A digitális pénzrendszerek biztonsági kérdései

(Networkshop 2006. konferencia-tanulmány)

Horváth Attila

Budapesti Műszaki és Gazdaságtudományi Egyetem
Információ- és Tudásmenedzsment Tanszék
1111 Budapest, Sztoczek u. 2. St. ép. I. em. 117.
Telefon: (36 1) 463-1932, Fax: (36 1) 463-4035
e-mail: hattila@itm.bme.hu

Bevezetés

A digitális pénzen alapuló elektronikus fizetési sémák, bár ma még nem széles körben elterjedtek, megfelelő alternatívát nyújthatnak, a mai, hitelkártya alapú digitális fizetési forgalom felváltására, és a ma élő szisztémák biztonsági és kezelési problémáinak kiküszöbölésére. A kártyán alapuló rendszer egész egyszerűen azért nem alkalmas a teljes körű digitális alkalmazásra, mert eredetileg nem erre fejlesztették, és rendelkezik olyan megváltoztathatatlan tulajdonságokkal, amelyek erőteljesen a fizikai világhoz kötik. Sok kritikai éri ezt a megoldást a biztonsági hiányosságok miatt is, amelyek jórészt szintén erre a problémára vezethetők vissza. A digitális pénzen alapuló rendszerek ezzel szemben eleve digitális környezetben való alkalmazásra lettek tervezve, megalkotásukkor számos biztonsági követelményre kell odafigyelni, amennyiben ezeket teljesíteni tudják elmondható, hogy egy, a jelenlegi hiányosságát valóban kiküszöbölő, életképes rendszerrel van dolga a felhasználónak. Ez a tanulmány a digitális pénzen alapuló fizetési rendszerek rövid áttekintése után ezeket a biztonsági követelményrendszereket járja végig, és igyekszik bemutatni minden lényeges elvárást, amelynek egy mai, modern fizetési rendszernek meg kell felelnie.

1. Elektronikus fizetési rendszerek

1.1. *A fizetési rendszerek fejlődése*

A kezdeti időkben cserekereskedelmet folytattak az emberek, de hamar szükségessé vált valamiféle csereeszköz bevezetése.

Megjelentek az első fizetőeszközök, amelyek esetében valódi a kereskedelmi forgalomban önmagukban is részt vevő áruk (pl. drágakövek, kagylók stb.) képviselték különféle értékeket valósan vagy szimbolikusan. Ezután nemesfémből vertek érméket. A következő lépésben különvált a fizetőeszköz belső (fizikai) és fizetési értéke, ami azt jelenti, hogy ezentúl megállapodáson alapult a pénz csereértéke, amely legtöbbször magasabb volt, mint a pénz előállítási költsége – pl. a papírpénz vagy a modern érmék esetében.

A készpénznek nyilvánvaló előnyein kívül azonban szép számmal akadnak hátrányai is: bizonyos mennyiség felett kezelése nehézkes; szállítása, őrzése költséges, sérülékeny, könnyen megsemmisülhet, ellophatják. Éppen ezért mindenképpen szükség volt egy olyan intézményrendszer kialakulására, amely szakértő módon, biztonságosan, akár nemzetközi szinten képes kezelni, tárolni a pénzt, hogy a tulajdonosnak mindig csak annyi pénzt kelljen személyesen kezelnie, amennyire az adott pillanatban ténylegesen szüksége van. Ez az igény alkotta meg a mai bankrendszert, és a számlapénzt. Innen már logikusan következett a jelölésen alapuló – vagy készpénzkímélő – fizetőeszközök megjelenése, melynek tipikus formája kezdetben a csekk és a váltó voltak. A jelöléses fizetési rendszerek jellemzője, hogy magát a pénzt bankszámlán tárolják, és a számlatulajdonos jogosult a bankban tárolt pénz (a csekken megjelölt személy pedig a csekk-érték) felett rendelkezni. A jelöléses fizetési rendszerekből fejlődtek ki a hitel alapú rendszerek, ahol a bankszámla a fedezet értéke feletti összeggel is megterhelhető.

A hagyományos fizetési rendszerekhez hasonlóan az elektronikus fizetések is két fő csoportra oszthatók, készpénzszerű és számla (nem feltétlenül bankszámla!) hátterű rendszerekre. Az alább felsorolt táblázat magában foglalja a számítógépen, mobil eszközökön, interaktív televízión, valamint az intelligens kártyákon alapuló megoldásokat is.

A másik dimenzió inkább technológiai szempontú felosztást jelent, hiszen míg az Internetes számla, bankkártya és digitális pénz használata már több mint tíz éves múltra tekint vissza, az intelligens kártyákon alapuló megoldások csak mostanában kezdenek utat törni maguknak, jórészt a hagyományos rendszerek hiányosságai miatt.

	Készpénzszerű rendszerek	**Számla hátterű rendszerek**
Hagyományos eszközök	➢ *elektronikus pénz* (számítógépen tárolt); ▪ merevlemezen tárolt ▪ megbízható kliensen tárolt	➢ bankkártya ➢ elektronikus csekk ➢ Internetes számlaterhelés ➢ hitel-betét modell: ▪ központi; ▪ Internetszolgáltatói-; ▪ telefontársasági számlavezetés.
Intelligens kártya	➢ elektronikus tárca	➢ intelligens kártya alapú számla hátterű modell

1. Táblázat: Elektronikus fizetési rendszerek osztályozása [2.]

Ebben a tanulmányban a készpénzszerű rendszerek állnak a vizsgálat középpontjában. A szerző és több kutató (Brands, Chaum, Chamenisch, stb.) szerint a digitális pénz fogja forradalmasítani a digitális fizetési rendszereket és ez jelenti majd egy, a jövőben széles körben elterjedő, mind digitális, mind valós, fizikai használatra alkalmas készpénzkímélő rendszer alapját.

1.2. *A digitális fizetési rendszerek jellemzői*

Az alább felsorolt tulajdonságok jellemezhetik az elektronikus pénzen alapuló fizetési módokat:

- rendszerük szimbolikus vagy jelöléses;
- atomicitás: a tranzakció végrehajtása csak akkor kezdhető meg, ha az garantáltan be is fejezhető;
- konzisztencia: minden résztvevőnek egyet kell értenie a tranzakcióval;
- függetlenség: a műveleteknek egymástól függetlennek kell lenniük;

- megbízhatóság: biztosítani kell a legutóbbi állapot visszaállíthatóságát;
- gazdaságosság: minimalizálni kell az átutalás költségeit;
- átválthatóság: biztosítani kell kis és nagy címletek közötti átválthatóságot (csak jelöléses rendszereknél);
- skálázhatóság: lehetővé kell tenni egyidejűleg több felhasználó kiszolgálását;
- kompatibilitás: biztosítani kell a különböző rendszerek közötti tranzakciók lehetőségét;
- értéktartósság: meg kell akadályozni a pénz értékének romlását.

A fizetési rendszerek sikerességét a felsoroltakon kívül egyéb, nem műszaki tényezők is befolyásolhatják:

- elterjedtség: minél több eladó használja a rendszert;
- megfelelő ügyfélkör: minél több felhasználó kapcsolódjon be a fizetési rendszerbe;
- rugalmasság: egy adott fizetési eszköz különböző más fizetési eszközökkel egy keretrendszerben legyen használható;
- használat egyszerűsége: hozzá nem értők számára is kezelhető legyen.

A két digitális fizetési eszköz csoporton belül különbséget tehetünk a tranzakció lebonyolításakor használt kommunikációs protokoll és a felhasználó azonosíthatósága szerint. Az első esetben két kategóriát különböztetünk meg:

- on-line: a kereskedő minden vásárlásnál kommunikál a bankkal és hitelesítteti az utalványt, ezáltal megakadályozva a csalást;
- off-line: a kereskedő a vásárlás közben nem hitelesítteti az utalványt a bankkal, a köztük levő kommunikáció eseti. Ezért a csalást már csak detektálni lehet, de megelőzni nem.

A felhasználó azonosíthatósága szerint is két kategóriát különböztetünk meg:

- azonosított elektronikus fizetés: megállapítható, hogy eredetileg ki vette fel a bankból a pénzt (a tranzakció „nyomokat” generál, és ezáltal követhető a pénz áramlása az üzleti életben);
- névtelen (*anonim*) elektronikus fizetés: a tranzakció nem követhető, mert nincs nyoma a rendszerben (leginkább a készpénzhez hasonlít).

2. A digitális pénz

A digitális pénz lényegét tekintve több, mint a teremtett pénz egyfajta elektronikus megjelenési formája. Leegyszerűsítve a digitális pénz maga egy információegység, amely értékkel rendelkezik. Ezt az információdarabot a kereskedelemben elfogadják, fel lehet használni vásárlásra, vagy akár készpénzfelvételre is bizonyos korlátok között. A digitális pénz az értéket önmagában hordozza, nem csupán reprezentál egy bankszámlán, vagy hitelkártyaszámlán elhelyezkedő összeget.

Az elektronikus pénz a valódi készpénzes fizetéssel megegyező tulajdonságokkal rendelkezik, vagyis teljesen anonim lehet, a fizetés kedvezményezettjének a tranzakció után a fizető fél felé nincs követelése. Az elektronikus pénz meghatározása a magyar jogszabályok (77/1999. kormányrendelet az elektronikus fizetési eszközök kibocsátására és használatára vonatkozó egyes szabályokról) szerint a következő: „elektronikus pénzeszköz az a távolról hozzáférést biztosító, fizetési eszköznek nem minősülő, újratölthető fizetési eszköz – akár értéktároló kártya, akár számítógép memória –, amelyen értékegységek elektronikus úton tárolhatók, lehetővé téve birtokosának azt, hogy … (fizetési, illetőleg pénzfelvételi) … műveleteket végezzen.”

Az elektronikus pénz monetáris értéket képvisel, vagyis önmagában vett értéke van és betöltheti a pénz négy közgazdaságilag klasszikus – forgalmi, fizetési, megtakarítási és értékmérő – funkcióját. Az értéket egyedileg azonosítható elektronikus jelcsomagok, ún. tokenek vagy érmék reprezentálják, amelyek a felhasználó számítógépén tárolódnak. A tárolás történhet egyszerűen a merevlemezen, szigorú kriptográfiai megoldások védelmében, vagy egy megbízható célhardveren, ún. elektronikus pénztárcán (chipkártya). Ekkor a védelem is hardveres, és a pénzegységek csak fizetési szándék esetén kerülnek kapcsolatba a számítógéppel. Az első esetben a felhasználónak még egy pénztárca software-t is telepítenie kell, ezen keresztül végezheti a fizetéseket.

A digitális pénz kiküszöböli a hagyományos készpénz sok hátrányát megtartva annak legtöbb előnyét. A digitális pénz teljesen tiszta, könnyen szállítható tetszőlegesen nagy tömegben. Megfelelő algoritmusok segítségével könnyű előállítani, mégis nehéz hamisítani, vagy másolni.

Amennyiben célhardveren, intelligens kártyán kerül tárolásra, úgy a hordozó előállítása itt is fejlett technológiát és költséges eljárásokat igényel, de pénzegységre vonatkoztatva még mindig a töredéke a papírpénz előállítási költségeinek, mivel egy eszközön tetszőleges mennyiségű pénz tárolható és bármikor újratölthető, kopása alacsony, és a környezeti hatásokat viszonylag jól tűrő eszközről van szó. A digitális pénz egyszerű átadással cserélhet gazdát, így alkalmas P2P fizetésekre is, az anonimitás megvalósítható, de ez olyan ellenőrzési eljárásokat igényel, amelyek csökkentik a rendszer hatékonyságát és növelik a tranzakciós időt, így az anonimitás és a hatékonyság között általában kompromisszumot kell találni.

2.1. *Digitális pénz sémák*

A digitális pénz séma azoknak a protokolloknak, algoritmusoknak és szabályoknak az összessége, melyek segítségével egy digitális pénz funkcionalitású rendszer építhető fel.

2.2. *A tranzakciók szereplői*

A digitális vásárlások igényelnek egy vevőt, egy eladót és legalább egy pénzügyi szolgáltató intézményt is. Általában külön intézmény tartozik a vásárlóhoz és az eladóhoz. Alapvető szereplők:

- vevő, felhasználó
- kereskedő, eladó;
- vásárló bankja, (issuer bank): a vásárlóval együttműködve digitális pénzt képes kibocsátani;
- kereskedő bankja

Ezen felül fontos szereplők még:

- megbízható harmadik fél (TTP – Trusted Third Party): a bankrendszertől független szereplők, melyek egy része kormányzati vagy bírósági irányítás alatt, más részük pedig felhasználói jogvédő szervezetek kezében van. Az ő segítségükkel lehetséges az anonimitás visszavonása;
- tanúsítvány-kiállító hatóságok (CA, Certification Authority): mivel a rendszerek többsége digitális aláírást használ, ezért szükség van tanúsítvány-kiállító hatóságokra (hitelesítés-szolgáltatókra), illetve a PKI-t (Public Key Infrastructure) felépítő más szervezetek szolgáltatásaira is.

2.3. *A tranzakció fő fázisai*

- Átutalási fázis : A felhasználó bankszámlájáról pénzösszeg emelődik le, és digitális pénz formájában belekerül a pénztárcájába.
- Fizetési fázis: A vásárló a kívánt áruért vagy szolgáltatásért cserébe átadja a kereskedőnek a megfelelő mennyiségű digitális pénzt. A rendszer on-line, ha ebben a fázisban szükséges a fizetési szolgáltatóval való kommunikáció.
- Pénzbetét fázis: A kereskedő a felhasználóktól kapott pénzt beváltja a bankjában, az ezzel egyenértékű összeg megjelenik a bankszámláján.

3. A digitális pénzrendszerek biztonsága

Mint minden pénzügyi folyamatban, a biztonság itt is elsőrendű fontosságú, sőt mivel a – többnyire csak a tervezőasztalon létező – digitális pénzrendszereket általában multidiszciplináris tudással rendelkező szakemberek dolgozták, a legfontosabbnak tartják a biztonságot és a személyes adatok védelmét. Alapvetően mindig úgy állnak hozzá a tervezéshez, hogy kompromisszumoktól mentes adatbiztonságot és adatvédelmet szeretnének. Jóllehet elméleti és gyakorlati okok miatt a tökéletesség eleve nem lehetséges, de egy üzleti vállalkozás ehhez képest más értékrendet képvisel. Egy bank vagy egy kereskedő szemszögéből nézve nagyobb hangsúlyt kapna a kivitelezhetőség, a gazdaságosság, a profitabilitás. Az utóbbi tulajdonságok mind az adatbiztonság és adatvédelem ellen hatnak. Mivel a csalások elkerülése miatt az adatbiztonság a bank érdeke is, ezért valószínűleg gondoskodik annak megfelelő szintjéről (bár sokszor ez sem igaz), azonban nincs kielégítő biztosíték arra, hogy megfelelő adatvédelmet nyújtson ügyfelei személyes adatainak kezelése szempontjából. Ezen rendszerek tervezésénél a kriptográfia mellett nagy szerepet kap többek között még a tranzakció tudománya, az adatbázis- és hálózati ismeretek. Fontosak a gazdasági, ergonómiai és jogi vetületek is. **A végcél pedig természetesen az, hogy megtalálva az egyensúlyt az egyes szempontok között egy működőképes, gazdaságilag és üzletileg hatékony és emellett a lehető legmagasabb adatvédelmi és –biztonsági szintet képviselő rendszer terjedjen el és kerüljön gyakorlati alkalmazásra.**

Ehelyt máris fontos rávilágítani az adatvédelem és az adatbiztonság – sokszor keverten használt fogalmainak – különbségeire. Mindkettő egyaránt fontos, és az alább bemutatásra kerülő digitális pénz protokollok mindkettőt igyekeznek megvalósítani.

Az **adatbiztonság** az adatot védi az illetéktelen kezekbe kerüléstől és a jogosulatlan felhasználástól, ide tartozik a pénzrendszer alapjául szolgáló szoftver és hardver eszközök valamint az adatátvitelt megvalósító hálózatok

- bizalmasságának,
- sértetlenségének, és
- rendelkezésre állásának védelme.

Az **adatvédelem** ezzel szemben a személyes adatokat védi, az adatok tartalmára helyezi a hangsúlyt. Célja, hogy az egyes tranzakciók esetében minden fél csak annyi személyes adathoz (itt általában a digitális pénz tulajdonosának adatairól van szó) jusson hozzá, amennyi a tranzakció biztonságos kivitelezéséhez feltétlenül szükséges. Tehát például a banknak, vagy a digitális fizetési szolgáltatónak csak azt kell tudni, hogy melyik kereskedőnek, mennyi pénzt utaljon át, de azt már nem kell tudnia hogy ezért a fogyasztó mit vásárolt.

A biztonságnak két szintje különböztethető meg a szerint is, hogy a védelem magából az adott fizetési rendszer működéséből eredően specifikusan az adott tranzakció résztvevőit támogatja, vagy szabványos módon a hálózatba beépülve biztosítja a biztonságos kommunikációt. A pénzrendszerek biztonságát az alábbiakban ismertetett követelmények teljesítésével lehet létrehozni, illetve fokozni. A hálózati szintű titkosítást pedig az esetek 99%-ában az SSL (Secure Socket Layer) hálózati protokoll segítségével valósítják meg a fizetési szolgáltatók.

3.1. *A biztonságos működés követelményei*

Ahhoz, egy digitális pénzrendszer megfelelően biztonságosnak minősüljön, rengeteg követelménynek kell megfelelnie. A később leírt bizalmasság, hitelesség, integritás és letagadhatatlanság tulajdonságok maguktól értetődőek, többnyire részei azon alaprendszereknek, sémáknak, amelyekre az egyes pénzrendszerek alapulnak. A bizalmasságot a kriptográfiai technikák és rejtjelezések explicit módon illetve mellékhatásként biztosítják. Az integritást az anonimitásért felelős kriptográfiai technikák biztosítják. Ha az ideális séma digitális aláírást is használ, a letagadhatatlanság implicit módon biztosítva van, ellenkező esetben bizonyítottnak kell lennie.

Ezeknek a tulajdonságoknak nem elég pusztán a megléte, az is fontos, hogy milyen kriptográfiai és matematikai technológiákkal éri el a séma a biztonságot, mivel védekezik a logikai támadások ellen. A bűncselekmények ellen védő kriptográfiai technikák alapvető jellemzői a bennük alkalmazott nevezetes kriptográfiai protokollok típusa. Ez adja meg miért nehéz feltörni, milyen nehézségeket állít az esetleges támadó elé.

A biztonsági követelmények fogalomkörén belül a következő tulajdonságokat szokták számba venni, ezeket egy megfelelő rendszernek mindenképpen teljesítenie kell.

3.1.1. Letagadhatatlanság (Non-Repudiation)

Miután érvényesen lezajlott egy tranzakció, egyik résztvevő sem tudja letagadni annak végbemenetelét. Fontos szerepet kap vitás esetekben az atomicitás is.

3.1.2. Hitelesség, hitelesítés (Authentication)

A tranzakció minden mozzanatában implicit vagy explicit módon ott kell lennie a hitelesítésnek. A kommunikáció során a hitelesség kölcsönösen biztosítja mindegyik felet, hogy a tranzakcióban résztvevő többi fél az akinek mondja magát, azaz érvényes az identitása. A hitelesség biztosíthat egy résztvevő felet arról, hogy egy entitás vagy információ hiteles:

- a kereskedőnek tudnia kell ellenőrizni, hogy a digitális pénz érvényes, valódi;
- a banknak tudnia kell megbizonyosodni arról, hogy a tranzakció hitelesített felek között ment végbe;
- léteznie kell olyan eljárásnak, amellyel leellenőrizhető a kereskedő bankja és bankszámlája, a vevő bankja és bankszámlája.

3.1.3. Integritás (Integrity)

Biztosítja, hogy a tranzakciót nem tudja megváltoztatni olyan résztvevő, aki közvetlenül nem vesz részt az ügyletben. A résztvevő felek is csak jól meghatározott, az ő érdekeltségi körükbe tartozó, paramétereket módosíthatnak a tranzakció lefolyása során (például a bank nem írhatja át a vételárat). Ez tehát egy külső és belső védelmet jelent a manipulációk ellen. Létezik az integritásnak egy olyan megfogalmazása is, miszerint nem adható hozzá monetáris érték a rendszerhez és nem vonható ki a rendszerből monetáris érték nem szabályos úton. Ez megakadályozza a hamisítást, dupla költéseket és egyéb bűncselekményeket. Az integritást egyrészt a rendszer kriptográfiai technikákkal elért biztonsági tulajdonságai, másrészt az atomicitás biztosítja.

Gyakran az integritás tulajdonság alatt bizalmassági követelményeket is értenek: titkos vagy privát információ nem férhető hozzá a rendszerben explicit engedély nélkül.

3.1.4. Engedélyezés (Authorization)

A rendszer lehetőséget biztosít arra, hogy résztvevő felek engedélyezhessék, jóváhagyhassák az elektronikus tranzakciót. Ez egy olyan lépés, amit a való életben is sokszor tapasztalunk, főleg nagy értékű vásárlás esetén. A megvalósításban nincs semmi különlegesség, csak arra kell figyelni a teljes rendszer megvalósítása során, hogy a vásárló láthasson egy számlát (lehet elektronikus is) a tranzakcióról, és ezt jóváhagyhassa. A tranzakció elvetése valamilyen rendszeren kívül származó rendellenesség esetén jön szóba, ami megjelenik a számlán (például egy bevásárlóközpontban a termékre az akciós ára helyett a normál árát számlázzák). A rendszert célszerűen úgy kell felépíteni, hogy ez még a fizetési tranzakció előtt kiderüljön, így nem szükséges egy visszavonási folyamaton keresztül menni, ami további idő és költségvonzatokkal, kényelmetlenségekkel jár együtt. Csak figyelembe kell venni a rendszer tervezése során ezeket a kívülről fakadó problémákat.

3.1.5. Bizalmasság (Confidentality)

Ez azt jelenti, hogy egyfelől a külső szemlélők nem képesek megfigyelni a résztvevő felek között végbemenő tranzakciókat, másrészt a tranzakciókban résztvevő felek számára az információhoz való hozzáférés a szerepüknek megfelelően korlátozva van. Az első feltételt a kriptográfiai technikák és rejtjelezések biztosítják; a másodikat, amelyet néhányan az integritás tulajdonságba sorolnak, az anonimitás illetve az azzal járó kriptográfiai technikák biztosítják.

3.1.6. Visszaigazolás (Confirmation)

Mind a kereskedőnek, mind a vásárlónak kapnia kell egy igazolást arról, hogy a tranzakció végbement, ezáltal mindketten tudják, hogy a pénz gazdát cserélt. Adott esetben ezek az igazolások lehetnek a bizonyítékok arra, hogy a fizetés megtörtént. A jelenlegi, hitelkártyákon alapuló rendszerek esetében az engedélyezés és a visszaigazolás is létező funkciók. Jogos az elvárás, hogy a digitális pénz is biztosítsa ezeket. Habár nagyon fontos ez a két tulajdonság, de mivel nem szerves részei a pénzrendszereknek, általában külön rendszerként, modulként építhetők be.

3.1.7. Megbízhatóság (Reliability), Rendelkezésre állás (Availability)

Egy digitális pénzrendszernek folyamatosan használhatónak kell lennie. A vásárló akkor és ott szeretne fizetni vagy pénzt kapni, ahol számára szükséges. Noha ez a tulajdonság is fontos része a tágabb értelemben vett biztonságnak, elsősorban szervezési eszközökkel biztosítható: redundáns erőforrások (szerverek, kommunikációs vonalak, stb.). Az ideális séma annyit segíthet a magas rendelkezésre állás elérésében, hogy megpróbálja minimalizálni az olyan támadások kockázatát, melyek a rendelkezésre állást sértik. Rendszer-szerkezetileg az segíthetne, ha nem lenne olyan központi szerver, ahol számítások koncentrálódnak és ily módon a rendszer gyenge pontját képezik. Sajnos ez nem megoldható, a védekezés szintén inkább szervezéssel oldható meg: például a fent említett módszerek, redundáns és backup rendszerek alkalmazása, különböző bankfiókokban való elhelyezése.

3.1.8. Ellenállás a logikai támadási lehetőségeknek

Ez a biztonságnak azt az aspektusát jelenti, amely a logikai támadásokkal szembeni védelmet és a bűncselekményekkel szembeni ellenállást biztosítja. Ahhoz, hogy jobban átlátható legyen, milyen feltételeket támaszt ez a sémákkal szemben, érdemes áttekinteni a lehetséges támadásokat [1.] alapján.

- Túlköltés (Overspending): Egy felhasználó egy szabályosan kivett összeget magasabb értékkel költ el, mint amekkora az valójában. Túlköltés az is, ha a felhasználó az érvényesen kivett érmével többször is fizet. Ekkor a második és az azutáni fizetési tranzakciók csalások. Dupla költésnek (double spending) nevezik, ha kétszer használja fizetésre az érmét.
- Hamisítás (Forgery): A támadók csoportja együttműködik, hogy olyan hamisított pénzösszeget vegyenek ki felhasználók számára, vagy olyan hamisított vásárlásokat vigyenek véghez, amelyek egy becsületes bank számára valódinak tűnnek.
- Megszemélyesítés (Impersonation): Többszörös terhelésnek is nevezik. A támadók csoportja egy felhasználót nagyobb összeggel terhel, mint amennyit az valójában elköltött. Ez például úgy lehetséges, hogy a résztvevő felek, közöttük egy kereskedő, duplán vagy még többször próbálnak pénzt betenni egy tranzakció információi alapján.
- Pénzmosás (Money laundering): egy vagy több résztvevő fél leplezi a megkérdőjelezhető forrásból származó bevételének forrását úgy, hogy az egy másik üzleti vállalkozás bevételének tűnik. Ez adott esetben illegális pénzmozgatási tranzakció segítségével érhető el. A kivédéshez a rendszernek képesnek kell lennie a fizetések nyomkövetésére, hogy stabil bizonyítékot lehessen felmutatni bűntény felmerülése esetén.

- Illegális vásárlások (Illegal purchases): Olyan tranzakciók, amelyek pénzforgalmi szempontból teljesen érvényesek, de a vásárolt áruk természete miatt nem legálisak.
- Zsarolás (Blackmail): Egy támadó arra kényszeríti a felhasználót, hogy vegyen ki pénzt neki oly módon, hogy végül csak a támadó ismerje az érték digitális reprezentációját. Ezt általában úgy érheti el, hogy a felhasználót és esetleg a bankot is egy nem standard protokollban való részvételre kényszeríti. A tökéletes anonim bűntény [8.] ellen szintén nyomkövetéssel lehet védekezni, azonban ez további problémákat vet fel (bizalmassági, adatvédelmi problémák, anonimitás megsértése).
- Bankrablás (Bank robbery): Kétféle támadást különítenek el ilyen néven. A kibocsátó (bankok és más entitások, amelyek kezében van a pénz készítéséhez vagy követéséhez szükséges titkos kulcs) entitástól egy támadó megszerzi a titkos kulcsot, például belső támadással, vagy valamilyen módon kényszeríti erre. Ezek a támadások azért nagyon súlyosak, mert ha az érme hitelessége csak a kibocsátó aláírásától függ, akkor praktikusan nem lehetséges az aláíró számára az illegálisan előállított pénzek követése, ezáltal a támadó kilétét nem lehet felfedni.
- Rosszindulatú nyomkövetés (Malicious tracing): Támadás Bankok és a TTP csoportja által, melynek során törvényes felhatalmazás nélkül nyomkövetnek pénzeket, pénzkivételeket, tranzakciókat. A banknak, mint profitorientált entitásnak érdekében állhat az ügyfeleiről adatokat gyűjteni (hovatovább esetleg más vállalatoknak statisztikákat vagy profilokat értékesíteni). Ennek elkerülése érdekében a követési tranzakciókba, és magába a digitális pénzrendszerbe további résztvevő feleket kell bevenni (Ombudsman, TTP), akik a kérdéses bank irányításán kívül esnek. Ezeket az entitásokat társadalmi érdekképviseleti szervezetek üzemeltethetik, illetve a törvényhozáshoz is tartozhatnak.
- Koholt vád (Framing): A támadásban résztvevő felek úgy tüntetik fel, hogy egy felhasználó vagy egy kereskedő részt vett egy adott tranzakcióban, miközben ez nem igaz. Adott esetben képesek fizetési számlát is generálni, melyet nyomon követve a becsületes felhasználóhoz vagy kereskedőhöz jutnak el a hatóságok.
- Sikkasztás (Embezzlement): Olyan támadás, melynek során a felhasználó pénzt veszít, mert a bank érvénytelennek tüntet fel egy tranzakciót, vagy csak kevesebb pénzt fogad el, pedig több érvényes érme/érték is rendelkezésére áll a felhasználónak.

Becsületes / *Támadó*	Felhasználó	Kereskedő	Bank	Trustee
Felhasználó	Zsarolás, Megszemélyesítés	Túlköltés	Hamisítás, Túlköltés, Bankrablás	-
Kereskedő	Sikkasztás, Megszemélyesítés	Megszemélyesítés	Hamisítás, Pénzmosás, Bankrablás	-
Bank	Rosszindulatú visszakövetés, Koholt vád, Sikkasztás	Koholt vád, Sikkasztás	-	-
Trustee	Rosszindulatú visszakövetés, Koholt vád	-	-	-

2.Táblázat: Logikai támadástípusok összegzése [1.]

3.1.9. A logikai támadási lehetőségekből fakadó követelmények

Hogy mindezek a támadások elkerülhetők legyenek, többek között a következő biztonsági tulajdonságok megléte is szükséges:

- Hamisíthatatlanság: Csak az arra felhatalmazott entitások képesek érvényes digitális pénzt kibocsátani.
- Megszemélyesíthetetlenség: A megszemélyesítés nem lehetséges.
- Túlköltés-érzékelés.
- Túlköltés-robosztusság: Ha több résztvevő fél követ el túlköltést ugyanazon információk (érme információk) felhasználásával, akkor a nyomkövetéssel mindegyikük identitása kideríthető.
- Nyomkövethetőség: lehetséges a pénzkivétel- és az érme-nyomkövetés. Opcionális esetben (pénzkivétel, érme) pár összetartozásának eldöntése.
- Visszavonhatóság: Gyanús érmék ideiglenesen elkölthetetlenné tehetők, például feketelistás technika segítségével. Egy ideális rendszer esetén pedig követelhetjük, hogy ez ne rontsa a rendszer hatékonyságát.
- Anonimitás
- Koholt vád lehetetlensége
- Visszaforgathatóság: sikkasztásos támadás esetén a kárt elszenvedő áldozat bizonyítani tudja támadást, és legalább az egyik támadó kiléte kiderül.

3.2. *Egy példa a tökéletes biztonságra való törekvésre: a vak aláírás alapú sémák*

A vak aláírás protokollhoz (blind signature protocol) a következő fizikai analógia képzelhető el. Az aláírás fogadó belehelyezi az aláírandó dokumentumot egy indigós papírral együtt egy borítékba, majd lezárja a borítékot. Az aláíró aláírja a borítékot anélkül, hogy kinyitná azt, vagy bármely módon tudomást szerezne a tartalmáról. A fogadó ezután megkapja a borítékot, melyben a dokumentum már alá van írva. A hitelességet a fogadó bárkinek bizonyítani is tudja az aláírás felmutatásával.

1. A vevő elkészít N darab V értékű névtelen fizetési utalványt. Az utalványokat véletlen egyedi sorszámmal (Random Uniqueness String – RUS) látja el.
2. A vevő különböző „vakoló”[1] faktorokkal „vakolja” az utalványokat (kriptográfiai eljárás), majd „digitális borítékba” helyezi őket és eljuttatja a banknak.
3. A bank kiválaszt N-1 darab borítékot és kinyitja, majd ellenőrzi – ehhez a banknak szüksége van a „vakoló” faktorokra –, hogy a névtelen utalványok azonos értékűek-e és az egyedi azonosítójuk különbözőek-e.
4. A bank anélkül, hogy ismerné a megmaradt egy boríték tartalmát, digitálisan aláírja az utalványt és visszaküldi a vevőnek; ezt követően megterheli a vevő számláját V összeggel.
5. A vevő leszedi a „vakolást” az utalványról és a kereskedőnél fizet az utalvánnyal. A fizetés annyit jelent, hogy a hálózaton keresztül elküldi a kereskedőnek az utalványt.
6. A kereskedő ellenőrzi a bank digitális aláírását az utalványon – ehhez a bank nyilvános kulcsát használja. Ha hitelesnek találja, kéri a vevőt, hogy lássa el az utalványt véletlen egyedi azonosítójával (Random Identyfying String – RIS). Ezután eljutatja a banknak az utalványt.
7. A bank ellenőrzi az utalványon a saját digitális aláírását, valamint adatbázisában megkeresi az utalvány egyedi sorszámát. Ha nem találja a nyilvántartásában az utalvány egyedi sorszámát, akkor azt az utalványon levő azonosítóval együtt nyilvántartásba veszi, és átutalja az eladónak az utalvány V értékét.

---

[1] M*egjegyzés:* Az eredeti, „blind signature” (vak aláírás) kifejezésből származtatott további fogalmak szó szerinti fordítása magyarul mulatságos, vagy éppen zavaró képzeteket keltő kifejezéseket eredményez. Tóth Csaba [1.] sajátos megoldást választott a „blinding” és a kapcsolódó fogalmak magyarítására: a két szó hangalakjának hasonlóságát kihasználva a „vakítást” „vakolás”-nak fordítja, utalva egyúttal a vakolás elfedő, elrejtő funkciójára. Ebből következően beszél „bevakoló” és „kivakoló” függvényről, „vakolási” faktorról, „vakolt” aláírásról. A nyelvi leleményt elismerve, egyúttal az egységes magyar szóhasználat hiányát figyelembe véve megtartottuk ezt a szóhasználatot, azonban mindenütt idézőjelbe téve, hogy elkerüljük téves értelmezését. Az elfedést az itt bemutatott borítékolási hasonlattal is ki lehet fejezni a magyar nyelvben. A szakirodalom tehát ezt a második elfedési fázist borítékolásnak, és az angolul szintén „blinded digital coin”-ként emlegetett fogalmat „borítékolt digitális érmének” nevezi.

A protokoll módot ad a csalás leleplezésére. Az utalvány azonosítóját összehasonlítva a nyilvántartásban levő azonosítóval az is megállapítható, hogy a vevő vagy az eladó csalt – ha megegyezők az azonosítók, akkor a kereskedő, különben az eladó.

Kis változtatással elérhető, hogy csalás estén a vevő személyazonossága is meghatározható legyen. Ennek lényege, hogy az utalványokat a vevő egy olyan azonosítóval látja el, mely tartalmazza az azonosításához szükséges adatokat.

A legtöbb aláírás teljes vak aláírás. A vak aláírás önmagában csak a nyomkövethetetlenséget biztosítja, nem véd a túlköltések ellen. Csak az úgynevezett one-show típusú vak aláírások [4.] garantálják, hogy akkor és csak akkor fedődik fel a tulajdonos kiléte, ha többször próbálja elkölteni ugyanazt a pénzt.

A vak aláírások olyan implementációja is lehetséges, ahol több résztvevő is egyszerre részt vesz a számításban. A számításhoz a bank szolgáltatja az egyik bemenetet (titkos aláíró kulcs), a vásárló a másikat (aláírandó üzenet), és végül egyedül a vásárló kapja meg a kimenetet (aláírt üzenet). A biztonság alapvető kriptográfiai feltételezésekre visszavezethető. Azonban az ilyen több-résztvevős protokollok hatékony megvalósítása nagy kihívást jelent.

Mint látható a megoldás csaknem tökéletes adatvédelmet és jelentős adatbiztonságot biztosít. Számításigénye meglehetősen nagy ezért valószínűleg csak elosztott feldolgozási rendszerben lehetne hatékonyan üzemeltetni. A logikai támadások elleni védelem az irányított, szabályozott visszafejthetőségen keresztül valósul meg, míg a biztonság többi aspektusát a többszörös kriptográfiai kódolás, valamint maga az elosztott rendszer biztosítja. Azzal, hogy minden szereplőnek csak a tranzakció végrehajtásában vállalt szerepének szigorúan megfelelő mennyiségű információ van a birtokában, lehetővé válik, hogy még ha sikerül is elfogni valamelyik pontján a tranzakciót, az információk elégtelensége miatt nem lehet visszaélni az így nyert adatokkal még akkor sem, ha a a kriptográfiai védelmet sikerülne feltörni. A rendelkezésre állás és a megbízhatóság követelményeit pedig a kiszolgáló rendszerek HW, SW teszik teljessé.

Összefoglalás

A sokrétű biztonsági és egyéb igények ellenére a szerző szerint létrehozható egy olyan valóban működőképes digitális pénzen alapuló fizetési rendszer, amely tökéletesített utódjává válhatna, a jelenlegi, többnyire hitelkártya alapú, hibrid megoldásoknak. A legnagyobb gond talán az, hogy az egyes követelmények teljesítésére, mint például a kvázi-tökéletes adatvédelem, vagy az adatbiztonság, külön-külön születtek már tudományos megoldások. Ezek integrációja, és üzletileg, gazdaságilag és ergonómiailag is működőképes keretbe foglalása hiányzik. Mindezen tulajdonságokat ugyanis egy könnyen kezelhető, gyors reakcióidejű, nem irreális számítási kapacitás-igényeket támasztó rendszernek kell megvalósítani. A legközelebb talán a már ma is használatos mikrokereskedelmi rendszerek jutottak a probléma megoldásához, de még ezek is jelentős engedményeket tesznek a biztonság területén a hatékonyság érdekében. A digitális pénzrendszerek eddigi mérsékelt sikere azonban nem csak ennek, hanem az erős piaci (Ki bocsáthat ki pénzt?, Ki lehet fizetési szolgáltató?) ellenérdekeltségnek és a hagyományokhoz való ragaszkodásnak is betudható. A technológia és az e-business fejlődése azonban kérlelhetetlenül halad előre és egyre inkább megmutatkozik a valós, piaci igény egy hatékonyabb fizetési rendszer iránt.

Hivatkozások

[1.] Tóth Csaba: Egy ideális anonim digitális pénzrendszer, *ALMA MATER: Szabad adatok, védett adatok*; BME ITM, 2005.

[2.] Gócza Zoltán: Mikrokereskedelem, Bagolyvár kiadó, Bp. 2002.

[3.] D. Chaum: Blind Signatures for Untraceable Payments, *Proceedings of Crypto '82,* p. 199–203, Plenum Press, New York and London, 1983.

[4.] D. Chaum, A. Fiat, M. Naor: Untraceable Electronic Cash, *Proceedings of Crypto '88,* LNCS Vol. 403, p. 319–327, 1990.

[5.] Tóth, Csaba: Anonim kommunikáció és a proxy szerverek, BME ITM, *ALMA MATER: Sokszínű e-világ,* p. 145–164, Budapest, 2002. február.

[6.] Horváth Zsolt: A bankkártya üzletág bemutatása, Giro Bankkártya Rt., 2003. nov.

[7.] Sántha Péter: Kártyatechnológia (kézirat), BME ITM, Bp. 2003.

[8.] S. von Solms, D. Naccache: On Blind Signatures and Perfect Crimes, *Computers and Security,* Vol. 11, No. 6, p. 581–583, 1992.

[9.] Székely Iván: PET technológiák: a személyes adatok védelmének korszerű eszközei, In: *Létezik-e adatvédelem adatbiztonság nélkül?,* Infoszféra Kft., Budapest 2000.

[10.] S. Brands: Electronic Cash on the Internet, *Proceedings of the Internet Society Symposium on Network and Distributed System Security,* San Diego, California, 1995 February