Vágujhelyi Ferenc
elnök
Nemzeti Hírközlési és Informatikai Tanács

Elektronikus választási rendszer – létezik a polgárok számára átlátható megoldás?

Bevezető

Napjainkban minden olyan feladatnál, amelyben nagy tömegű információval dolgozunk, felmerül egy elektronikus rendszer kifejlesztésének a gondolata. A választások esetén a felszínes szemlélő számára egyszerűnek tűnik a feladat: az arra jogosult megtekinti a politikai választékot, dönt, majd ennek eredményét beírja a választási szerv rendszerébe, ahol a szabályok szerint kiszámolják az eredményt. A témában nem kell túlságosan elmélyülni ahhoz, hogy az egyszerű megoldás reménye gyorsan elillanjon. Ez az írás egyrészt azt vizsgálja, hogy a választásokkal szemben támasztott gyakorlati feltételek hogyan fogalmazhatók meg egy elektronikus rendszerben, másrészt azt, hogy az elektronikus hitelesség és a kriptográfia *„közönséges"* eszközeinek használatával milyen rendszert lehet létrehozni. Lehetséges-e olyan biztonságos rendszert kialakítani, amelynek korrekt működése belátható az *„átlagos választó"* számára? Aki az online szavazási folyamat feltételeinek kielégítésére létrehozandó rejtjel-rendszerrel kapcsolatban kíván ismereteket szerezni, annak a témában megjelent számos publikáció tanulmányozását javaslom1. Ha pedig az olvasó arra kíváncsi, hogy hogyan lehet a sok egyéni döntésből egy közösségit kreálni, akkor az erre vonatkozó irodalom tanulmányozását javaslom[2].

Először fogalmazzuk meg, hogy milyen előnyöket várunk el egy elektronikus választási rendszertől?

1. Legyen a véletlen vagy a szándékos emberi hibáktól mentes a végrehajtás és a számlálás[3]!
2. Legyen meg azonnal (vegyes rendszernél gyorsabban) az eredmény!
3. Legyen könnyebb / egyszerűbb a részvétel!
4. Mindenki számára (így a jelöltek számára is) legyen ellenőrizhető minden szavazat, de
5. a szavazatok legyenek anonimek!
6. A választó számára legyen ellenőrizhető, hogy helyesen számlálták-e meg a saját (és csak a saját!) szavazatát, de
7. ha akarja se tudja bizonyítani, hogy ez a szavazat mi volt (kényszer vagy szavazatvásárlás kizárása)!

Már ezek, a követelményként megfogalmazott előnyök is vita tárgyát képezhetik. Például a 7. pont esetében implicite kimondjuk, hogy a kényszer kizárását fontosabbnak tartjuk az egyéni szavazat tartalmára vonatkozó jogorvoslat lehetőségénél. A fentiek mellett természetesen nem akarunk lemondani a hagyományos (fülkés-szavazólapos) módszer során ma meglévő garanciákról sem. Ehhez először nézzük meg, hogy a technikai garanciák szempontjából hogyan működik a hagyományos rendszer!

A papír alapú választási rendszer

A jelenlegi választási rendszert azért nevezem papír alapúnak, mert a jogkövetkezményt kiváltó információ elsődleges hordozója a papír, így hitelességének kellékeit (pl.: bélyegzőt, aláírást) is papír hordozza[4]. Mivel a választási folyamat átláthatóságát és tisztaságát informatikai szempontból vizsgáljuk, szükségünk van egy olyan definícióra, amely ezzel az eszközkészlettel kezelhető: „a választási rendszer akkor működik jól, ha a választáson az arra jogosultak*, és csak ők kinyilváníthatják véleményüket, és az eredmény a szavazólapon rögzített információ alapján kerül kiszámításra"*. Ennek a következő technikai feltételei vannak[5]:

1. az arra jogosultak valamennyien szavazhatnak (névjegyzékbe kerülnek),

[1] Pl: Helger Lipmaa (2005): *Secure Electronic Voting Protocols*

[2] (1) Mészáros József, Szakadát István (1993): *Választási eljárások, választási rendszerek*; (2) Arrow, K. J. (1951): *Social Choice and Individual Values*; (3) Török Tamás (1995): *A választások elmélete és magyarországi gyakorlata*

[3] Pl.: nem ad rossz szavazólapot, nem számol rosszul, nem rögzíti hibásan a jegyzőkönyvet.

[4] Ezért a kihirdetett eredmény kizárólag papír alapú dokumentumok (szavazólapok, jegyzőkönyvek) vizsgálatával ellenőrizhető. Ez a garancia csak kiegészíti azt, hogy az ellenérdekű jelöltek delegáltjai fizikailag is kontrolljuk alatt tarthatják a szavazás és számlálás folyamatát.

[5] A lista a téma jelen cikkben történő bemutatására, ismeretterjesztési célból készült.

2. csak az arra jogosultak szavazhatnak (mások nem kerülnek a névjegyzékbe),
3. a törvény által meghatározott választókerületre (általában lakóhelyükre) vonatkozó döntésben vehetnek csak részt,
4. a szavazóköri névjegyzékben a részvétel ellenőrzése megoldott (mindenki legfeljebb egy érvényes szavazólappal rendelkezhet, így szavazólap-fajtánként mindenkinek pontosan egy szavazata van),
5. a szavazólapok érvényesítése (pecsételése) *ellenőrzött*,
6. a gyűjtőurna kezdeti üres állapota *ellenőrzött*,
7. a szavazás végrehajtása a szavazófülkében (azaz titkosan) történik,
8. a szavazólapok urnába kerülése *ellenőrzött*,
9. urnabontás után a szavazólapok érintetlensége *ellenőrzött* az eredményt tartalmazó jegyzőkönyv aláírásáig,
10. a szavazólapok érintetlensége (remélhetően) *ellenőrzött* a jogorvoslati határidő végéig.

Az „*ellenőrzött*" szó elsősorban azt jelenti, hogy az egymással versenyben lévő jelöltek megbízottjai számára korlátozás nélküli az ellenőrzés lehetősége. Magyarul reggel belenézhetnek az üres urnába, azt egész nap szemmel tarthatják, és láthatják, hogy minden megjelenő szavazó a bemutatott okmányának megfelelő helyen ír alá (és egyáltalán aláír) a névjegyzékben. A rontott szavazólapra vonatkozó szabály alkalmazása a szemük láttára történik. Bontás után láthatják, hogy a lapokból nem vesz el és nem tesz hozzá, valamint nem ír rá senki, az eredményt maguk is megszámolhatják, vitás esetben véleményüket jegyzőkönyvezik. Azt, hogy a névjegyzékbe felvételre került-e egy arra jogosult választó, saját maga ellenőrizheti, hiba esetén jogorvoslatot kérhet. Azt, hogy a névjegyzékre felvételre került-e valaki, aki nem, vagy nem ott jogosult szavazni, a jelöltek ellenőrizhetik például úgy, hogy a korábbi választásokhoz képest megnézik, hogy van-e jelentős változás a jogosultak darabszámát illetően (összességében vagy egy adott címen). Jelentős változást okozhat például egy új lakópark felépülése, de az indokolatlannak tűnő változás utalhat visszaélésre. Belátható, hogy a teljes folyamat átláthatóságát technikai és adatvédelmi okokból nem lehet valamennyi választópolgár és a sajtó számára biztosítani az itt leírt módon. Ezért kell a feltételek szabályos teljesülésének ellenőrzését az ellenérdekű jelöltekre, illetve az általuk megbízott személyekre (a jelöltek által delegált szavazóköri tagokra) ruházni. Az is látható, hogy a fenti feltételek sértetlenségét a jelöltek, illetve megbízottjaik nem informatikai eszközökkel, hanem saját érzékszerveikkel (elsősorban a szemükkel) ellenőrzik.

A hagyományos választási folyamat mennyiben függ az informatikától?

A névjegyzék összeállítása, ellenőrzése, kinyomtatása ugyan informatikai eszközökkel támogatott folyamat, de végrehajtását nem akadályozza meg egy adott pillanatban vagy egy rövid időszakban beálló üzemszünet. A szavazás végrehajtásához és a szavazóköri szavazatszámláláshoz, annak tisztaságának és transzparenciájának ellenőrzéséhez nincs szükség informatikai támogatásra. A jegyzőkönyvet is meg lehet kézzel írni. Megjegyzendő, hogy a 8. pont betartásának ellenőrzése a gyakorlatban nem megoldott. A választó bármit bedobhat az urnába, ami egy szavazólapra vagy borítékra hasonlít. Ez teremti meg a láncszavazásnak nevezett visszaélés lehetőségét, amikor a csalásba bevont első szereplő elhozza a kitöltetlen, de lepecsételt szavazólapot, azt átadja a csalás szervezőjének, ő saját szándéka szerint kitölti, majd a következő résztvevő ezt a lapot dobja be az urnába, és elhozza saját kitöltetlen lapját. Az utolsó résztvevő ilyenkor két lapot dob be az urnába, amely nem megoldhatatlan feladat. A csalásban esetleg kényszer hatására részt vevő személy a fülkében akár érvényteleníteni is tudja a szavazólapot, vagy üres borítékot dobhat be. Megteheti azt is, hogy új szavazólapot kér arra hivatkozva, hogy az elsőt elrontotta. Ilyenkor meghiúsítja a csalást (az esetleges jövedelem megtartása mellett), bár az elrontott szavazólap miatti cserének a híre már nem feltétlenül marad titokban a csalás szervezője előtt.

A szavazókörökből az eredmény a helyi választási bizottsághoz kerül. A jelöltek megbízottjai jellemzően a jelölő szervezet (párt vagy független jelölt) helyi irodájába továbbítják sms-ben, telefonon vagy személyesen az eredményt. A gyakorlatban egy jelölt nem tud minden szavazókörbe saját tagot küldeni, aki reggel háromnegyed hattól este hétig egyszerre figyeli az urnát, a névjegyzéki aláírásokat, a hitelesítő pecsétet, a mozgóurnát, urnabontás előtt és után a tollak elrakását, miközben számol, majd a jegyzőkönyv adatainak ellenőrzése és aláírása után az adatokat még hibátlanul a megadott helyre továbbítja. Ha azonban ez a szavazókörök reprezentatív mintájában megtörténik, akkor statisztikai értelemben elfogadható megbízhatóságú következtetést lehet levonni a többi szavazókörre vonatkozóan is. A jelentős eltérés így kimutatható, annak oka általában kideríthető. A választókerületi eredmények ezután az országos választási központba kerülnek, illetve jellemzően a pártok is bekérik őket országos központjaikba. Ehhez informatikai rendszereket használnak, de a jellemzően nem nagy adatmennyiségek akár más online kommunikációs eszközön (üzenetküldő rendszereken) vagy telefonon is továbbíthatók. Így még a hivatalos előzetes végeredmény megállapítása előtt észre lehet venni a pártok saját gyűjtéséből származó és a hivatalos adatok közti eltérést. Megjegyzendő, hogy az eredményt és az átláthatóságot az sem befolyásolná, ha az ország teljes távközlési hálózata (a telefon is) működésképtelenné válna, mivel ekkor például autóval lehetne az adatokat utaztatni. Ezt a választási bizottságok és a pártok egyaránt megtehetik saját adataikkal. Az összesítő számításokat hálózatra nem kötött gépeken vagy papíron, kézzel is el lehet végezni.

Ki lehet jelenteni, hogy a magyar választási rendszerben az eredményt, és a jelöltek, jelölő szervezetek számára biztosított átláthatóságot veszélyeztető, pusztán informatikai módszerekre épülő támadás nem kivitelezhető, ha az érintett közigazgatási szervezetek és a pártok felkészültek a meglehetősen egyszerű hagyományos módszerek használatára. A műszaki problémák vagy hiányosságok az eredmény azonnali közzétételét akadályozzák, de magát az eredményt nem befolyásolják.

Az elektronikus választási rendszer

Térjünk át az elektronikus választási rendszerre! Először tisztázzuk, hogy mit értünk ez alatt a fogalom alatt! Vannak, akik a papír alapú szavazatszámláló eszközöket[6] is ide értik. Az ilyen megoldás érdemben nem változtat a hagyományos rendszeren, mivel a kézi számlálást kiváltó berendezés kivételével a teljes folyamat megfelel a hagyományosnak. A választó döntését közvetlenül elektronikus eszközben rögzítő szavazásra korlátozzuk a fogalom használatát. Ebben az esetben is két különböző elven működő rendszerről beszélhetünk. Az egyik esetben a szavazást a választások lebonyolításáért felelős szervezet által felügyelt szavazó-kioszknak[7] hívott berendezésen, a helyszínen kell végrehajtani. A módszer fenntartja a papír alapú szavazás előnyeit, sőt a láncszavazást lehetetlenné teszi. Műszakilag biztosítani kell viszont azt, hogy minden szavazásra jelentkező kapjon egy olyan szavazásra jogosító eszközt (tokent), amelynek érvényességét a kioszk felismeri, és megállapítja, hogy azzal szavazatot még nem adtak le. A token információ tartalma lehet egy véletlenszám, amelyet a választási szerv elektronikus aláírással hitelesít. Ilyen információ (adatsor) előállítására – az elektronikus aláírás tulajdonságai miatt – más nem képes. A kioszk beolvassa például egy QR kódról a tokent, az elektronikus aláírást visszafejti, majd ellenőrzi, hogy a véletlen szám szavazásra kiadottként van-e jelölve. Ha igen, lehetővé teszi a szavazást, annak értékét, azaz a választó döntését tárolja. Így a leadott szavazat és a választó között nem létesül logikai kapcsolat, a titkosság nem sérül[8]. De a választó hogyan győződhet meg arról, hogy valóban az ő döntése került-e be az adatbázisba? A szavazás értékéhez hozzá lehet rendelni egyedi azonosítót, amelyet a választó, ha akar, felír magának, vagy kérésére a kioszk kinyomtatja. Az „urnazárás" után bármelyik kioszk vagy egy online szolgáltatás segítségével bárhonnan ellenőrizheti, hogy a szavazatát valóban a kívánt jelölthöz számolták-e. Ha külső kényszertől tart, nem írja fel, vagy nem nyomtatja ki a kioszktól kapott egyedi azonosítót. A rontott szavazat megismétlésének lehetőségével – az előző tokenhez tartozó szavazat érvénytelenítése mellett – kaphat új tokent is, amellyel újra szavazhat. Ilyenkor a kényszerrel fenyegetett a kényszerítőnek át tudja adni az érvénytelenített tokenhez tartozó azonosítót, aki egy online szolgáltatáson keresztüli ellenőrzéskor megelégedéssel láthatja, hogy minden a szándéka szerint történt, miközben a második szavazás tényét a kényszerített szavazó titokban tartja. A második azonosítóval történő ellenőrzéskor az érvénytelen szavazás tényét is megerősíti a rendszer, de ezzel az információval a kényszerítő nem rendelkezik. A szavazás titkossága úgy biztosítható, ha az azonosítást követően véletlenszerűen kiadott tokent logikailag nem kötik a választó személyéhez, illetve a szavazás értékét és az ellenőrzéshez használt sorszámot logikailag nem kötik a tokenhez.

A kioszkkal végrehajtott szavazás elleni legfőbb érv az szokott lenni, hogy általában sem a választó, sem a jelöltek nem képesek annak a szoftvernek a korrektségét ellenőrizni, amely a szavazás időpontjában éppen a kioszkon fut. A fent leírt eljárás esetén azonban erre nincs is szükség, hiszen a választó képes a szavazatok adatbázisában a saját szavazatának ellenőrzésére, illetve mindenki képes minden szavazat értékét ellenőrizni a többiek anonimitásának megőrzése mellett[9].

Az online választási rendszer

Az elektronikus választási rendszerek közül az online az, amelyik a digitális írásbeliség képességével rendelkező választóktól a legkisebb erőfeszítést igényli. Ideális esetben a világon bárhonnan, akár egy mobil eszközzel is végrehajtható a szavazás, feltéve, hogy internet kapcsolat elérhető. Ez az eset azonban egy lényeges körülményben különbözik az eddig tárgyaltaktól: a választó fizikai értelemben nem jelenik meg a választási szerv hivatalos képviselői és a jelöltek megbízottjai előtt. Nem lehet tudni, hogy hol, milyen körülmények között szavaz, illetve azt, hogy ezek a körülmények alkalmasak-e arra, hogy a választó szabad akaratát kifejezze. A választó azonosítása itt praktikusan csak elektronikus módszerekre támaszkodhat. Ennek ma már mind a jogi[10], mind a műszaki feltételei adottak az új személyi igazolványt használók számára, ha rendelkeznek kártyaolvasóval.

Az online választási rendszerben az első problémát az jelenti, hogy a választót azonosítani kell, miközben a szavazatát logikailag helyreállíthatatlanul el kell választani a személyétől. Erre igen egyszerű módszert kínál a vak aláírás. A papír alapú vak aláírás lépései a következők:

1. A választó a szavazatát berakja egy belső oldalán indigóval ellátott borítékba.
2. Ezt a borítékot berakja egy normál borítékba, amelyet megcímez a hitelesítő aláíró (névjegyzéket kezelő szerv) részére. A saját azonosításához szükséges adatokat és kellékeket (például aláírás) elhelyezi ebben a külső borítékban (vagy a borítékon), majd ezt feladja.
3. Kézbesítés után a hitelesítő aláíró ellenőrzi, hogy az aláíró rendelkezik-e választójoggal. Ha igen, annak felbontása nélkül aláírja és/vagy lebélyegezi a belső, zárt borítékot, amelynek a belső oldalán lévő indigó a benne lévő szavazatra nyomja a hitelesítő jelet, majd
4. ismét borítékba helyezi az indigós borítékot, amelyet így bontatlanul visszaküld.
5. A választó a visszakapott indigós borítékból kiveszi az indigón keresztül hitelesített szavazatát, majd postán a feladó megjelölése nélkül elküldi a választási szerv részére.

A fenti példa azt szemlélteti, hogy a vak aláírással úgy hitelesíthető egy szavazat, hogy annak tartalma a hitelesítő szá-

[6] https://en.wikipedia.org/wiki/Voting_machine#Document_ballot_voting_system

[7] https://en.wikipedia.org/wiki/DRE_voting_machine

[8] A szemléltető példa megbízható működéséhez még számos feltétel előírása szükséges.

[9] Mindenki egyformán a token-szavazat párokat látja. A token érvényességét a rajta lévő elektronikus aláírás hitelesítésével ellenőrzi, a szavazat értékét pedig nyílt adatként látja.

[10] Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.)

mára ismeretlen marad, de a feladója nem. A szavazatszámláló előtt viszont a feladó marad ismeretlen, de a szavazat nem. Ő csak azt látja, hogy a szavazat olyan személytől származik, akinek választójoga van. A módszert csak szemléltető példaként mutattuk be, alkalmazása számos kérdést vethet fel, amelyet most nem tárgyalunk.

A feladat adott: a fenti analógiára építve készítsünk elektronikus rendszert! Ez azt jelenti, hogy a szavazat értékét el kell takarnunk az elől, aki azt a jelet „ráteszi", amely igazolja – miután azonosított minket és megtalált a névjegyzékben – hogy az egy választójoggal rendelkező személytől származó érvényes szavazat. Elektronikus információt rejtjelezéssel rejtünk el. Ehhez olyan, egymás inverzeként működő függvénypárt használhatunk, mint az elektronikus aláírásnál. A *c* vakító függvénnyel az *m* szavazatot egy olyan *c(m)* értékre képezzük le, amely elrejti az információ tartalmát. Ez felel meg az indigós borítékba helyezésnek. Ezt az értéket aláírjuk az elektronikus személyi igazolványunkon található privát kulccsal (ez adataink megadásának és kézzel történő aláírásának feleltethető meg), majd mindkettőt elküldjük a hitelesítőnek. Ő két dolgot ellenőriz: az aláírás érvényességét, majd a névjegyzéket (és azt, hogy még nem írt alá nekünk szavazatot). Ha mindkettő rendben van, saját titkos *„s"* aláíró leképezésével aláírja *c(m)*-et. A kapott *s(c(m))* értéket visszaküldi, és mi eltávolítjuk róla a vakítást („kibontjuk az indigós borítékot"). Ha megfelelő leképezéseket használunk – márpedig az elektronikus aláírásra használtak megfelelőek – akkor *c'(s(c(m)))* az éppen *s(m)*-et adja (ez annak felel meg, hogy látjuk a hitelesített szavazólapot), azaz a vakító függvény hatását úgy vettük le, hogy a hitelesítő által aláírt szavazatot kaptuk (azaz felbontottuk az indigós borítékot). Ezt követően az *m* szavazatot elküldjük a számlálásért felelős hatóságnak, aki egy azonosításra használható véletlenszámot rendel hozzá. Ezt a számot felírhatjuk, hogy később ellenőrizni tudjuk saját szavazatunk értékét. „Urnabontás" után a teljes adatbázis nyilvánosságra kerül, így mindenki maga is ki tudja számolni az eredményt az érvényesen hitelesített szavazatokból. Ezen kívül képes ellenőrizni, hogy a saját sorszámú szavazatát a szándékának megfelelően tárolja-e a rendszer, de ha akarja sem tudja hitelt érdemlően bizonyítani, hogy kire szavazott. Még azt a korántsem apró problémát is kezelni kell, hogy ebben a példában mindenki, aki adott módon szavaz, ugyanazt az adatot és hozzá ugyanazt az aláírást küldi be (azaz ugyanahhoz az értékű szavazathoz ugyanaz az adatsor tartozik). Ezt megteheti annyiszor amennyiszer csak akarja, azaz a rendszer így nem működik. A hiba javítása azonban egyszerű: a szavazat értékét ki kell egészíteni valamilyen egyedi véletlenszámmal, így az azonosan szavazók is különböző *m* értékeket használnak. Szavazatukat annyiszor küldhetik be, ahányszor akarják, de azt csak egyszer fogadja be a rendszer.

Ha a szavazat azonosítására használt véletlenszámot az azt generáló választási szerven kívül más nem képes előállítani, például azért, mert egy véletlen értéket és annak elektronikus aláírását tartalmazza, akkor az előtt az időpont előtt, hogy a szavazatok nyilvánosságra kerülnének, a választó kérheti az adott sorszámú szavazat érvénytelenítését, és új szavazat leadásának lehetőségét (ezt az értéket „urnabontás" előtt ugyanis csak akkor ismerheti, ha tőle származik a szavazat). Így ha valaki kényszer hatására ad le szavazatot, akkor azt akárhányszor érvényteleníthetí. Ezért a *„sikeres"* kényszernek a választásra rendelkezésre álló idő végéig fenn kell állnia (addig akadályozni kell a szavazót, hogy előző szavazatát érvénytelenítse, majd újra szavazzon). Mivel az elektronikus szavazásra általában több napon keresztül van lehetőség, így ennek kivitelezése nem egyszerű. Az ismételt szavazásra vonatkozó szabály, és az érvénytelenített azonosítójú szavazat értékének látszólag sikeres ellenőrizhetősége a szavazatvásárlás kontrollját szinte lehetetlenné teszi a *„vevő"* számára. A leleményes *„eladó"* ugyanis több konkurens *„vevővel"* is üzletet köthet a lebukás reális veszélye nélkül.

A vak aláírásra épülő eljárás helyett az online szavazás is épülhet – a kioszkoknál már említett – szavazásra jogosító elektronikus token használatára. A kioszkok esetében azonban a szavazó megjelenik a szavazókörben a választást lebonyolító szerv képviselői és a jelöltek küldöttei előtt, a token kiválasztásának véletlenszerűségét mindenki ellenőrizheti. Például a szavazó egy összekevert átlátszó dobozból húzza ki a papírra nyomtatott QR kódot. Az online szavazás esetén viszont nehéz feloldani azt a problémát, hogy a tokent kiadónak azonosítania kell a választót, de a token érvényességét ellenőrző szavazatszámlálónak nem szabad. Ehhez hinni kell az informatikai rendszer és üzemeltetőinek megbízhatóságában. A vak aláírásos példában a résztvevők között mozgó adatok önmagukban hordozzák a hitelesség kellékét, illetve bármely hozzáértő szavazó számára áttekinthetően rejtik el a szavazó személyét vagy a szavazat értékét, mikor melyikre van szükség. A szavazó informatikai rendszerének csupán az előre meghatározott szabályok szerint kell működnie. Bármilyen szoftvert használhat, amely ezeknek megfelel. Akár saját maga is írhat ilyet, vagy a számára hiteles fejlesztőét használhatja. Ez hasonlít a nyilvános blockchain rendszerek pénztárca (wallet) vagy csomóponti (node) szoftverére, amelynek tranzakcióiban a többi résztvevő csak a protokoll betartását ellenőrzi, a benne szereplő adatokat a felhasználó elvileg akár kézzel is kiszámolhatja. Ezzel el is jutottunk ahhoz a kérdéshez, hogy a nyilvános blockchain rendszerek esetleg alkalmasak-e a választások lebonyolítására.

A kripto-valutákat létrehozó blockchain technológia megbízhatóságáról sokat elárul az, hogy óriási, készpénzre váltható értékek jöttek bennük létre, mégsem sikerült senkinek a rendszer létét érdemben veszélyeztető támadást kivitelezni. Az elektronikus azonosítás és a névjegyzék ellenőrzése már csak adatvédelmi megfontolásokból is az állam ellenőrzése alatt kell, hogy maradjon. Magának a szavazásnak az anonim végrehajtása egy kifejezetten blockchain-re szabott feladat[11]. Az urnabontás, azaz annak megvalósítása, hogy a szavazatok értéke maradjon titokban egy adott időpontig, már további intézkedést igényel. Triviálisan a szavazók megtehetik, hogy rejtjelezetten töltik fel szavazatukat, majd az *„urnazárást"* követő pl.: egy órában töltik fel a rejtjelkulcsot. Ez a módszer azonban kétszer követel aktivitást a választótól. A rejtjelkulcs feltöltésének hiánya a szavazat elvesztését jelenti. A számlálást

[11] John R. Patrick (2016): *Election Attitude: How Internet Voting Leads to a Stronger Democracy*

a közös főkönyv adatai alapján bárki elvégezheti, akár magán a blockchain-en belül egy erre létrehozott okosszerződés[12] is.

Összefoglalás

Ha az olvasónak a cikk végén olyan érzése van, hogy most kevésbé bízik az elektronikus választási módszerekben, mint mielőtt belekezdett az olvasásba, igaza van! Egy választási rendszernek ugyanis a legfontosabb, *„nulladik"* követelményéről még nem beszéltünk. Ez pedig az, hogy a választónak legalább nagy vonalakban értenie kell, hogy hogyan működik. Azt láttuk, hogy a hagyományos választási rendszer hitelessége nem az informatikára épül. Egy elektronikus választási rendszer iránti bizalom viszont vagy arra a hitre épül, hogy informatikai rendszerét korrektül építették fel és becsületesen üzemeltetik, vagy a kriptográfiára. Az első feltétel a garancia szempontjából irracionális, a második pedig a választókkal szemben fogalmaz meg irracionális elvárást. Attól az embertől várható el, hogy az itt felvetett módszereket megértse, aki annak belátására képes, hogy a magyar jogban teljes bizonyító erő létrehozására alkalmas[13] jelenleg is használt elektronikus aláírás miért hiteles. Az elektronikusan tárolt, bárki által írható, módosítható, másolható nullák és egyek sorozata miért kötődik elválaszthatatlanul ahhoz a dokumentumhoz, amelyet aláírtak, és miért kötődik elválaszthatatlanul az azt aláíró személyéhez? Miért nem lehet azt észrevétlenül módosítani? Ehhez legalább az RSA[14] rejtjelezési eljárás megértésére, a kriptográfiai hash-függvények[15] fontosabb tulajdonságainak tudomásul vételére van szükség... és természetesen arra, hogy ezek milyen eljárást[16] követve használhatók aláírásra és annak ellenőrzésére. Időnként hallani, hogy a tranzisztorról sem tudja a többség azt, hogy miként működik, mégis hallgat rádiót. A hasonlat sántít: ha a tranzisztor nem működik, akkor néma marad a rádió. A rossz elektronikus aláíró rendszert viszont egészen addig bizalommal használom, ameddig ki nem derül, hogy az én aláírásomat más is létre tudja hozni. De a választások esetére vonatkozóan pedig ez a példa sántít, mert a bárki által ellenőrizhető protokoll, és a bárki által végrehajtható számlálás miatt elég, ha van néhány ezer, különböző politikai oldallal szimpatizáló szakember, akinek megvan a kellő szakértelme. Ez a feltétel pedig adott! Emellett figyelembe kell venni, hogy egy külső informatikai támadás veszélyét, sikerének esélyét és következményeit nagyon nehéz reálisan felmérni. Ezért először az elektronikus és hagyományos szavazás önkéntes kiválasztásán alapuló hibrid megoldások megjelenése várható.

[12] https://en.wikipedia.org/wiki/Smart_contract

[13] 2016. évi CXXX. törvény a polgári perrendtartásról 325. § *f)* pontja

[14] https://hu.wikipedia.org/wiki/RSA-eljárás

[15] https://hu.wikipedia.org/wiki/Kriptográfiai_hash_függvény

[16] https://www.tankonyvtar.hu/hu/tartalom/tamop425/0046_informatikai_biztonsag_es_kriptografia/ch09s02.html