeget. Ez azonban azt is jelenti, hogy nem minden szereplő jogosult blokkot lezárni, csak azok, akiknek elég kriptopénz áll rendelkezésükre, azaz eléggé „gazdagok”. Ez tehát egy nem teljesen elosztott rendszer, hiszen nem mindenki egyenrangú, azonban sokkal kevesebb energiát

fogyaszt. Mindemellett ez is biztosítja a véletlenszerűséget, amelyre különböző, igen bonyolult algoritmusok léteznek. Ha ugyanis meg lehetne jósolni a következő blokk lezáróját, akkor fennállna a csalás, összebeszélés lehetősége. A *PoS-algoritmusok* széles, itt nem tárgyalandó skálája áll rendelkezésre (az egyszerű PoS-t használja például a Reddcoin, Navcoin blockchain, az ún. delegated PoS-t (dPoS) az EOS, Steem, Bitshares, az ún. delegated Byzantine Fault Tolerante (bBFT) rendszert pedig a NEO).

A blockchain fenti leírásából következik, hogy a benne tárolt adatok nem kizárólag tranzakciók lehetnek, hanem bármiféle más is, így többek között a fentebb jelzett okosszerződés-kódok, de bármilyen egyéb adatok is. Több cég és szervezet is foglalkozik a felhasználási területek osztályozásával, vagy magukkal az egyes blockchain-ek jellemzőivel (kriptopénzek, blockchain-platformok, „szolgáltatási" – utility tokenek, „értékpapír" – security tokenek). Egy adott blockchain működőképessége így végső soron „csak" az adott résztvevők tárolóhely-kapacitásától és az igénybe vett hálózat sávszélességétől függ.

Mindemellett léteznek olyan blockchain-hálózatok, amelyekhez nem kapcsolódhat bárki (publikus blockchain), hanem csak egy előre meghatározott, „privát", vagy „engedélyezett" *(permissioned)* szereplői kör (privát blockchain). Privát blockchaineket akár vállalatok együttműködése során, akár vállalatokon belül, valamint állami, kormányzati, egészségügyi, oktatási, szerzői jogi területeken is lehet alkalmazni. Mind a publikus, mind a privát blockchaineknek megvannak a maga előnyei és hátrányai, amelyekkel itt most részletesebben nem foglalkozunk.

A blockchain az első olyan innováció, amely nem csak az informatikára, hanem más iparágakra, sőt a társadalmi berendezkedésre is felforgató (diszruptív) hatással van. Eredetileg a bankrendszer „kikerülése" volt a cél, de például az okos szerződéseknek köszönhetően a jogra is hatással van, elosztott rendszer lévén olyan szolgáltatásokat tud biztosítani, amelyek mögött nincs egy-egy vállalat, sőt, például választási rendszer is létrehozható segítségével, így a politikai berendezkedést is érinti. Ezért a blockchain napjaink talán legjelentősebb infokommunikációs innovációja az internet megjelenése óta.

Mivel azonban, mint technológiai megoldás a fentiek szerint értékeket tárol és közvetít, ezért különösen kitett az ellene irányuló támadásoknak. A támadások mindegyike azonban valamilyen sérülékenységet használ ki, természetesen olyat, aminek kihasználása gazdaságilag, vagy valami másért megéri a kockázatot. A blockchain esetén figyelembe kell venni, hogy az új technológia olyan sérülékenységeket is hordoz, amelyekkel az infokommunikációs világ eddig még nem szembesült. Mindemellett, miután „közvetlen" anyagi értéket is képviselnek a benne tárolt adatok, valamint többnyire anonim módon történnek a tranzakciók, ezért más – nem feltétlenül infokommunikációs – területek is érintettek, illetve támadásoknak kitettek a blockchain megjelenése okán. Ez utóbbi esetre példa a zsarolóvírusok *(ransomware)* megjelenése, vagy akár egy váltságdíj kriptopénzben való megváltásának igénye.

A blockchain mindazonáltal – legalábbis az eddig leírtak szerint – bombabiztosnak tűnik, de mégsem az. Vannak ugyanis olyan sérülékenységek, amelyeket a blockchain „környezetének" centralizáltsága okoz, vagy maga a blockchain válik valamilyen módon centralizálttá, holott pont ennek az elkerülésére jött létre.

Centralizált, és így nagyobb sikerrel támadhatók pl. az egyes felhasználók pénztárcái. Nem maga a kriptográfiai algoritmus, hanem a pénztárcában lévő rejtjelező kulcs (az ún. privát kulcs) védelme érdekében használt jelszavak és egyéb védelmi mechanizmusok (még a hardveresek is). Minél több kriptopénz van egy tárcában, annál inkább megéri azt valamilyen módon feltörni, igaz, ezt leginkább az infokommunikációban már hagyományos módszerekkel kísérlik meg (a brute forcetól egészen a keyloggerekig).

Ugyanúgy centralizáltak a *kriptotőzsdék* is, ahol a különböző kriptopénzekkel kereskednek, illetve a kriptopénz és hagyományos pénz (fiat) közti váltók is. Csak az utóbbi időben fejlesztettek ki szintén blockchain alapú, decentralizált kriptotőzsdéket (pl. a Waves blockchain platformon). A centralizált kriptotőzsdéken igen nagy pénzek forognak, és ahhoz, hogy ezzel a felhasználók kereskedni tudjanak, szükségképpen kriptotőzsdén is kell, hogy legyen pénztárcájuk, amelynek rejtjelező kulcsát ezért maga a kriptotőzsde tárolja. Egy kriptotőzsde feltörése tehát gazdaságilag igen kifizetődő, dollármilliók, -tízmilliók vesznek oda, igen kevéssé lenyomozható módon (szintén hála a blockchainnek). A centralizált tőzsdék szoftvermegoldásai ráadásul sokkal sérülékenyebbek, mint a blockchain-en futó okos szerződések kódjai, hiszen csak egy helyen hajtódnak végre, nincs egy közösség, amelynek számítógépei validálják a helyes programfutást. Egy-egy ilyen centralizált tőzsde hagyományos módszerekkel való feltörése ily módon is kifizetődő.

Ugyanígy PoW esetén az ún. *bányásztársaságok* is sérülékenyek. Ezek azok a – szintén centralizált szoftvert használó – vállalkozások, amelyek az egyes kisebb kapacitással rendelkező (pl. otthoni gépeket használó) bányászok számítástechnikai kapacitását összegyűjtve, sokkal nagyobb eséllyel indulnak a fentiekben már említett speciális szám *(nonce)* megtalálásáért, így a sikeres blokk lezárásáért és az érte járó nem kevés jutalék begyűjtéséért.

Ezek a bányásztársaságok, bár nem tárolnak közvetlen pénztárca-kódokat, a begyűjtött jutalékot elosztják egymás között a megadott algoritmus alapján. Ezért náluk, ha ideiglenesen is, de igen nagy kriptopénzben kifejezett összegek vannak tárolva, így ezek feltörése is kifizetődő. Továbbá az egyes kisebb bányászok által futtatott kódot is feltörik (egy-egy gépen az a kód is csak egy példányban, tehát centralizáltan működik), és az általa termelt kriptopénzt mintegy „átirányítják" más pénztárcára. De ugyanígy bányászatra is tudják fogni azokat a számítógépeket – természetesen a tulajdonos tudta

nélkül –, amelyek eredetileg más feladatot végeznek és semmi közük a kriptopénz bányászathoz (az ilyen támadások neve a *cryptojacking*).

Ezt kisebb gépeknél vírus telepítésével el lehet érni, nagyobb kapacitású gépeknél pedig akár fizikai hozzáféréssel is lehetséges bányászszoftvert telepíteni. Bár ez utóbbi gyorsan kiderül, ha egy szuperszámítógép az egyik pillanatról a másikra éjjel-nappal teljes kapacitással kezd dolgozni, az ezzel járó villanyáram fogyasztással együtt (2017-ben el is fogtak négy orosz számítógépes szakembert, akik egy ilyen gépet bányászatra kezdtek használni). A teljesség igénye nélkül még megemlíthető az a példa is, amikor az egyetemi kollégisták a nyári szünet idejére „véletlenül” bekapcsolva hagynak egy bányászgépet az ágyuk alatt, természetesen a kollégium villanyszámlájának terhére.

Szintén a PoW-rendszert használó blockchain-ekhez tartozik még több féle támadás (attack) is, amelyek közül ma már több helyen is felbukkant az ún. *51%-attack*. Ez a gyakorlatban azt jelenti, hogy az adott kriptopénz bányászatához szükséges számítástechnikai kapacitás egy kézbe kerül, irányítás alá vonva így magát a blockchain-protokollt. Hiszen így az tudja megmondani a „szabályokat”, aki többségben van, így a kisebbséget tudja kizárni (ez igen hasonló a parlamenti demokráciák egyszerű többséget igénylő szavazati rendszeréhez). Az 51% összegyűjtése mindemellett nem is mindig derül ki azonnal (legutóbb az Ethereumból kivált Ethereum Classic rendszer esett ennek áldozatául, lehetővé téve az eredetileg elkerülendő dupla költést). Az így összeállt többség mögött ugyanis nem kell ugyanannak a pénztárcának állnia (ahová a jutalékot begyűjtik), hiszen az nem ellenőrizhető, hogy egy-egy pénztárcának fizikailag ki a tulajdonosa. Az ilyen, többszöröződésen alapuló támadást nevezik *Sybill-attack*nak, amely nevét egy Sybill nevű betegről kapta, akinek állítólag többszörös személyisége (Multiple Personality Disorder, MPD) volt.

A PoS-rendszereknél azonban az 51%-attack nem működik, hiszen ott előre kiválasztott, és nagy összegeket kockáztató, ezért mindenki által legalább pénztárca szinten ismert szereplők közt kell konszenzusra jutni. A konszenzus a legtöbb esetben a kétharmad (66,66...%), hasonlóan a parlamenti demokráciák minősített többséget igénylő szavazásaihoz. Itt leginkább az *összebeszélés* esete áll fenn, ami legutóbb az EOS blockchain-rendszerben fordult elő, itt a megkövetelt 26 kiválasztottból 16 beszélt össze, biztosítva ezzel, hogy nagy többségben közülük kerüljön ki a sikeres blokklezáró (megjegyzendő, hogy a PoW-rendszertől eltérően itt nem bányászok *(miner)*, hanem ötvözők és kovácsok *(minter,* illetve *forger)* a blokklezárást végzők nevei).

A centralizált területeket tekintve igen fontos szólni még az adott blockchain-rendszer kitalálóiról, fejlesztőiről. Ők egy adott szűk kört képviselnek, akik végül is a protokollt lefektetik, amely alapján az általuk kitalált blockchain-rendszer működik. Bár mindenki egyenlő, ők itt az „egyenlőbbeket” képviselik, hiszen a blockchain továbbfejlesztéseinél is ők vannak előnyben, mivel ők látják át a rendszer- és a programkódokat. Például a Bitcoin-rendszert kitaláló, azonban ilyen néven nem létező Satoshi Nakamoto személy volt a kitalálója a protokollnak és a köré gyűlt fejlesztők értettek hozzá annyira, hogy akár továbbfejlesztéseket is tudjanak javasolni *(Bitcoin Improvement Proposal, BIP)*, illetve a javaslatokat elfogadni és beépíteni a protokollba (végül is bárki javasolhat továbbfejlesztést, de beláthatóan szűk az a kör, akinek erre esélye van). Ezen még az sem segít, hogy a blockchain-rendszerek protokollja és megvalósítási programkódjai nyílt forráskódúak (pl. a Github-on elérhetők). Ez a megközelítés egyébként minden blockchain-rendszerre igaz (pl. az Ethereumnál az Ethereum Improvement Proposal, EIP révén). A fentiekben említett EOS-rendszernél is a rendszer kitalálói egyeztek meg abban, hogy 26 partner kell (és abból kell kétharmadnak egyezségre jutnia).

Az „egyenlőbbek” sem értenek azonban mindig egyet. Ha mondjuk jelentős számú fejlesztő, illetve számítási kapacitást birtokló node például két összemérhető nagyságrendű táborra oszlik, akkor ún. elágazás *(fork)* alakul ki, és az adott blokkig egy blockchain egy idő után két (bár közös gyökerű) blockchainre oszlik. Így alakult ki a Bitcoin mellett 2017 augusztus elején a *Bitcoin Cash,* valamint 2014-ben az Ethereum rendszerből kivált *Ethereum Classic*. Ezek a rendszerek így külön kriptopénztípust képviselnek, illetve keltenek életre (amelyek tőzsdei árfolyama is különbözik attól, amiből forkoltak).

Az ilyen forkok viszont újabb sérülékenységi pontokat is jelenthetnek, hiszen a fork egyik ágán más a protokoll, mint a másikon és az új ágon lévő protokoll nem biztos, hogy olyan kiforrottan, megbízhatóan működik, mint amelynek működőképességét az idő igazolta (más kérdés, hogy a fenti két esetben pont azért váltak ki, mivel az eredeti protokoll nem működött az idő közben, a tapasztalatok alapján kialakult új kívánalmak szerint).

Megjegyzendő, hogy blockchain-protokoll megvalósítási hiba nem fordulhat elő, hiszen a helyes kódot futtató többség a helytelen kódot futtatót azonnal kizárja (kivéve a már fent említett 51%-attack-ot, de a protokollmódosítást akkor is csak sikeres attack után lehet bevezetni).

Azonban, ha már a forkoknál tartunk, egy jelentős sérülékenységi ponthoz érkeztünk, ezek pedig a protokollhibák. Azok az esetek, amelyekre nem gondoltak, vagy előfordulásukat igen elenyészőnek tartották, de az idők folyamán a fenyegetettség jelentősen megnőtt. Satoshi Nakamoto nem gondolta volna, hogy a Bitcoin-rendszer tranzakciószáma egyszer olyan mértékű lesz, hogy az 1 MB-ban megállapított blokkméret, valamint a 10 percben megállapított *blokkidő* (az egymást követő blokkok sikeres bányászatához számított és a feladat bonyolultságát megfelelően ehhez állító időintervallum) egyszer kevésnek bizonyul. Ezt a skálázhatósági gondot akarta kiküszöbölni sok javaslat (BIP), amelyek közül az eddig egyetlen, ténylegesen sikeresnek bizonyuló a Bitcoin Cash lett.

Ugyanígy nem gondolták volna, hogy a blokkba való bekerülésre váró tranzakciókat még módosítani lehet *(transaction malleability* – magyarul tranzakció képlékenység), amely hibának a kihasználása 2014-ben a bitcoin kereskedés 70%-át lebonyolító Mt.Gox kriptotőzsde órák, illetve percek alatt való összeomlásához, és így hihetetlen mennyiségű kriptopénz odaveszéséhez vezetett. Mivel a blockchainekben, természetüknél fogva nincs storno tranzakció, ezért a veszteséget nem lehetett visszahozni, hiszen a pénztárcák mögött anonimek a tényleges résztvevők, akiket szép szóval igen nehéz rávenni arra, hogy adják vissza az ellopott kriptopénzt (mert kit is szólítanánk meg egyáltalán?).

Ugyanígy, Vitalik Buterin (ő viszont létezik), az Ethereum rendszer akkor 19 éves feltalálója sem gondolta volna, hogy a rendszerébe beépített okos szerződések kódját is meg lehet írni hibásan. Egy ilyen programozási hiba az okos szerződésben (rekurzív jóváírás a terhelendő számla nullázását megelőzően) vezetett oda, hogy a 2014 május-júniusában létrehozni kívánt központ nélküli szervezet *(Decentralized Autonomous Organisation, DAO)* – amit, mivel az első volt, egyszerűen csak „The DAO" névre kereszteltek, – áldozatául esik egy ilyen programhiba szándékos kihasználásának. A The DAO esetén a részvénykibocsátásokhoz hasonlóan kriptopénzben (inkább tokenben) kifejezett pénzgyűjtést szerveztek, amihez bárki csatlakozhatott. Az ilyen tőkebevonás neve az *Initial Coin Offering* (ICO) a hagyományos részvénykibocsátáshoz (Initial Public Offering, IPO) hasonlóan, bár jelentős különbségek vannak köztük. A The DAO-hacker a fenti módon a begyűjtött pénzt kb. egyharmadát átirányította egy másik, általa birtokolt pénztárcába és ha nem figyelnek fel erre, akár az egészet is átirányíthatta volna anélkül, hogy bárki bármit tehetett volna ellene (mivel a blockchainben minden node-on ugyanaz az okos szerződés kód fut, ezért azt megváltoztatni nem lehet, ha hibás, akkor sem). Így alakult ki az Ethereum Classic fork, amikor is Vitalik Buterin egyszemélyben megmondta, hogy a könyvelés az x-edik blokkig visszafejtendő és attól kezdve érvénytelen. Akik ezt elfogadták, maradtak az Ethereum rendszerben, akik pedig abban hittek továbbra is, hogy „a protokoll szent", azt centralizált erő nem változtathatja meg, még ha maga a kitaláló is az, egy fork révén létrehozták a fentebb már többször is említett Ethereum Classic rendszert. Az Ethereum rendszerben azóta is figyelik, hogy azzal a pénztárcával, ahová a The DAO hacking-ből származó, mintegy 3,641,694 ether-t átirányították (ether az Ethereum rendszer kriptopénzének neve), nehogy valamilyen tranzakciót végezzenek.

Az eset csattanója pedig az, hogy a The DAO-hacker nyílt levelet írt a közösségnek, amelyben kéri, hogy fizessék ki neki ezt a „díjat", mivel ő részletesen tanulmányozta a kódot és sok munkája fekszik benne, valamint, ha valaki egy személyben megmondhatja, hogy mi történjen egy blockchainnel, akkor a blockchainbe, mint technológiába vetett hit és bizalom inog meg. A helyzet pedig az, hogy még igaza is volt. A The DAO-hacker egyébként 2017-ben elnyerte a blockchain-rendszerek legbefolyásosabb személyiségei közt az első helyet a kriptovilággal foglalkozó meghatározó online folyóiratok szerint (CoinTelegraph, CoinDesk).

A szerzőről

SÍK ZOLTÁN NÁNDOR jogi szakokleveles villamosmérnök, MBA, politikai szakértő. Tőzsdei szakvizsgával és értékpapír-kereskedői szakvizsgával rendelkezik. Villamosmérnöki diplomájának 1986-os megszerzését követően a versenyszférában látott el különböző vezetői pozíciókat. 1999-től a Hírközlési Főfelügyelet (ma Nemzeti Média és Hírközlési Hatóság) informatikai igazgatója volt, 2000–2002-ig informatikai kormánybiztos. 2000–2003-ig a Nemzeti Hírközlési és Informatikai Tanács (NHIT) tagja, majd szakértője, 2011-től a Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ) tanácsadója, 2015–2019-ig az NHIT alelnöke. 2018-tól a Magyar Államkincstár tanácsadója. Jelenlegi kutatási témája a blockchain.