HU 000221396 B1

(19) Országkód

HU

MAGYAR KÖZTÁRSASÁG

MAGYAR SZABADALMI HIVATAL

SZABADALMI LEÍRÁS

(11) Lajstromszám:

221 396 B1

(21) A bejelentés ügyszáma: P 98 00982
(22) A bejelentés napja: 1996. 04. 19.
(30) Elsőbbségi adatok:
08/427,287 1995. 04. 21. US
(86) Nemzetközi bejelentési szám: PCT/US 96/05521
(87) Nemzetközi közzétételi szám: WO 96/33476

(51) Int. Cl.[7]

G 07 F 7/08
G 06 F 17/60

(40) A közzététel napja: 1998. 08. 28.
(45) A megadás meghirdetésének dátuma a Szabadalmi Közlönyben: 2002. 09. 30.

(72) Feltaláló:
Rosen, Sholom S., Ne York, New York (US)

(73) Szabadalmas:
CITIBANK, N.A., New York, New York (US)

(74) Képviselő:
Szuhai Elemér, DANUBIA Szabadalmi és Védjegy Iroda Kft., Budapest

(54) **Eljárás pénznemek közötti átváltásra**

KIVONAT

A találmány eljárás pénznemek közötti átváltásra, első idegen pénznemű pénz ügyfél tranzakciós pénztármodulj̈ában tárolt elektronikus megjelenítője és második idegen pénznemű pénz tulajdonos második pénztármoduljában tárolt elektronikus megjelenítője között, amelynek során

a) az első tranzakciós pénztármodul (1186) és második pénztármodul (1188) között rejtjelezéssel biztosított kapcsolatot hoznak létre,

b) az ügyfél az első tranzakciós pénztármodulján (1186) beadja az első pénznemben eladni kívánt – első – pénzösszeget,

c) leellenőrzik, hogy az első tranzakciós pénztármodulban (1186) van-e tárolva a tranzakcióhoz szükséges mennyiségű elektronikus pénzmegjelenítő,

d) az első tranzakciós pénztármodulból (1186) rejtjelezéssel biztosított kapcsolatban átküldik az első pénzösszegadatot a második pénztármodulba (1188),

e) a második pénztármodul (1188) tulajdonosától átváltási árfolyamot vagy a második pénznemben megadott – második – összegadatot kérnek,

f) leellenőrzik, hogy a második pénztármodulban van-e tárolva a tranzakcióhoz szükséges mennyiségű elektronikus pénzmegjelenítő,

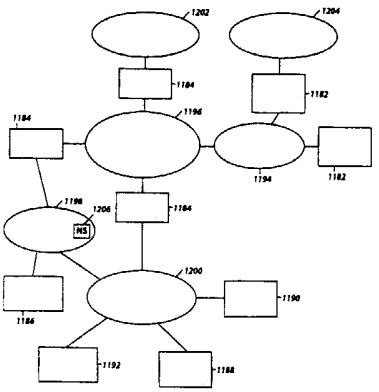
g) a második pénztármodulból (1188) üzenetet küldenek az első, tranzakciós pénztármodulba (1186) rejtjelezéssel biztosított kapcsolatban, közölve az átváltási arányt és/vagy a második összeget,

h) az első ügyfél elfogadja az átváltási arányt és/vagy a második összeget,

i) az első tranzakciós pénztármodulból (1186) rejtjelezéssel biztosított kapcsolatban átküldik az első pénzösszegnek megfelelő, első pénznemű elektronikus pénzmegjelenítőt a második pénztármodulba, (1188)

j) a második pénztármodulból (1188) rejtjelezéssel biztosított kapcsolatban átküldik a második pénzösszegnek megfelelő, második pénznemű elektronikus pénzmegjelenítőt az első, tranzakciós pénztármodulba, (1186)

k) az első, tranzakciós pénztármodul (1186) átadja, a második pénztármodul (1188) átveszi az első pénznemű, első összegű pénzmegjelenítőt, a második pénztármodul (1188) átadja, az első, tranzakciós pénztármodul (1186) átveszi a második pénznemű, második összegű pénzmegjelenítőt, előre meg nem határozott sorrendben.



2. ábra

A leírás terjedelme 74 oldal (ezen belül 54 lap ábra)

HU 221 396 B1

A találmány tárgya eljárás pénznemek közötti átváltásra, első idegen pénzű ügyfél tranzakciós pénztármoduljában tárolt elektronikus megjelenítője és második idegen pénznemű pénztulajdonos második pénztármoduljában tárolt elektronos megjelenítője között.

Manapság évente mintegy 350 milliárd fizetés, illetve pénzátutalás történik egyének és intézmények között. A fémpénz és papír bankjegyek alkalmazása fizetőeszközként korlátozza a fizetési, váltási és banki műveletek automatizálhatóságát. A készpénzfizetéshez rendelkezésre kell állnia a pontos összegnek, illetve a visszaadáshoz szükséges váltópénznek. A fémpénzek és papír bankjegyek kezelése körülményes, kényelmetlen és költséges az egyén és az intézmény számára egyaránt. Becslések szerint csak az USA-ban évente 60 milliárd dollárba kerül a pénzmozgatás. További hiányosság, hogy a papír bankjegyek viszonylag könnyen, akár színes fénymásolóval is hamisíthatók.

Bár a csekkek tetszés szerinti összegről kiállíthatók, az átruházhatóságuk erősen korlátozott és kitöltendő csekket csak egy meglévő fizikai érték alapján bocsátanak ki. A papírpénz-kibocsátó rendszerek a bankjegyek kezelésével járó kényelmetlenség és a csekkek későbbi beváltása miatt nem képesek a készpénzforgalom megfelelő korlátozására. Szükség van tehát egy gazdaságosabb és kényelmesebb pénzkezelési eszközre, amely megfelelő biztonságot és titokvédelmet is nyújthat.

Létezik egy bankrendszer központi számítógépes hálózatán alapuló, EFT elektronikus transzfer rendszer (EFT=electronic fund transfer), amely a nagytételű pénzátutalások elektronikus „csekkfizetés" jellegű megvalósítására alkalmas, banki számítógépek, főként nagy kereskedelmi szervezetek közötti pénzmozgatásra.

Más fizetési rendszerek is léteznek, így az ACH (Automated Clearing House) és a POS (point of sale) rendszerek, amelyeket az elosztó és kereskedő cégek alkalmaznak üzlethálózatukban. E rendszerek alkalmazásának korlátja azonban, hogy bankrendszer bekapcsolása nélkül nem működőképesek. Az ACH rendszer további korlátja, hogy csak munkaidőben üzemeltethető.

A „Home Banking" számlafizető szolgálatok természetes személy ügyfelek által is használható elektronikus fizetési rendszerek, amelyek használata azonban nem terjed el, főként azért, mert az ügyfél nem tudja pénzzel feltölteni a rendszerét, illetve nem tud onnan készpénzt kivenni. A szolgáltatást nyújtó bankok adatai szerint ügyfeleiknek kevesebb, mint egy százaléka veszi igénybe ezt a szolgáltatást.

Az alkalmazott EFT rendszerek, kreditkártyák, debitkártyák, amelyekkel online fizetés eszközölhető egy kereskedő számlája és egy ügyfél számlája között, nem elégíthetik ki az automatikus pénzmozgatással kapcsolatos igényeket: sem az általános alkalmazhatóságra, sem a bankrendszer kiiktatására vonatkozó igényeket. A bankkártyák ráadásul nem is kielégítően biztonságosak és titkosak, csalás ellen nem nyújtanak kellő védelmet.

Automatikusan és általánosan, bankrendszer átutalási folyamatba iktatása nélkül alkalmazható pénzmozgató rendszerre, amellyel monetáris érték közvetlenül átadható, leginkább off-line fizetési módú megoldásokat dolgoztak már ki. E megoldások némelyikében „elektronikus pénz" van tárolva egy ügyfél pénztárcamoduljában, ahonnan bankjegyek átadása nélkül, közvetlenül fizethet. Ilyen megoldások vannak ismertetve az USA 4,977,595 „Method and Apparatus for Implementing Electronic Cash" és 4,305,059 „Modular Funds Transfer System" szabadalmak leírásában.

A legismertebb ilyen jellegű megoldás egy pénztárcaként működő mágnescsíkos kártya, amely megvásárolható a benne tárolt összegért, és amely benne tárolt összegből kifizetéskor mindig levonódik a kifizetett összeg. Amikor a mágnescsíkos kártyán tárolt összeg elfogyott, a kártya értéktelenné válik és eldobható. Ilyen kártyára példa az ismert telefonkártya. Léteznek újra tölthető memóriakártyák is.

Ezek a fizetőrendszerek azonban egyrészt nem használhatják az ügyfél bankszámláján elhelyezett betét összegét, másrészt papír bankjegyekért vásárolhatók, azaz szorosan ráépülnek a meglévő pénzmegjelenítőkre. Ezekben a megoldásokban a monetáris értéket képviselő pénzmegjelenítők – akár elektronikusak, akár papír formátumúak – anélkül kerülnek kibocsátásra, hogy ellenőrizhető lenne a gazdasági értékfedezetük.

A papírpénzt megkerülő fizetőrendszerek egyike sem eléggé átlátható ahhoz, hogy betöltse egy olyan többcélú elektronikus pénzrendszer szerepét, amely egyrészt alkalmas közvetlen kifizetések teljesítésére, másként egy bankrendszer alapjaként szolgálhat, ahol az elektronikus pénzmegjelenítő eredeti monetáris értékhordozó is lehet, ellenőrzött kibocsátással és egyensúlyban lévő gazdasági értékfedezettel.

Igény van tehát olyan pénz- és fizetőrendszerre, amely egy fizető és egy fizetést elfogadó fél között lehetővé teszi a pénzmozgatást és pénzváltást anélkül, hogy a pénzmozgatásba bankot bevonnának, és amely rendszer megfelelő biztonságot nyújt az egyéni fizetőnek és fizetést elfogadónak manipulálhatóság ellen. Ugyanakkor kívánatos, hogy a rendszer legyen alkalmas nagy szervezetek közötti, nagytömegű és nagy tételszámú pénzmozgatásra is, az EFT rendszerek korlátai nélkül.

A bejelentő US 5 453 601 számú (1991. nov. 15) szabadalmi leírásban olyan EMS elektronikus pénzrendszer (EMS=electronic monetary system) van ismertetve, amely az ismertetett hiányosságok és korlátok többségének kiküszöbölésére alkalmas. Ebben a komplex bankrendszert képező elektronikus pénzrendszerben eredeti monetáris értékű, általánosan használható, elektronikus pénz alkalmazható, amely pénz, hasonlóan a hagyományos idegen pénznemek közötti átváltáshoz, átváltható hagyományos papírpénzre és viszont. Ez a rendszer lehetővé teszi az ellenőrzött és kibocsátott pénzek egyensúlyát biztosító pénzkibocsátást, és a pénzösszegek biztonságos transzferét ügyfelek között, pénzintézetek között és ügyfél-pénzintézet között. Ez a pénzrendszer lehetővé teszi továbbá egynél több pénznem kezelését és átváltását is. Szükség és lehetőség van azonban ezen elektronikus pénzrendszer megbízhatóság és biztonság tekintetében történő továbbfejlesztésére.

Célunk a találmánnyal az ismert megoldások említett hiányosságainak kiküszöbölése és az US 5 453 601 szá-

mú szabadalmi leírás szerinti elektronikus pénz- és fizetési rendszer továbbfejlesztése és gazdagítása, főleg olyan új megoldásokkal, amelyek alkalmasak a hamisítás és duplikálás elleni fokozott védelemre, továbbá amelyek alkalmasak a rendszerben elveszett pénz visszaszerzésére, és amelyek továbbá ügyfélcentrikusak, az ügyfél azonnali fizetéseinek megbízhatósága, biztonsága tekintetében előnyösek.

A feladat találmány szerinti megoldása eljárás pénznemek közötti átváltásra, első idegen pénznemű pénz ügyfél tranzakciós pénztármoduljában tárolt elektronikus megjelenítője és második idegen pénznemű pénz tulajdonos második pénztármoduljában tárolt elektronikus megjelenítője között, amely eljárás során

a) az első tranzakciós pénztármodul és második pénztármodul között rejtjelezéssel biztosított kapcsolatot hozunk létre,

b) az ügyfél az első tranzakciós pénztármodulján beadja az első pénznemben eladni kívánt – első – pénzösszeget,

c) leellenőrizzük, hogy az első tranzakciós pénztármodulban van-e tárolva a tranzakcióhoz szükséges mennyiségű elektronikus pénzmegjelenítő,

d) az első tranzakciós pénztármodulból rejtjelezéssel biztosított kapcsolatban átküldjük az első pénzösszegadatot a második pénztármodulba,

e) a második pénztármodul tulajdonosától átváltási árfolyamot vagy a második pénznemben megadott – második – összegadatot kérünk,

f) leellenőrizzük, hogy a második pénztármodulban van-e tárolva a tranzakcióhoz szükséges mennyiségű elektronikus pénzmegjelenítő,

g) a második pénztármodulból üzenetet küldünk az első, tranzakciós pénztármodulba rejtjelezéssel biztosított kapcsolatban, közölve az átváltási arányt és/vagy a második összeget,

h) az első ügyfél elfogadja az átváltási arányt és/vagy a második összeget,

i) az első tranzakciós pénztármodulból rejtjelezéssel biztosított kapcsolatban átküldjük az első pénzösszegnek megfelelő, első pénznemű elektronikus pénzmegjelenítőt a második pénztármodulba,

j) a második pénztármodulból rejtjelezéssel biztosított kapcsolatban átküldjük a második pénzösszegnek megfelelő, második pénznemű elektronikus pénzmegjelenítőt az első, tranzakciós pénztármodulba,

k) az első, tranzakciós pénztármodul átadja, a második pénztármodul átveszi az első pénznemű, első összegű pénzmegjelenítőt, a második pénztármodul átadja, az első, tranzakciós pénztármodul átveszi a második pénznemű, második összegű pénzmegjelenítőt, előre meg nem határozott sorrendben.

Előnyösen a k) lépésben

a) az első és második pénztármodul számára felosztunk egy közös, bináris értéket, annak első vagy második értékét választva az egyik vagy másik pénztármodul számára,

b) az első, tranzakciós pénztármodul visszafejtést megengedő módon, feltételesen bevezeti bináris értéktől függően vagy az első pénznemű pénzmegjelenítő átadását vagy a második pénznemű pénzmegjelenítő fogadását,

c) az első tranzakciós pénztármodulból üzenetet küldünk a második pénztármodulnak arról, hogy a feltételes tranzakció be van vezetve,

d) a második tranzakciós pénztármodul visszafejtést megengedő módon, feltételesen bevezeti bináris értéktől függően vagy a második pénznemű pénzmegjelenítő átadását vagy az első pénznemű pénzmegjelenítő fogadását,

e) a második tranzakciós pénztármodul, ha a közös véletlenszáma első értékű, kezdeményezi az első tranzakciós pénztármodulnál a tranzakció folytatását,

f) az első tranzakciós pénztármodul válaszul a második tranzakciós pénztármodul üzenetére a feltételes átutalást feltétel nélkülivé teszi, és kezdeményezi befejező protokoll lefuttatását, amelyben az első tranzakciós pénztármodul visszavonhatatlanná teszi első pénznemű átutalását és a második tranzakciós pénztármodul is visszavonhatatlanná teszi második pénznemű átutalását,

g) a második tranzakciós pénztármodul, ha a közös véletlenszáma a második értékű, a feltételes átutalást feltétel nélkülivé teszi, és kezdeményezi befejező protokoll lefuttatását, amelyben a második tranzakciós pénztármodul visszavonhatatlanná teszi második pénznemű átutalását és az első tranzakciós pénztármodul is visszavonhatatlanná teszi az első pénznemű átutalását.

Célszerűen a közös véletlenszámot a rejtjelesen kódolt kapcsolat létrehozása során, kapcsolatkulcsként hozzuk létre.

Előnyösen a két tranzakciós pénztármodul között folyamatban lévő pénzátutalást befejező, egy adott pénztármodul által kezdeményezett protokoll lépései az alábbiak:

a befejező protokollt kezdeményező pénztármodulból „befejezésre kész" üzenetet küldünk a másik pénztármodulba,

a másik pénztármodulból válaszként tudomásul vevő üzenetet küldünk a kezdeményező pénztármodulba,

a kezdeményező pénztármodul visszafejthetetlenné teszi a folyamatban lévő pénztranszfer műveleteit, és így véglegesíti a pénzátutalást,

a másik pénztármodul is visszafejthetetlenné teszi a folyamatban lévő pénztranszfer műveleteit.

Célszerűen a b) lépésben az első ügyfél az átváltandó, első összeget bankjegyenként adja meg.

Az alábbiakban kiviteli példákra vonatkozó rajz alapján részletesen ismertetjük a találmány lényegét. A rajzon az

1A. ábra EMS elektronikus pénzrendszer hálózati szerkezete, tömbvázlatban, a

1B. ábra biztonságiszerver-hálózat tömbvázlata, a

2. ábra EMS elektronikus pénzrendszer biztonsági hálózatának szerkezete, tömbvázlat, a

3A. ábra biztonsági szerver funkcionális egységei, tömbvázlat, a

3B. ábra hálózati szerver funkcionális egységei, tömbvázlat, a

4A. ábra ügyfélkiszolgáló modul funkcionális egységei, tömbvázlat, a
4B. ábra elsődleges biztonsági szerver funkcionális egységei, tömbvázlat, az
5. ábra hálózatra bejelentkezés kapcsolatrendszere, tömbvázlata, a
6A–6K. ábra hálózatra bejelentkezés protokoll folyamatábrája, a
7A–7E. ábra kapcsolat létesítése protokoll folyamatábrája, a
8A–8B. ábra bankjegy-transzfer protokoll folyamatábrája, a
9A–9D. ábra pénznemek közötti átváltás protokolljának folyamatábrája, a
10. ábra kapcsolatlezáró protokoll folyamatábrája, a
11A–11B. ábra tranzakció megszakítása protokoll folyamatábrája, a
12A–12C. ábra POS (point of scale) fizetés protokolljának folyamatábrája, a
13A–13B. ábra kredit megújítása kibocsátó banknál protokoll folyamatábrája, a
14. ábra kreditkérés kezdeményező protokoll folyamatábrája, a
15A–15B. ábra kreditkérés protokoll folyamatábrája, a
16. ábra elektronikus bankjegy transzfereinek története, a
17. ábra a 16. ábra szerinti transzferek rekord fája, a
18A–18C. ábra pénztármodul bankszámlához hozzáférése protokoll folyamatábrája, a
19A–19C. ábra pénztármodul bankszámlához hozzáférése újraérvényesítésének folyamatábrája, a
20. ábra bankszámla aktiválásának folyamatábrája, a
21A–21B. ábra elveszett pénzkövetelés készítésének folyamatábrája, a
22A–22E. ábra elveszett pénz visszakövetelése protokoll folyamatábrája.

A találmány szerinti megoldás ismertetését a korábbi P 9302008 bejelentési számú magyar szabadalmi bejelentésünkben US 5453601 1991. nov. 15 szabadalmi leírásban ismertetettekre, mint referenciára alapozzuk, amely bejelentés szerinti elektronikus pénzrendszer és eljárások továbbfejlesztésére vonatkozik a jelen szabadalmi bejelentésünk. A továbbfejlesztés eredményei többek között az alábbiak: biztonság további javítása, pénznemek közötti átváltás (F/X) és transzfer bankjegyek tranzakciós folyamatának javítása, elveszett pénz visszakövetelésének, tranzakciós modul bankszámlához történő hozzáférése javítása, POS fizetés és kreditmegújítás folyamatának új megoldása.

Biztonság

Egy pénzrendszer hatásos biztonsági rendszerének van három fő jellemzője: csalások, illetéktelen beavatkozások megakadályozása, felfedése és nyilvántartása, tárolása. Az ismertetett EMS elektronikus pénzrendszer célja szerint mindhárom jellemzőnek megfelelően van kialakítva.

A csalások, illetéktelen beavatkozások megakadályozására szimmetrikus és aszimmetrikus kulccsal történő rejtjelezést, rejtjelezéssel védett adatátvitelt alkalmazunk. Nincs olyan üzenet, ami rejtjelezés nélkül továbbítunk. A rendszer feltörés ellen védett fizikai felépítésű moduljai ugyancsak rejtjellel kódolt bizonylattal vannak ellátva.

A csalások, illetéktelen beavatkozások felfedésére bankjegy életpálya feljegyző és visszakereső eljárásokat alkalmazunk. A bankjegyek bizonylatának lejárata van, az elektronikus bankjegyek, illetve pénzmegjelenítők rendszeres frissítésre szorulnak, a lejárt bankjegyek nem forgalomképesek. Az elektronikus bankjegyek frissítése megtörténik mindegyik banki transzfer során, amikor is új lejárati dátumot kapnak.

Azok a pénztármodulok, amelyekhez duplikált vagy hamis bankjegy forgalomba kerülése kapcsolódik, automatikusan kizáródnak a pénzforgalomból és azonosítójuk „rossz azonosító" listára kerül. Azok a bankjegyek, amelyek átmentek ilyen modulon, forgalomképtelenné válnak. A duplikálás vagy hamisítás miatt forgalomképtelenné vált bankjegyek transzferadatait a rendszerben megőrizzük. Az EMS pénzrendszer súlyosabb biztonsági probléma felfedése esetén globálisan újrabizonylatolható. Ez azt jelenti, hogy a rendszer mindegyik egysége új bizonylatot kap, és azok, az ügyfelek birtokában lévő tranzakciós pénztármodulok, amelyek az adott időpontban nincsenek bekapcsolva a hálózatba, az első, következő bejelentkezésükkor kapnak új bizonylatot.

Az alábbi listába foglaltuk azokat a javításokat, amelyek az információk telefonlehallgatóktól való eltakarására szolgálnak a modulok közötti forgalomban. (A rendszerben minden információs üzenet, modul azonosító és közös kulcs, órajelhez van szinkronizálva):

1) a hálózatra bejelentkezést biztosítjuk úgy, hogy senki ne csaphassa be a pénztármodult vagy avatkozhasson be a műveleteibe kódolatlan üzenettel (részletes ismertetés az 5. ábra alapján),
2) eljárást dolgoztunk ki a biztonsági szerver, pénzformátum-generátor és banki pénztármodul azonosítóinak összerendelésére (lásd később: modul számozási séma).

Ezeket az azonosítókat ellenőrizzük az alábbi módon:

a) kapcsolat létesítésekor (lásd 7A–7E. ábrák),
b) bankjegyek továbbításánál a bankjegyhez fűzött transzferrekordok ellenőrzésével (8A–8B. ábra).
3) kétlépcsős biztonságiszerver-hierarchiát (és biztonsági hálózatot) alkalmazunk, ahol mindegyik modul bizonylata tartalmazza az elsődleges biztonsági szerver (SS) és egy rendes biztonsági szerver (NS) közös kulcsát, amely rendes biztonsági szerver bizonylatolja az összes többi modult.
4) a transzfer bankjegyeket leellenőrizzük minden elfogadás vagy átváltás előtt, hogy nincs-e rajta olyan azonosító adat, amely a rossz azonosítók listáján szerepel, vagy nincs-e duplikálva (8A–8B. ábrák),
5) egy biztonsági szerver egyedi kulcsaival kódolunk minden bizonylatot (lásd bizonylat szerkezete és értékelés),
6) a közös kulcsok hosszát dinamikusan változtatjuk (6A–6K. ábra),

7) a befejező protokollt úgy változtattuk, hogy a bankjegyek duplikálása lehetetlenné váljék (10. ábra),
8) pénznemek közötti átváltás (F/X) tökéletesítése, hogy egyik fél se tarthassa vissza egy megkapott pénz ellenértékét (9A–9D. ábra),
9) megszakításról log információt készítünk, ha a fizető teljesít és kilép a kapcsolatból, amíg a fizetés fogadója megszakít (11A–11B. ábra),
10) szükség esetén alkalmazható globális újrabizonylatolás (lásd biztonsági hálózat és (6A–6K. ábra).

A fenti lista szerinti intézkedések rávilágítanak a jelen bejelentésben foglalt, biztonságnövelő megoldások hatására az elektronikus pénzrendszerben. Ezeket és más új intézkedéseket bővebben tárgyalunk az alábbiakban:

Biztonsági hierarchia

A találmány szerinti kialakításban az elektronikus pénzrendszer hálózatához kétlépcsős biztonságiszerver-rendszer tartozik. Az 1A. ábra szerint van egy vagy több elsődleges 1182 biztonsági szerver (PSS) és egy vagy több rendes 1184 biztonsági szerver (SS). Az elsődleges 1182 biztonsági szerver (csak másik elsődleges 1182 biztonsági szerverrel és) a rendes 1884 biztonsági szerverekkel képez biztonsági hálózatot (1B. ábra). Az elsődleges 1182 biztonsági szerver bizonylatolja a rendes 1184 biztonsági szervereket, a rendes 1184 biztonsági szerverek bizonylatolják a pénzrendszer egyéb moduljait (M), mint az egy vagy több tranzakciós 1186 pénztármodult (MM), banki 1188 pénztármodult (TM), 1190 pénzformátumgenerátort (MG) és 1192 ügyfélkiszolgáló modulokat (CSM).

Az elsődleges 1182 biztonsági szerverek, egymással egy biztonsági 1194 helyi hálózaton (LAN) át, rendes 1184 biztonsági szerverekkel egy a helyi hálózattal biztonsági kapun át összekötött, nagyobb biztonsági 1196 hálózaton (SN) át állnak kapcsolatban (2. ábra), amely nagyobb biztonsági 1196 hálózatra már csak a rendes 1184 biztonsági szerverek vannak közvetlenül csatlakoztatva. Mindegyik biztonsági szerver feltörés ellen fizikailag védetten van kialakítva. A rendes 1184 biztonsági szerverek másrészt az elektronikus pénzrendszer adatátviteli EMS 1198 hálózatára vannak csatlakoztatva, amely EMS 1198 hálózatra egy vagy több bank 1200 helyi hálózata csatlakozik. A biztonsági szerverek olyan megoldásúak, hogy lehetővé teszik minden más modullal létrejött kapcsolatukban azok érvényesítését, illetve érvényességük ellenőrzését.

Csak a 1184 biztonsági szervereknek és a különböző moduloknak van bizonylatuk, amely bizonylatok többek között tartalmazzák az elsődleges 1182 biztonsági szerver közös kulcsát. Kétféle bizonylat létezik: biztonságiszerver-bizonylat és modulbizonylat.

A bizonylatok szerkezete és érvényessége:

☒

Biztonságiszerver-bizonylat:

Cert(SS)=E_{PSS}[SS(id)2 SS(PK)2 lejárat 2 Φ_{PSS} (X)] 2 [PSS(id) XOR C]

Modulszerver-bizonylat:

Cert(M)=E_{SS} [M(id)2 M(PK) 2 lejárat 2 2 Φ_{SS}(Y)] 2 Cert(SS)

A bizonylat érvényét vizsgáló protokoll az alábbi:

1) biztonságiszerver-bizonylat értékelése:
   a) PSS(id)=[PSS(id)XOR C] XOR C
   b) D_{PSS} (E_{PSS}(X 2 Φ_{PSS} (X)))=2 Φ_{PSS} (X)
   c) modulszámozás-séma alapján ellenőrizzük SS(id) autentikusságát
   d) ellenőrizzük a lejárati dátum érvényét
   e) ellenőrizzük, hogy D_{PSS} (Φ_{PSS} (X))=h(X)
2) modulbizonylat értékelése:
   a) értékeljük a biztonsági szerver Cert(SS) bizonylatát
   b) D_{SS} (E_{SS}(Y 2 Φ_{SS}(Y)))=Y 2 Φ_{SS} (Y)
   c) modulszámozás-séma alapján ellenőrizzük M(id) autentikusságát
   d) ellenőrizzük a lejárati dátum érvényét
   e) ellenőrizzük, hogy D_{SS} Φ_{SS} (Y))=h(Y)

ahol PSS elsődleges biztonsági szerver
SS biztonsági szerver
M modul
2 láncolás
id azonosító szám
h Hash függvény
C konstans véletlen szám, közös minden modul számára
PK közös kulcs (a közös kulcs hosszának megadásával)
Φ digitális szignó=E×h
Cert bizonylat
E algoritmus, kódoláshoz és szignó készítéshez használt egyedi kulccsal
D algoritmus, kódoláshoz és szignó ellenőrzéshez használt közös kulccsal
E és D használható továbbá biztonsági kódolásra és dekódolásra, más alkalmazásokban.

Modulszámozás-séma

Az elsődleges 1182 biztonsági szervereknek, a rendes 1184 biztonsági szervereknek, a banki 1188 pénztármoduloknak, a 1190 pénzgenerátoroknak, a 1192 ügyfélkiszolgáló moduloknak és a tranzakciós 1186 pénztármoduloknak egyedi azonosító (id) számuk van, amelyekkel egymástól megkülönböztethetők és azonosíthatók. Ehhez egy biztonságtechnikailag védett folyamatban egy 48 bites *p* prímszámot és ennek 'a' modulo *p* primitív gyökét (ahol a^n □1(p) generáljuk minden egyes 1#n < p-1 értékre. 'a' és *p* be van töltve a rendszer mindegyik moduljába és ott védetten tárolva van. A betöltés már a modul gyártása során megtörténik.

A modulszámozás-séma az alábbiak szerint működik:

ha a^n / m(p) és
(1) 1#m#99 999, akkor n egy elsődleges biztonsági szerver id azonosítója
(2) 100 000 #m# 999 999, akkor n egy biztonsági szerver azonosítója,
(3) 1 000 000 #m# 6 999 999, akkor n egy banki (jegybanki) pénztármodul id azonosítója,

(4) 7 000 000 #m# 9 999 999, akkor n egy pénzformátum-generátor id azonosítója,
(5) 10 000 000 #m# 11 999 999, akkor n egy ügyfélkiszolgáló modul azonosítója,
(6) m ∃ 12 000 000, akkor n egy tranzakciós pénztármodul azonosítója.

Amikor egy modulban vagy szerverben egy bizonylat ellenőrzése történik, ellenőrizzük az n azonosító szám (például M(id), SS(id), PSS(id) autentikusságát is, kiszámítva az $a^n=m(p)$ értéket, majd ellenőrizve, hogy *m* a megfelelő tartományba esik-e.

Biztonsági hálózat

A 2. ábra szerinti 1196 biztonsági hálózat és biztonsági 1194 helyi hálózat (LAN) köti össze a 1184 biztonsági szervereket az elsődleges 1182 biztonsági szerverrel. A 1184 biztonsági szerverek először már a gyártás során bizonylatolják a pénztármodulokat és az 1192 ügyfélkiszolgáló modulokat. Ennek érdekében a megfelelő 1184 biztonsági szerverek összekapcsolhatók egy modulgyártó 1202 helyi hálózattal. A modulgyártó 1202 helyi hálózaton át a 1184 biztonsági szerver olyan biztonsági információkat továbbít az épp elkészült modulokba, mint a rossz azonosítók listája, az elsődleges biztonsági szerverek listája és ezek közös kulcsai. A rossz azonosítók (id-k) listája tartalmazza mindazon pénztármodulok, ügyfélkiszolgáló modulok és biztonsági szerverek azonosító számait, amelyek valamilyen okból ki vannak zárva a tranzakciós forgalmazásból. Az ilyen modulok újrabizonylatolhatók, aminek folyamatát a későbbiekben ismertetjük.

A 1184 biztonsági szervereket először, a gyártásuk során, elsődleges 1182 biztonsági szerver bizonylatolja. Ennek érdekében a megfelelő elsődleges 1182 biztonsági szerverek összekapcsolhatók egy biztonságiszerver-gyártó 1204 helyi hálózattal. A biztonságiszerver-gyártó 1204 helyi hálózaton át a 1182 biztonsági szerver biztonsági információkat továbbít az épp elkészült biztonsági szerverekbe. Az 1B. ábra szerint ilyen információk a biztonsági hálózat rejtjel-kulcsa, a 1182, 1884 biztonsági szerverek, modulok közös kulcsának hossza, a rossz azonosítók listája, az elsődleges biztonsági szerver egyedi kulcsa, a globális újrabizonylatoláshoz szükséges információ. A 1184 biztonsági szerverek ezekre a biztonsági információkra alapozzák hitelesítő funkcióikat, ezeket az információkat adják tovább a bizonylatolandó moduloknak.

A 1184 biztonsági szerverek látják el az EMS 1198 hálózat és bankok 1200 helyi hálózatának (LAN) biztonsági szolgálatát, főként a különböző modulok hálózatra bejelentkezése során adott, friss biztonsági információk alapján. Ezeket a friss információkat a 1184 biztonsági szerverek a biztonsági 1196 hálózaton át az elsődleges 1182 biztonsági szerverektől kapják.

A tranzakciós 1186 pénztármodulok 1206 hálózati szervereken (NS) át az EMS 1198 hálózatra kapcsolódhatnak. A résztvevő bankok a banki (1188) pénztármoduljaikkal és esetleg a 1190 pénzformátum-generátoraikkal kapcsolódnak a bank 1200 helyi hálózatára.

A biztonsági 1196 hálózaton minden összeköttetés (kapcsolat) kódolással titkosítva van. Az elsődleges és rendes 1182, 1184 biztonsági szervereknek továbbá közös szimmetrikus kulcsuk (biztonsági hálózat rejtjelező kódkulcsa) van. Ezt a közös, szimmetrikus kulcsot az elsődleges 1182 biztonsági szerver, meghatározott időközönként, a közös kulcsának változtatásával, periodikusan változtatja.

A rossz azonosítók listáját az elsődleges 1182 biztonsági szerver őrzi. A lista adatai a különböző résztvevő bankokkal, jognak érvényt szerző hatóságokkal és ügyfelekkel, a rendszeren belül létrejött kapcsolatokból gyűlnek össze.

Rendszeresen változtatható a 1182, 1184 biztonsági szerverek és modulok közös kulcsának hossza is. A kulcshossz általában hosszabbodik a változtatással, mert minél hosszabb a közös kulcs, annál magasabb az alkalmazásától függő biztonság szintje. Az új közös kulcshossz adatot elsődleges 1182 biztonsági szerverekhez egy erre kijelölt elsődleges 1182 biztonsági szerver továbbítja. Az elsődleges 1182 biztonsági szerverek a 1184 biztonsági szerverekhez ezt az új közös kulcshossz adatot akkor továbbítják, amikor amúgy is kapcsolatot létesítenének velük, például frissített rossz azonosítók listájának küldésekor vagy újrabizonylatoláskor. Ha veszélyes biztonságtörés következett be, egy elsődleges 1182 biztonsági szerver globális újrabizonylatolást kezdeményez.

Az elsődleges 1182 biztonsági szerverek közös kulcsának hossza nem változó. Viszont az elsődleges 1182 biztonsági szerverek egy időtáblázat szerint aktívak vagy inaktívak, tehát mintegy váltják egymást. Az új szervereknek általában hosszabb a közös kulcsa, mint a korábbiaknak, ami összefügg a lebonyolított tranzakciók nagyobb számával. Az aktív elsődleges 1182 biztonsági szerverek közös kulcsairól egy lista készül, amely listát elsődleges 1182 biztonsági szerver készíti és szignálja digitálisan a saját egyedi kulcsával. Az így elkészített listát megkapja mindegyik másik 1182 biztonsági szerver.

A 3A ábrán egy 1184 biztonsági szerver funkcionális egységei vannak feltüntetve. A 1184 biztonsági szerver egy 1208 külső interfészen át kapcsolódik hálózatra. A hálózati kapcsolatában egy biztonsági 1210 kapcsolatmenedzser ellenőrzi a kapcsolat biztonsági paramétereit. Egy 1212 hálózati bejelentkező funkció végzi el a biztonságos és védett hálózati bejelentkezés műveleteit. Egy 1214 bizonylatkészítő funkció készít bizonylatot minden 1186, 1188 pénztármodul számára (az elsődleges 1182 biztonsági szerverben ez a funkció a 1182 biztonsági szerverek számára készít bizonylatot). Egy 1218 bizonylatkulcs elosztó terjeszti a pénztármodulok között a bizonylatoló szerver listáját az érvényes elsődleges biztonsági szerverek közös kulcsairól (az elsődleges 1182 biztonsági szerver terjesztheti továbbá a globális újrabizonylatoló üzenetet). Egy 1220 rossz azonosító lista ellenőrző funkció ellenőrzi és frissíti a rossz azonosítók listáját. Egy 1222 dátum/idő szinkronizáló funkció igazítja a rendszeridőhöz az egyes pénztármodulok óra/időzítőjét Egy 1224 óra/időzítő és 1226 rejtjelező

funkciók azonosak a 1186, 1188 pénztármodulok hasonló funkcióival.

A 3B. ábrán egy 1206 hálózati szerver (NS) funkcionális egységei vannak feltüntetve. A 1206 hálózati szerver egy 1228 külső interfészen át kapcsolódik hálózatra. A hálózati kapcsolatában egy pénztármodul 1230 kapcsolatmenedzser vezérli a kapcsolatot a modulok egymás közötti és biztonsági modullal létrejövő kapcsolatában. Egy 1232 hálózati bejelentkező funkció végzi el a biztonságos és védett hálózati bejelentkezés műveleteit. Egy 1234 útvonalvezérlő funkció útvonaltérkép és irányító feladatokat lát el és ellenőrzi az útvonalüzeneteket a hálózatra bejelentkezés során és a létrejött kapcsolat alatt. Egy 1236 banki szolgáltatástár funkció információt szolgáltat a résztvevő bankok lehetséges szolgáltatásairól. Egy 1238 rejtjelező funkció lát el egy1240 szimmetrikuskulcs-adó funkciót és egy 1242 véletlenszám-generátor funkciót. A 1240 szimmetrikus kulcs funkcióban kódolja a 1206 hálózati szerver és a hálózatba bejelentkező modulok közötti üzeneteket, továbbá a 1206 hálózati szerver és 1184 biztonsági szerverek közötti üzeneteket. A 1242 véletlenszám-generátor funkció véletlen számot képez a titkosító kódhoz és a kiértékelő üzenetekhez.

A találmány szerint, a rendszerben előnyösen alkalmazunk további biztonságot és flexibilitást növelő, 1192 ügyfélkiszolgáló modult (CSM) is. A 1192 ügyfélkiszolgáló modul (CSM) egy feltörés ellen fizikailag védett eszköz, amely főként bankszámlafejelések (profilok) kialakítására és frissítésére alkalmas. A 1192 ügyfélkiszolgáló modulnak is egyedi bizonylata van, hasonlóan a 1186, 1188 pénztármodulokéhoz és a 1182, 1184 biztonsági szerverekéhez. A 1192 ügyfélkiszolgáló modul biztonságos kapcsolatot tud létesíteni más modulokkal (vagy 1182, 1184 biztonsági szerverekkel is). A 1192 ügyfélkiszolgáló modulnak szüksége van egy gazdára, amelyen át kapcsolatot létesíthet egy ügyféllel vagy egy banki megbízottal, továbbá az on-line bankrendszerrel.

A 1192 ügyfélkiszolgáló modulnak (4A. ábra) két alapfunkciója van: Egyrészt a 1192 ügyfélkiszolgáló modul bankszámla-fejelést készít, aminek segítségével egy 1186, 1188 pénztármodul kapcsolatot létesíthet egy adott bankszámlával, megújíthatja kapcsolatát a bankszámlával, értékelheti a bankszámlafejeléseket. Ezeket a folyamatokat (tranzakciókat) a későbbiekben a 18A-20 ábrák kapcsán még részletesebben ismertetni fogjuk. Másrészt a 1192 ügyfélkiszolgáló modul elveszettpénz-visszakövetelést készíthet a gazda utasítására, illetve a banki megbízott számára. Ezt a folyamatot a későbbiekben a 21A–21B., 22A–22E. ábrák alapján ismertetjük részletesen. A 1192 ügyfélkiszolgáló modul hasonló biztonsági funkciókat lát el, mint egy 1186, 1188 pénztármodul, és azonosítására egy speciális számtartományból választott azonosító szolgál (lásd: modulszámozásséma). Az, hogy a fent említett funkciókat a 1192 ügyfélkiszolgáló modul látja el, nagyban egyszerűsíti a számlaszám-azonosítás folyamatát a banki pénztármodulban.

Egy 1192 ügyfélkiszolgáló modult tartalmazó EMS pénzrendszer 1198 hálózatban a bankszámlafejtés az alábbiak szerint leegyszerűsödik:

lejárati dátum || *M(id)* || *B(id)* || *LA* || $\sigma_{csm}(X)$ || *Cert (CSM)*

X

ahol M(id) modulazonosító

B(id) bankazonosító

LA bankszámlaszámok listája számlatípus-megadással (hitel vagy depozit)

σ_{csm} ügyfélkiszolgáló modul szignója

Cert(CSM) ügyfélkiszolgáló modul bizonylata

|| láncolás (kaszkád).

A bankszámlafejelés értékelésének folyamatát a későbbiekben, a 20. ábra alapján ismertetjük.

A 4A. ábrán egy 1192 ügyfélkiszolgáló modul (CSM) funkcionális egységei vannak feltüntetve. A 1192 ügyfélkiszolgáló modul egy 3000 külső interfészen át kerülhet adatátviteli kapcsolatba a gazda 1192 ügyfélkiszolgáló modulon belül más műveletvégző és adatátvivő egységekkel. Egy 3001 kapcsolatmenedzser vezérli a 1192 ügyfélkiszolgáló modul kapcsolattartását, ez fejezi be sikeresen vagy szakítja meg a kapcsolatot mind az ügyfél, mind a banki megbízott irányában. Egy 3002 számlaprofil-készítő az ügyféltől kapott számlainformációból bankszámla-fejelést készít, ez teszi lehetővé, hogy egy 1186, 1188 pénztármodul hozzáférjen az ügyfél különböző bankszámláihoz. Egy közös kulcs funkció hitelesíti és szignálja a bankszámla-fejelést. Minthogy a 1192 ügyfélkiszolgáló modul belül van egy gazda 1192 ügyfélkiszolgáló modulon, csak a gazdán át tud kapcsolatot létesíteni egy banki megbízottal és az on-line bankrendszerrel, egy 3006 funkció-megosztó közvetít a 1192 ügyfélkiszolgáló modul funkciók és a gazda funkciók között. Egy 3008 bankjegykereső funkció kezeli az ügyfél elveszettpénz-visszakövetelését, amit a 1192 ügyfélkiszolgáló modul értékel és továbbít a bankjegyeket kibocsátó bankokhoz. Egy 3004 biztonságőr-funkció kezeli a kompromittált 1186, 1188 pénztármodulok listáját, bizonylatot kér, helyesbíti az órákat, menedzseli új digitális kulcsok képzését. Egy 3012 óra/időzítő és 3010 rejtjelező funkciók megegyeznek a 1186, 1188 pénztármodulok hasonló funkcióival.

A 4B. ábrán elsődleges 1182 biztonsági szerver funkcionális egységei vannak tömbvázlatszerűen ábrázolva. Egy 3020 külső interfész biztosít kapcsolatot a biztonsági hálózattal. Egy 3022 kapcsolatmenedzser vezérli a 1182, 1186 biztonsági szerverek közötti kapcsolatok biztonsági műveleteit, amelyeket megbízhatatlanokként kezel. Egy 3024 bizonylatkészítő funkcióban mindegyik 1182, 1184 biztonsági szerver számára bizonylat készül. Egy 3026 bizonylatkulcs-elosztó osztja ki az érvényes elsődleges biztonsági szerverek közös kulcs listáját a 1182, 1184 biztonsági szervereknek. Egy 3032 biztonságihálózatkulcs-elosztó funkció kezeli és osztja ki a biztonságihálózat-kulcsokat az elsődleges és a rendes biztonsági szerverek között. Egy 3030 globális bizonylatoló funkció határozza meg, szükség van-e globális újrabizonylatolásra és elindítja a globális újrabi-

zonylatolást, ha arra szükség van (nagy biztonsági hiba esetén). Egy 3028 rossz azonosító lista ellenőrző funkció ellenőrzi és kiosztja a rossz azonosító listát. A 3034 óra/időzítő és 3036 rejtjelező funkciók megegyeznek a másféle modulok hasonló funkcióival.

Bejelentkezés hálózatra

Egy hálózatra történő bejelentkezés során létrejövő kapcsolatok az 5. ábrán tömbvázlatszerűen vannak szemléltetve. A „bejelentkezés hálózatra" protokoll akkor fut le, ha egy 1243 modul rá kíván kapcsolódni az EMS 1198 hálózatra például újrabizonylatolás, depozit, pénzkivétel vagy más okból. A 1243 modul lehet például tranzakciós 1186 pénztármodul, pénzkibocsátó banki 1188 pénztármodul, 1188 pénzformátum-generátor vagy 1192 ügyfélkiszolgáló modul. A „bejelentkezés hálózatra" protokoll szerint az alábbi kapcsolatok és műveletek valósulnak meg: a) Kapcsolat létesül a 1243 modul és a 1206 hálózati szerver között. b) A 1243 modul bizonylatát a 1206 hálózati szerverhez továbbítjuk. c) A 1206 hálózati szerver V értékelő véletlen számot és ehhez K kulcsot generál, amely V értékelő véletlen számot és K kulcsot egy 1184 biztonsági szerverhez továbbít (NS/SS kapcsolatkulccsal kódolva). d) A 1243 modul és a 1184 biztonsági szerver között (MM/SS kapcsolatkulccsal) védett adatátviteli kapcsolatot létesítünk. e) A 1184 biztonsági szerver dátum/idő adatot, frissítő rossz azonosító listát és elsődleges 1182 biztonsági szerverek közös kulcs listáját, a közös kulcsok hosszát – és amennyiben szükséges – globális újrabizonylatoló információt és újrabizonylatolt 1243 modulbizonylatot ad ebben a kapcsolatban. f) A 1243 modullal a sikeres kapcsolatot lezárjuk a V véletlen szám és K kulcs megküldésével. g) A V véletlen számot kódoljuk a K kulccsal és így küldjük meg a 1206 hálózati szervernek. h) A 1206 hálózati szerver a bejelentkezést tudomásul vevő üzenetet küld a 1243 modulnak. i) A 1243 modul informálja a 1206 hálózati szervert az általa elérni kívánt célállomásról (ha ilyen van). j) A 1206 hálózati szerver létrehozza a kapcsolatot a 1243 modul és a célállomás modul között.

A „bejelentkezés hálózatra" protokoll úgy van kialakítva, hogy senki se csaphassa be a 1243 modult vagy nyerhessen ki belőle információt a kódolás ismerete nélkül.

A 6. A–K. ábrán a „bejelentkezés hálózatra" protokoll részletes folyamatábrája van feltüntetve. Eszerint *A* bejelentkező a 1244 lépésben kapcsolatot létesít az EMS 1198 hálózattal. Az *A* biztonságőr a bizonylatát megküldi 1206 biztonsági szervernek egy 1246 lépésben, 1206 hálózati szerver hálózati bejelentkezője fogadja a bizonylatot a 1248 lépésben. Hálózati szerver véletlenszám-generátora V értékelő véletlen számot és K kulcsot generál a 1250 lépésben. A 1206 hálózati szerver szimmetrikuskulcs-adója kódolja a V véletlen számot és K kulcsot egy NS/SS kapcsolatkulccsal a 1252 lépésben. Az NS/SS kapcsolatkulcsok helyi szimmetrikus kulcsok, amelyek a bejelentkezés folyamatában részt vevő 1206 hálózati szerverekben és a 1184 biztonsági szerverekben tárolva vannak. A 1254–1258 lépésekben a 1206 hálózati szerver hálózati bejelentkezője megküldi a bizonylatot továbbá a V véletlen számot és K kulcsot a 1184 biztonsági szervernek, ahol a 1184 biztonsági szerver 1212 hálózat bejelentkezője veszi az üzenetet és a 1184 biztonsági szerver szimmetrikus kulcsával kódolja az üzenetet. Részletesebben: a 1254 lépésben a 1206 hálózati szerver a V véletlen számot és K kulcsot a 1184 biztonsági szerverhez továbbítja, a 1256 lépésben a 1184 biztonsági szerver hálózati bejelentkezője veszi a V véletlen számot és K kulcsot, a 1258 lépésben a 1184 biztonsági szerver szimmetrikuskulcs-adója dekódolja a V véletlen számot és K kulcsot. A 1260–1264 lépésekben a 1184 biztonsági szerver 1212 hálózati bejelentkezője tárolja a V véletlen számot és K kulcsot, majd a modul bizonylatát értékelésre a 1184 biztonsági szerver között kulcs funkciójához továbbítja. Részletesebben: a 1260 lépésben a 1184 biztonsági szerver 1212 hálózati bejelentkezője eltárolja a V véletlen számot és K kulcsot, és bizonylatot küld értékelésre, a 1262 lépésben a 1184 biztonsági szerver közös kulcs adója értékeli a bizonylatot, a lejárat kivételével, a 1264 lépésben megállapítja a bizonylatról, hogy az érvényes-e vagy sem. A 1184 biztonsági szerver közös kulcs adó funkciója azért nem értékeli a lejárat dátumának érvényét, hogy nyitva hagyja egy esetleges újrabizonylatolás lehetőségét.

Ha a 1243 modul bizonylata nem érvényes, akkor a 1184 biztonsági szerver hálózati bejelentkezője a bejelentkezést megtagadó üzenetet készít a 1206 hálózati szerver és a 1243 modul számára, a 1266 lépésben. A 1184 biztonsági szerver közös kulcs adó funkciója kódolja a 1243 modulhoz menő üzenetet a 1243 modul közös kulcsával és a 1184 biztonsági szerver 1210 kapcsolatmenedzsere az üzenetet a hálózati szerverhez küldi a 1268–1270 lépésekben. Részletesebben: a 1268 lépésben a 1184 biztonsági szerver közös kulcs adója kódolja az üzenetet, a 1270 lépésben a 1184 biztonsági szerver kapcsolatmenedzsere a 1206 hálózati szerverhez küldi a kódolt üzenetet. A 1272 lépésben a 1206 hálózati szerver 1212 hálózati bejelentkezője veszi az üzenetet, és megjegyzi, hogy a kapcsolat meg van tagadva. A kódolt üzenetet ezután továbbküldi a 1243 modulhoz és a 1206 hálózati szerver megszünteti a kapcsolatot. Az *A* kapcsolatmenedzsere a 1274 lépésben veszi az üzenetet, az *A* közös kulcs adó a 1276 lépésben dekódolja az üzenetet, az *A* kapcsolat menedzser a 1278 lépésben megjegyzi, hogy a bejelentkezést megtagadták (1274–1278 lépések). Ha a bejelentkezést kérő modul egy tranzakciós 1186 pénztármodul volt (1280 lépés), akkor *A* ügyfél számára a modul kijelzi, hogy a kapcsolat megtagadva (1182 lépés). Ha a 1280 lépésben az derül ki, hogy a bejelentkezést kérő nem tranzakciós 1186 pénztármodul volt, akkor a 1284 lépésben *A* bankjához megy a kapcsolatmegtagadó üzenet.

Ha viszont a 1243 modul bizonylata érvényes, akkor a 1184 biztonsági szerver rossz azonosító lista ellenőrzője megvizsgálja a 1243 modul azonosítóját, hogy nincse az a listán (1286 lépés) és megállapítja, hogy igen, vagy nem (1288 lépés). Ha az azonosító rossz azonosítók listáján szerepel, a 1198 hálózathoz hozzáférést megtagadja a 1184 biztonsági szerver. Ha az azonosító nem

szerepel a rossz azonosítók listáján, akkor a 1184 biztonsági szerver 1242 véletlenszám-generátora R véletlen számot és értékelő üzenetet generál a 1290 lépésben. A 1184 biztonsági szerver 1212 hálózati bejelentkezője a 1292 lépésben az R véletlen számot és az üzenetet egy üzenetbe foglalja, amely üzenetet a 1184 biztonsági szerver közös kulcs adója a 1594 lépésben *A* közös kulcsával kódolja, a kódolt üzenetet a bizonylattal összetűzi, és *A*-hoz küldi. A 1296 lépésben *A* közös kulcs adó dekódolja az üzenetet, a 1298 lépésben megvizsgálja a biztonsági szerver bizonylatának érvényét.

Az esetben, ha a bizonylat érvénytelen, *A* megjegyzi a kapcsolat megszakítását és vagy az ügyfelet, vagy a bankot informálja (1304–1306 lépések). Részletesebben: *A* kapcsolatmenedzser megjegyzi: a kapcsolat megszakad (1300 lépés), egy 1302 lépésben megvizsgáljuk, hogy van-e eközben pénzügyi tranzakció folyamatban. Ha igen, akkor egy 1304 lépésben *A* ügyfelet informáljuk a kapcsolat megszakadásáról, ha nincs tranzakció folyamatban, akkor *A* ügyfél számlavezető bankját (1306 lépés). Az esetben, ha a bizonylat érvényes, *A* biztonságőr ellenőrzi: a 1184 biztonsági szerver azonosítója nincs-e a rossz azonosítók listáján (1308, 1310 lépés). Ha a 1184 biztonsági szerver azonosítója rajta van a rossz azonosítók listáján, visszatérünk az 1300 lépéshez, amelyben *A* kapcsolatmenedzser megjegyzi: a kapcsolat megszakad és az 1300–1306 lépéseket lefuttatjuk. Ha a 1184 biztonsági szerver azonosítója nincs rajta a rossz azonosítók listáján, akkor az *A* véletlenszám-generátor R(A) véletlen számot generál (1312 lépés) és *A* biztonságőr MM/SS kapcsolatkulcsot képez R(A) XOR R képlet alkalmazásával, majd tárolja az így képzett kapcsolatkulcsot, továbbá érvényesítő üzenetből és az R(A) véletlen számból üzenetet állít össze (1314 lépés). *A* közös kulcs adó az üzenetet kódolja a 1184 biztonsági szerver közös kulcsával a 1316 lépésben. *A* kapcsolatmenedzser az üzenetet 1184 biztonsági szervernek küldi (1318 lépés), a 1184 biztonsági szerver 1212 hálózati bejelentkezője veszi az üzenetet (1320 lépés), a 1184 biztonsági szerver közös kulcs adója dekódolja a vett üzenetet (1322 lépés). A 1184 biztonsági szerver 1212 hálózati bejelentkezője ellenőrzi az üzenet érvényét, tehát azt, hogy az érvényesítő üzenet az-e, amely épp most készült (1324–1326 lépések). Ha az ellenőrzés eredménye a 1326 lépésben *nem,* akkor a 1184 biztonsági szerver megtagadja a hozzáférést a 1198 hálózathoz egy a 1266 lépéssel kezdődő lépéssorban. Ha az érvényesítő üzenet korrekt, akkor a 1184 biztonsági szerver szimmetrikuskulcs-adója R(A) XOR R összefüggés szerint MM/SS kapcsolatkulcsot képez egy 1328 lépésben. A 1184 biztonsági szerver 1210 kapcsolatmenedzsere megjegyzi a kapcsolat kezdetét és tudomásul vevő üzenetet küld *A*-nak egy üzenetküldő szubrutin alkalmazásával (1330, 1332 lépés). A 1210 kapcsolatmenedzser veszi az üzenetet és megjegyzi a kapcsolat kezdetét (1334 lépés).

A óra/időzítő idő/dátum adatot ad *A* kapcsolatmenedzsernek egy 1336 lépésben, amely idő/dátum adatot *A* kapcsolatmenedzser a 1184 biztonsági szervernek megküld (1338 lépés). A 1184 biztonsági szerver összehasonlítja a kapott idő/dátum adatot saját idő/dátum adatával (1342 lépés), illetve megvizsgálja, hogy a kapott idő/dátum adat egy adott tűréshatáron belül helyes-e (1344 lépés). Ha a kapott idő/dátum adat kívül van a tűréshatárokon, akkor a biztonsági szerver új idő/dátum adatot küld *A* kapcsolatmenedzsernek (1348 lépés). A 1210 kapcsolatmenedzser veszi az üzenetet (1350 lépés) és *A* óra/időzítő az üzenet szerint igazítja saját idő/dátum adatát (1352 lépés). A 1184 biztonsági szerver a neki újra megküldött (újabb) idő/dátum adatot is leellenőrzi, arra nézve, hogy az belül van-e az adott tűréshatárokon. Ez a próbálkozás megadott kísérlet küszöbszámig ismétlődhet. A kísérletek számát a biztonsági szerver számlálja, és ha a kísérletek száma túllépi a küszöbszámot (1354 lépés), ami azt jelenti, hogy az *A* óra/időzítő nem működik helyesen, akkor megvizsgálja azt is, van-e folyamatban pénztármodul tranzakció (1356 lépés). Ha igen, akkor az *A* ügyfélhez küld „óra rossz" üzenetet (1358 lépés), ha nem, akkor az A ügyfél bankjának küld „óra rossz" üzenetet (1362 lépés). Mindkét esetben eldönthető, történjen-e további időegyeztető próbálkozás (1360 lépés).

Ha viszont az idő/dátum adatok a tűréshatárokon belül egyeznek, akkor a 1184 biztonsági szerver hálózati bejelentkezője A üzenetet állít össze az alábbiakból: rossz azonosítók listája, új elsődleges 1182 biztonsági szerver közös kulcs lista (amit a bizonylatoló kulcs elosztó funkciótól kap), közös kulcsok hossza (1364 lépés). A 1184 biztonsági szerver bizonylatkészítője megvizsgálja hogy egy globális újrabizonylatolás volt-e kérve és megbizonyosodik arról, hogy a globális újrabizonylatolás időperiódusa még nyitva van (1366, 1368 lépés). Egy ilyen időperiódusnak elég hosszúnak kell lennie ahhoz, hogy benne minden bizonylat újrabizonylatolható legyen vagy érvényessége lejárjon. A 1184 biztonsági szerver azt is megvizsgálja, mikor volt a bizonylat utoljára felülbizonylatolva, mert így kiszűri azokat, amelyeket nem szükséges újrabizonylatolni.

Ha volt újrabizonylatolás-kérés, akkor a 1184 biztonsági szerver bizonylatkészítője hozzáfűzi az üzenethez: a 1243 modul újra bizonylatolandó (1370 lépés), majd a 1184 biztonsági szerver közös kulcs adója szignálja az üzenetet (1372 lépés). A 1184 biztonsági szerver a szignált üzenetet *A*-nak küldi (1374 lépés), *A* közös kulcs adója ellenőrzi az üzenet szignójának érvényét (1376, 1378 lépés). Ha a szignó érvénytelen, a kapcsolat megszakad. Ekkor *A* biztonságőr frissíti a rossz azonosítók listáját, a közös kulcs listát és a kulcshosszadatot (1382 lépés).

A modul ellenőrzi, szükséges-e újrabizonylatolni a bizonylatot (vagy globális újrabizonylatolás keretében (1384 lépés) vagy mert lejárt bizonylat (1386 lépés)). Ha új bizonylatra van szükség, akkor *A* biztonságőr új bizonylat készítését kezdeményezi (1388 lépés). *A* közös kulcs adó új kulcsokat generál és a régi kulccsal szignálja az új közös kulcsot (1390 lépés). *A* kapcsolatmenedzser a szignált új közös kulcsot 1184 biztonsági szervernek küldi (1392, 1394 lépés), a 1184 biztonsági szerver bizonylatkészítője veszi a bizonylatoló üzenetet

(1396 lépés) és a 1184 biztonsági szerver közös kulcs adója értékeli az új közös kulcs szignóját (1398, 1400 lépés). Ha a szignó nem érvényes, akkor a 1184 biztonsági szerver megtagadja a hozzáférést a 1198 hálózathoz (1266 lépéssel kezdődő folyamat). Ha a szignó érvényes, *A* közös kulcs adó szignálja a bizonylatot és *A* modulhoz küldi (1402 lépés). *A* kapcsolatmenedzser veszi a bizonylatot (1404 lépés) és *A* biztonságőr értékeli a bizonylatot (1406 lépés), *A* közös kulcs adó is értékeli a bizonylatot (1408 lépés) (érvénytelen a bizonylat? 1410 lépés).

Ha a bizonylat nem érvényes, akkor *A* kapcsolatmenedzser „bizonylat érvénytelen" üzenetet küld a 1184 biztonsági szervernek (1412 lépés) egy üzenetküldő funkcióban (1413 lépés). A 1184 biztonsági szerver 1212 hálózati bejelentkezője veszi az üzenetet (1414 lépés), a 1184 biztonsági szerver közös kulcs adó értékeli a szignót (1416 lépés) és megállapítja, hogy érvényes-e a bizonylat? (1418 lépés). Ha a 1184 biztonsági szerver megállapítja, hogy a bizonylat tényleg érvényes, megtagadja a 1243 modultól a hozzáférést a hálózathoz. Ha viszont a bizonylat érvénytelen, akkor a biztonsági szerver kapcsolatmenedzsere „lekapcsolás a hálózatról" üzenetet küld a 1206 hálózati szervernek (1420 lépés). A hálózati szerver bejelentkezője hibajelző üzenetet küld a modulhoz (1422 lépés). *A* modul azután új próbálkozásra szólítja fel az ügyfelet vagy a bankot (1424–1432 lépések). Részletesebben: A 1424 lépésben *A* kapcsolatmenedzser veszi az üzenetet, és megvizsgálja van-e folyamatban pénztármodul-tranzakció? (1426 lépés), *A* kapcsolatmenedzser előfizetőt új próbálkozásra szólítja fel (1428 lépés). 1430 lépés: lesz új próbálkozás? *A* kapcsolatmenedzser *A* bankot újabb próbálkozásra szólítja fel (1432 lépés), 1430 lépés: lesz új próbálkozás?

Másrészt, ha a 1243 modul megállapítja,hogy az új bizonylat érvényes, akkor *A* kapcsolatmenedzser elfogadó üzenetet küld a biztonsági szervernek (1434 lépés). Ha nem kellett megújítani a bizonylatot, akkor az *A* biztonságőr ehhez hasonló üzenetet küld a 1184 biztonsági szervernek, (1436, 1438 lépések). Mindkét esetben a 1184 biztonsági szerver 1210 kapcsolatmenedzsere veszi a tudomásul vevő üzenetet és megjegyzi a 1243 modullal fenntartott kapcsolata végét (1440 lépés). Ezután a 1184 biztonsági szerver 1210 hálózati bejelentkezője a V véletlen számot és K kulcsot *A*-nak küldi (1442, 1444 lépés). *A* kapcsolatmenedzser veszi az üzenetet (1446 lépés), *A* szimmetrikuskulcs-adó kódolja a V véletlen számot K kulccsal, és a céladatot, a kódolt adatokat a 1206 hálózati szerverhez küldi (1448 lépés). A 1206 hálózati szerver 1212 hálózati bejelentkezője veszi az üzenetet (1450 lépés), a 1206 hálózati szerver szimmetrikuskulcs-adója dekódolja az üzenetet és ellenőrzi annak érvényét (1452 lépés), érvényes az üzenet? 1454 lépés. Ha V véletlen szám nem helyes, akkor a 1206 hálózati szerver 1210 hálózati bejelentkezője megtagadja a hozzáférést *A*-nak és bont (1456 lépés). *A* kapcsolatmenedzser veszi az üzenetet (1458 lépés). Ha a V véletlen szám helyes, akkor a 1206 hálózati szerver 1212 hálózati bejelentkezője kapcsolatot létesít a célállomással és erről *A*-t értesíti (1460 lépés). Végül az A kapcsolatmenedzser veszi az üzenetet és megjegyzi, hogy bekapcsolódott az EMS 1198 hálózatba (1462 lépés).

Kapcsolat létesítése

A 7A–7E. ábrán kapcsolat létesítése protokolljának folyamatábrája van feltüntetve. *A* biztonságőr modulbizonylatot küld *A* kapcsolatmenedzsernek (1464 lépés), *A* kapcsolatmenedzser veszi a bizonylatot és leellenőrzi, hogy az *A* pénztármodul hálózatra van-e kapcsolva (1466, 1468 lépés). Ha az *A* pénztármodul nincs a hálózaton, akkor *A* kapcsolatmenedzser az *A* biztonságőrtől kapott bizonylatot *B* célállomásra továbbítja (1476 lépés).

Ha viszont az *A* pénztármodul rá van kapcsolva a 1206 hálózatra, akkor *A* szimmetrikuskulcs-adó kódolja a bizonylatot kulccsal, (1470 lépés) és a kódolt bizonylatot *A* kapcsolatmenedzser megküldi a hálózati szervernek (1472 lépés). A 1206 hálózati szerver dekódolja a bizonylatot a K kulcs alkalmazásával és a bizonylatot *B* célállomásnak megküldi (1474 lépés). Függetlenül attól, hogy a bizonylatot a 1206 hálózati szerver vagy az *A* kapcsolatmenedzser küldte meg, *B* kapcsolatmenedzser veszi a bizonylatot (1480 lépés), és a *B* biztonságőr (ha *B* egy biztonsági szerver, akkor a kapcsolatmenedzsere) értékeli a bizonylatot (1482 lépés). 1484 lépés: érvényes a bizonylat? Ha a bizonylat nem érvényes, akkor a *B* kapcsolatmenedzser megjegyzi, hogy a kapcsolat megszakítva (1486 lépés) és informálja erről az ügyfelet vagy annak bankját (1486–1492 lépések). Részletesebben: *B* kapcsolatmenedzser megvizsgálja, van-e folyamatban pénztármodul-tranzakció? (1488 lépés). *B* ügyfélhez üzenet: tranzakció megszakítva (1490 lépés). *B* bankhoz üzenet: tranzakció megszakítva (1492 lépés). (Ha a B egy biztonsági szerver, akkor *B* csupán megjegyzi, hogy a tranzakció megszakítva).

Ha a bizonylat érvényes, akkor *B* biztonságőr leellenőrzi, nincs-e *A* a rossz azonosítók listáján (1494 lépés). 1496 lépés: A nincs-e rossz azonosító listán? Ha *A* rajta van a rossz azonosítók listáján, akkor a kapcsolat megszakad. Ha *A* nincs a rossz azonosítók listáján, akkor *B* véletlenszám-generátor R(B) véletlen számot és B értékelő üzenetet generál (1498 lépés). *B* óra/időzítő óra/dátum adatot küld *B* biztonságőrnek (1500 lépés). *B* biztonságőr egy üzenetbe összegyűjti az R(B) véletlen számot, a B értékelő üzenetet és az óra/dátum adatot (1502 lépés) és az üzenetet *B* közös kulcs adó kódolja A közös kulcsával (1504 lépés), *B* kapcsolatmenedzser B bizonylatát a kódolt üzenethez fűzi és az üzenetet *A*-hoz továbbítja (1506 lépés).

A kapcsolatmenedzser veszi az üzenetet (1508 lépés), *A* közös kulcs adó dekódolja az üzenet kódolt részét (1510 lépés). *A* biztonságőr értékeli a bizonylatot (1512 lépés), érvényes bizonylat? 1514 lépés. Ha a bizonylat nem érvényes, akkor *A* kapcsolatmenedzser megjegyzi, hogy a kapcsolat megszakad (1516 lépés) és a kapcsolat megszakadásáról informálja vagy az ügyfelet vagy a bankot (1516–1522 lépés). Részletesebben: *A* kapcsolatmenedzser megvizsgálja, van-e folyamatban pénztármodul-tranzakció (1518 lépés), üzenet *A* ügyfélnek: a tranzakció megszakad (1520 lépés), üze-

net *A* banknak: a tranzakció megszakad (1522 lépés). Ha a bizonylat érvényes, akkor *A* biztonságőr ellenőrzi, nincs-e *B* a rossz azonosító listán (1524 lépés), B rossz azonosító listán van-e? 1526 lépés. Ha B a rossz azonosítók listáján szerepel, akkor a kapcsolat megszakad. Ha *B* nincs a rossz azonosítók listáján, akkor *A* biztonságőr lehívja az idő/dátum adatot és összeveti *B* idő/dátum adatával (1528 lépés). Ha az idő/dátum adat kívül esik egy megadott tűréshatáron (1530 lépés: idő/dátum tűréshatáron kívül?), a kapcsolat megszakad.

Ha az idő/dátum adat az adott tűréshatárokon belül pontos, akkor az *A* véletlenszám-generátor R(A) véletlen számot és érvényesítő A üzenetet készít (1532 lépés). Az *A* biztonságőr R(A) XOR R(B) kapcsolatkulcsot formál, és összegyűjti A és B érvényesítő üzeneteket, az idő/dátum adatot és R(A) üzenetet egy üzenetbe (1534 lépés). *A* közös kulcs adó kódolja az üzenetet B közös kulcsával (1536 lépés). *A* kapcsolatmenedzser az üzenetet *B*-nek küldi (1538 lépés). *B* kapcsolatmenedzser veszi az üzenetet (1534 lépés), *B* közös kulcs adó dekódolja az üzenetet (1542 lépés), *B* biztonságőr értékeli az érvényesítő üzenetet (1544 lépés, 1546 lépés): B érvényesítő üzenet rendben? Ha a *B* érvényesítő üzenet hibás, a kapcsolat megszakad. Ha a B érvényesítő üzenet korrekt, a *B* biztonságőr R(A) XOR R(B) kapcsolatkulcsot készít egy 1548 lépésben, lehívja a *B* óra/időzítőből annak óra/dátum adatát és ezzel összeveti A óra/dátum adatát. 1550 lépés: óra/dátuma tűréstartományon kívül van-e? Ha az óra/dátum adat kívül van a tűréshatáron, akkor a kapcsolat megszakad. Ha az óra/dátum adat belül van a tűréshatáron (eléggé pontos), akkor a *B* kapcsolatmenedzser megjegyzi a kapcsolat megnyitását (1552 lépés).

Ekkor a *B* kapcsolatmenedzser tudomásul vevő és értékelő üzenetet küld *A*-nak (1554 lépés), 1556 lépés: BΨA. *A* kapcsolatmenedzser veszi az üzenetet (1558 lépés), *A* biztonságőr értékeli az üzenetet (1560 lépés), 1562 lépés: Az érvényesítő üzenet rendben? Ha igen, *A* kapcsolatmenedzser megjegyzi a kapcsolat megnyitását (1564 lépés).

Bankjegytranszfer

A 8A–8B. ábrán bankjegytranszfer protokoll folyamatábrája van feltüntetve. *X* bankjegykönyvtár transzferálandó bankjegyeket és értékeket választ, frissíti a bankjegyek összegét, sorszámát és üzenetet küld *X* bankjegytárnak (1566 lépés). A választás különféle szempontok szerint történhet: (1) minimalizálni a digitális szignók számát, (amellyel kapcsolatos műveletek viszonylag sok időt igényelnek), (2) minimalizálni a pakett méretét, (3) maximalizálni a transzfer pénztármodulban maradó elektronikus bankjegyek használhatóságát (tehát a legrövidebb maradék érvényű bankjegyektől megszabadulni). Ilyen célok elérhetők az alábbi bankjegytranszfer algoritmus alkalmazásával: (1) meghatározunk minden lehetséges alternatívát, amelyekben a bankjegyek legalább egyike szerepel, (2) meghatározzuk, hogy az alternatívák közül melyik jár legkevesebb bankjegymozgatással, (3) ha a (2) szerint több alternatíva marad, ezekből azt választjuk, amelyikhez a legkevesebb pénzegység × nap érvényesség tartozik. Pénzegység × nap érvényességet úgy kapjuk meg, hogy a bankjegy érvényének (jövőbeli) napjait megszorozzuk a bankjegy maradék pénzértékével és ezt összegezzük a pakett mindegyik bankjegyére.

X bankjegytár veszi *X* bankjegykönyvtár üzenetét és előkészíti mindegyik bankjegy transzferét úgy, hogy transzferfeljegyzést fűz hozzá (1568 lépés). *X* közös kulcs adó a bankjegyek számára szignót készít (1570 lépés). *X* pakettmenedzser pakettbe gyűjti az átutalandó bankjegyeket, transzferutasításokat és szignókat, *Y* számára (1572 lépés). A pakettet *XΨY*-nek megküldi (1574 lépés). *Y* pakettmenedzser veszi és megbontja a pakettet (1576 lépés).

Y értékelő értékeli a bankjegyek bizonylatait (a pénzformátum-generátor bizonylatát és a bizonylatok transzferadatait), mindegyik bankjegy tartalmát és a teljes összeget (1578 lépés). Az *Y* értékelő az értékelés során megvizsgálja, hogy az azonosító számok a transzfercsoportban egyeznek-e a modulazonosítókkal, amelyek az elektronikus bankjegyhez élete során hozzáfűződtek, mint az átutaló modulok azonosítója, bizonylatoló és szignáló modulok azonosítója. Az *Y* értékelő az értékelés során megvizsgálja minden múltbeli transzferösszeg adatát is, annak megállapítására, hogy azok egymással és a bankjegy megmaradt értékével összhangban vannak-e, nem vettek-e el már többet belőle, mint amit a legutóbbi transzferadat tükröz. Az *Y* értékelő megvizsgálja továbbá hogy a bankjegyek teljes összege összhangban van-e a várt összeggel (1578–1780 lépések). 1580 lépés: pakett rendben? Ha nem, a tranzakció meghiúsul (1582 lépés).

Ha a pakett rendben van *Y* egy tranzakciós pénztármodul, akkor *Y* értékelő értékeli a pakett bankjegyeinek lejáratát (1484–1588 lépések). Részletesebben: van-e folyamatban pénztármodul-tranzakció? (1584 lépés), *Y* értékelő értékeli a lejárati napokat (1586 lépés), vannak lejárt bankjegyek? (1588 lépés). Ha van a pakettben lejárt bankjegy, a tranzakció meghiúsul (1582 lépés). Ha a pakettben mindegyik bankjegy érvényes, *Y* értékelő mindegyik transzferazonosítóját összeveti a rossz azonosító listával (1590 lépés), 1592 lépés: van-e rossz listán szereplő transzferazonosító? Ha van, a tranzakció meghiúsul.

Ha nincs olyan azonosító a transzferrekordokban, amely rajta van a rossz azonosítók listáján (vagy Y nem egy transzferpénztármodul), akkor Y közös kulcs adó értékeli a szignókat (1594 lépés). 1596 lépés: érvényesek a szignók? Ha a szignók bármelyike nem érvényes, a tranzakció megszakad. Ha a szignók érvényesek, akkor *Y* értékelő leellenőrzi, hogy a bankjegy-testek egyeznek-e a bankjegytárban vagy a Tran Log-ban lévő bankjegyekével (1598 lépés), 1600 lépés: bankjegy-testek egyeznek? Y értékelő bankjegytranszferfát készít minden egyes megfelelő bankjegy számára, annak megállapítására, hogy nem történt-e duplikáció (1602 lépés). 1604 lépés: van-e a bankjegytestnek másolata? Ha bármelyik bankjegyről kiderül, hogy van másolata, a tranzakció meghiúsul. Ez a másolatkimutató funkció különösen alkalmas az ügyfelek elijesztésére attól, hogy manipulált tranzakciós pénztármodul használatával pénzt próbáljanak sokszorosítani.

Ha nincs másolat vagy nincsenek egymással egyező bankjegytestek, akkor *Y* bankjegytár az egy vagy több transzferálandó bankjegyet pénztartóba helyezi (1606 lépés). Végül Y bankjegykönyvtár frissíti a bankjegyek hollétére és összegére vonatkozó adatait és kezdeményez egy sorszámadást (1608 lépés).

Tudni kell azt is, hogy a bankjegytranszfer folyamata tartalmaz adatfrissítő és sorszámozó lépéseket is, amelyek a kibocsátott és forgalomban lévő bankjegyek összhangjának visszaállításához szükségesek, ha egy bankjegyet utaló modul a rossz azonosítók listájára került vagy bankjegymásolás felfedését célzó vizsgálatot folytatunk. Ezek a kiegészítő jellemzők és lépések teszik nehézzé és kockázatossá az illetéktelen behatolást a rendszerbe és bankjegymásolat készítését, forgalomba hozását.

Különböző pénznemek közötti átváltás

A 9A–9D. ábrákon a pénznemek közötti átváltás protokolljának folyamatábrája van feltüntetve. A példában az egyik pénznem a $, a másik pénznem a Ł. A példa azzal kezdődik, hogy *A* megállapodik *B*-vel, hogy A $-jáért B-től Ł-ot vásárol egy meghatározott $/Ł átváltási árfolyamon (1602' lépés). *A* és *B* a tranzakciós pénztármoduljaik igénybevételével bonyolítják le a tranzakciót az alábbiak szerint: *A* bejelentkezik a tranzakciós *A* pénztármodulba (1604' lépés). *B* bejelentkezik a tranzakciós *B* pénztármodulba (1606' lépés). *A* tranzakció-üzemmódot választ (1608' lépés), *B* tranzakció-üzemmódot választ (1610 lépés). *A* Ł (idegen pénz) vásárlását kezdeményezi (1612 lépés), *B* Ł eladását kezdeményezi (1614 lépés). *A* kapcsolatmenedzser védett kapcsolatot hoz létre (1616 lépés), *B* kapcsolatmenedzser védett kapcsolatot hoz létre (1618 lépés). *A* és *B* között létrejött a kódolással védett, adatátviteli kapcsolat (1620 lépés). *A* ügyféltől *A* pénztármodul az átváltani kívánt $ összeg megadását kéri (1622 lépés). *A* pénztármodul fizet/vált funkciója veszi a pénznem és összeg adatot (1624 lépés) és *A* pénztármodul bankjegy-könyvtára megvizsgálja, rendelkezésre áll-e ekkora összeg a modulban (1626 lépés). 1628 lépés: van elég pénz a modulban? Ha nem elég a pénz a végrehajtani kívánt tranzakcióhoz, akkor az *A* pénztármodul új összeg megadását kéri *A* ügyféltől (1630 lépés). 1632 lépés: van új összeg megadva? Ha van új összeg megadva, ismétlődnek a 1624–1628 lépések, ha nincs új összeg megadva, a tranzakció megszakad (1634 lépés).

Ha a megadott összeg rendelkezésre áll *A* pénztármodulban, akkor *A* fizet/vált funkciója $ összeg üzenetet küld *B*-hez (1636, 1638 lépés), amire a *B* pénztármodul Ł összeg vagy $/Ł árfolyam megadását kéri *B* ügyféltől (1640 lépés). *B* bankjegykönyvtár megvizsgálja, rendelkezésre áll-e a tranzakcióhoz szükséges Ł összeg a modulban (1642 lépés), (1644 lépés: van elég pénz a *B* modulban?) és ha nem, *B* modul új $/Ł árfolyam megadását kéri *B* ügyféltől (1646 lépés). (1648 lépés: van-e új $/Ł árfolyam megadva?) Az új $/Ł árfolyam megadása után *B* bankjegykönyvtár ismét megnézi, van-e elég pénz a modulban. Ha *B* ügyfél nem ad meg újat $/Ł árfolyamot, akkor *B* fizet/vált funkció „elégtelen pénzkészlet" üzenetet küld *A*-nak (1650, 1652 lépés). *A* ezután újabb összeget ajánlhat fel átváltásra vagy megszakad a tranzakció (1630–1634 lépések). Ha *B* pénzkészlete elégséges a tranzakcióhoz, *B* fizet/vált funkció elfogadó és Ł összeg valamint $/Ł árfolyam adat üzenetet küld *A*-nak (1654, 1656 lépés). *A* pénztármodul felhívja *A* ügyfelet az összeg és árfolyam jóváhagyására (1658 lépés) 1660 lépés: Ł összeg és $/Ł árfolyam rendben? Ha *A* ügyfél nem fogadja el a Ł összeget vagy $/Ł árfolyamot, akkor *A* fizet/vált funkció „helytelen érték" üzenetet küld *B*-nek (1662, 1664 lépés). A *B* pénztármodul ekkor új $/Ł árfolyam megadását kéri *B* ügyféltől (1666 lépés). 1668 lépés: Van új $/Ł árfolyam megadva? Ha nincs, a tranzakció megszakad (1670 lépés).

Ha viszont *A* jóváhagyja a *B* által megadott összeget, akkor *A* fizet/vált funkció a $ összegű bankjegyet a modul pénztartójába helyezi (1672 lépés), ahonnan átutalja *B*-nek (1674 lépés). A *B* fizet/vált funkció a Ł összegű bankjegyet a modul pénztartójába helyezi (1676 lépés), ahonnan átutalja *A*-nak (1678 lépés).

A tranzakciónak ezen a pontján *A* és *B* modul ideiglenesen tartja meg a megkapott, korrekt pénzösszeget. *A* és *B* két transzferben vesz részt párhuzamosan: a) transzfer: (1) *A* $-t utal át *B*-nek, (2) *B* $-t fogad el *A*-tól, b) transzfer: (1) *B* Ł-ot utal át *A*-nak, (2) *A Ł-ot fogad el B*-től. Az átutalásoknak ezt az ideiglenes jellegét úgy kell megszüntetni, hogy egyik fél se tudja visszavonni átutalását, amikor a másik fél már erre képtelen helyzetben van. Az átutalások ideiglenes jellegének véglegesre változtatása a kapcsolatok lezárásával történik. *A* lezárja a kapcsolatát és állandó rekordot képez a tranzakciós feljegyzéseiben (Tran. Log) mindkét tranzakciójáról. Ehhez hasonlóan *B* is lezárja kapcsolatát. *A* a kapcsolatát külön-külön képes lezárni a fenti két tranzakciója tekintetében: egyrészt a $ AΨB utalása, másrészt a Ł BΨA elfogadása tekintetében és *B* a kapcsolatát külön-külön képes lezárni a fenti két tranzakciója a tekintetében: egyrészt a Ł BΨA utalása, másrészt a $ AΨB elfogadása tekintetében.

☒

A pénznemek közötti átváltás protokolljának következő részében a tranzakciókban részt vevő egyik fél sem tudja, milyen sorrendben fognak megtörténni a fent ismertetett kapcsolatok lezárásai. Ez a bizonytalanság eliriasztja a feleket attól, hogy csalást vagy beavatkozást kíséreljenek meg. Van egy S(X) háttérfüggvény, amely úgy van definiálva, hogy S(0)=A, S(1)=B, ahol A és B az *A* és *B* pénztármoduloknak felel meg. X értéke véletlen szám, amely automatikusan választódik, például az alábbi rutin szerint: R(A) és R(B) az A, illetve B modul által generált véletlen számok, amelyek egy szubrutin kapcsolat lefutásával képződnek. Meghatározzuk az R(A) XOR R(B) paritását. Ez a paritás az X véletlen szám, amelynek $\bar{X}$ a komplementere: ($\bar{X}$=X XOR 1)

A 9D ábrán *A* Tran Log feltételesen felfrissíti S($\bar{X}$) transzfer log-ot (transzferfeljegyzést) (S(X) Ψ S(Ł)) egy 1680 lépésben. Ha X=0, akkor az A Ψ B ($) transzfer lesz feltételesen feljegyezve. Ha X=1, akkor a B Ψ A Ł transzfer lesz feltételesen feljegyezve. Minthogy a log

feltételes, visszafejthető akkor is, ha *A* lezárta a kapcsolatot. A log akkor válik véglegessé, amikor a frissítését véglegesítjük. *A* kapcsolatmenedzser ekkor „log frissítve" üzenetet küld *B*-nek (1682, 1684 lépés). Válaszul *B* Tran Log is feltételesen frissíti a log-ját és rekordot készít az S(X) Ψ S($\bar{X}$) frissítésnek megfelelő transzferről (1686 lépés).

Ha X=1 (1688 lépés), akkor *B* Tran Log a log frissítést feltételessé teszi (1688, 1690 lépések). E ponton *B* lezárta B Ψ A (Ł) transzferét. Ezután *B* a megfelelő protokoll (10. ábra) szerint lezárja a tranzakciót (1692 lépés). Ebben a helyzetben *A* mindkét transzferét ($ átutalás és Ł fogadása) le akarja zárni, és *B* le akarja zárni a még lezáratlan $ fogadása transzferét.

Ha viszont X=0 (1688 lépés), akkor a *B* kapcsolatmenedzser „lezárni" üzenetet küld *A*-nak (1694, 1696 lépés). *A* Tran Log a log frissítését erre feltétel nélkülivé teszi (1698 lépés), azaz a $ átutalása véglegessé vált. Ezután *A* a 10. ábra szerinti lezárásprotokollt lefuttatja (1700 lépés). Ebben a protokollban *B* lezárja mindkét transzferét (Ł utalása, $ vétele) és *A* lezárja még le nem zárt transzferét (Ł vétele).

Amint látható, az F/X átváltás tranzakció mindegyik résztranszfer külön lezárásával fejeződik be, azaz a bankjegyek védve vannak a duplikálás lehetőségétől, ami addig áll fenn, amíg csak az egyik fél zárta le a kapcsolatot. A különböző pénznemek közötti átváltás protokollja biztosítja, hogy egyik fél se tudja, melyik résztranszfer lesz a másik előtt lezárva, így egyik fél sem lehet érdekelt a tranzakciók manipulálásában, 50–50% annak valószínűsége, hogy nyer vagy veszít egy ilyen kísérleten. Azért sem érdemes manipulálással kísérletezni, mert van mód az elveszett pénz visszaigénylésére.

Lezárás

A 10. ábrán modulok közötti kapcsolat, illetve tranzakció-lezáró protokoll folyamatábrája van feltüntetve. *X* kapcsolatmenedzser „lezárásra kész" üzenetet küld *Y*-nak (1702, 1704 lépés). Ezzel átadja a lezárás kötelességét annak a modulnak *(Y)*, amely veszi az üzenetet. Egy hagyományos pénztranszferfolyamatban ezt az elsőként megszüntetési kötelesség áthárítási technikát arra használják, hogy a pénzt átutaló partner már ne hívhassa vissza az átutalt pénzét, tehát a pénz ne duplikálódhasson.

Y kapcsolatrendszer tudomásul vevő üzenetet küld *X*-nek (1706, 1708 lépés) és lezárja a még lezáratlan tranzakcióit a tranzakció log frissítésével (1710 lépés). Ha *Y* modul egy tranzakciós pénztármodul, akkor az *Y* modul tájékoztatja az ügyfelét a tranzakciók sikeres lezárásáról (1712, 1714 lépés). *Y* kapcsolatmenedzser ezután megjegyzi a kapcsolat lezárását (1716 lépés).

Tranzakció megszakítása

A 11A–11B. ábrán egy tranzakció-megszakítás protokoll folyamatábrája van feltüntetve. *X* kapcsolatmenedzser visszafejti a változásokat és megjegyzi, hogy a tranzakció meghiúsult (1726 lépés). *X* kapcsolatmenedzser ezután megnézi, volt-e „lezárásra kész" üzenet (1728 lépés). 1730 lépés: küldtek „lezárásra kész" üzenetet? Ha igen, akkor *X* Tran Log frissíti a tranzakció logot (1732 lépés), feljegyezve, hogy *X* „lezárásra kész" üzenet után megszakított, és feljegyezve a bankjegy azonosítókat és összegeket vett bankjegyenként, egy transzferfeljegyzések protokollban. A tranzakció megszakítása protokoll tehát információkat jegyez fel (log), amikor a megszüntető szubrutint indítják egy sikertelen lezáró szubrutinból.

Ha *X* tranzakciós 1186 pénztármodul, és „lezárásra kész" üzenet volt, akkor *X* modul informálja ügyfelét arról,hogy a tranzakció sikertelen volt, megszakadt, és hogy ennek valószínű oka pénztranszferhiba (1734–1738 lépések). Részletesebben: *X* Tran Log megnézi, van-e folyamatban pénztármodul tranzakció? (1734 lépés), küldtek-e „lezárásra kész" üzenetet? (1736 lépés), *X* modul *X* ügyfélnek kijelzi: a tranzakció meghiúsult, lehetséges pénztranszferhiba (1738 lépés).

Ha *X* modul egy banki 1188 pénztármodul, (1740 lépés: banki pénztármodul?) akkor *X* modul információt küld a banknak, hogy fejtse vissza a könyvelésébe állított változásokat (1742 lépés). Ha *X* egy tranzakciós pénztármodul és nem volt „lezárásra kész" üzenet, akkor az *X* modul informálja *X* ügyfelet arról, hogy a tranzakció meghiúsult (1744 lépés).

Az *X* kapcsolatmenedzser mindegyik esetben üzenetet küld *Y*-nak, miszerint a tranzakció nem befejezhető (1746, 1748 lépések). *Y* kapcsolatmenedzser visszafejti a változásokat és megjegyzi, hogy a tranzakció meghiúsult (1750 lépés). *Y* modul ezután informálja *Y* ügyfelet a tranzakció meghiúsulásáról(1754, 1756 lépések), vagy visszafejteti a bankkal (1756 lépés: banki pénztármodul?) a könyvelésén átvezetett változásokat (1758 lépés).

Amint már említettük, ha egy tranzakció megszakad a lezárás szakaszában, lehetséges, hogy elvesznek bankjegyek egyik vagy másik modul számára. Ez akkor történhet meg, ha az átutalást vevő transzfer szakadt meg, amíg a bankjegyet átutaló transzfer rendesen lezárult. Ez esetben az átutalást vevő pénztármodulja feljegyzi a bankjegyek adatait, amely bankjegyeket meg kellett volna kapnia, és értesíti ügyfelét, hogy hiba van (az A által szabályosan utalt bankjegyeket nem kapta meg).

Az átutalás címzettje ilyen esetben elveszettpénz-visszakövetelést nyújthat be a bizonylatoló ügynökségnél. A követelés tartalmazza a meghiúsult tranzakcióval kapcsolatos, automatikusan rögzített feljegyzéseket. A bizonylatoló ügynökség ilyenkor leellenőrzi az elveszett bankjegyet kibocsátó banknál, hogy a bankjegyek érvényben voltak-e. A kérelmező egy meghatározott időintervallum elmúlásával, ha addig nem került forgalomba a bankjegy, visszakapja a pénzét.

POS fizetés

A 12A–12C. ábrán „Point of Sale" (POS) fizetés (a vásárlás helyszínén történő fizetés) protokolljának folyamatábrája van feltüntetve. A POS fizetés egy vevő és eladó tranzakciós 1186 pénztármoduljai között lebonyolítható, egyszerű és közvetlen fizetésmód. Az eladó 1186 pénztármodulja lehet például egy szupermarket pénztárgépe.

A vevő adott áron meg kíván vásárolni valamely terméket vagy szolgáltatást *B* eladótól (1760 lépés). *A* vevő bejelentkezik a saját *A* pénztármoduljába (1762 lépés), *A* pénztármodul *A* vevőtől kéri a tranzakció jellegének megadását (1764 lépés). Vevő POS fizetésmódot választ (1766 lépés). Eközben a kereskedő meghatározza a számla végösszegét (1768 lépés), bejelentkezik a saját *B* pénztármoduljába (1768 lépés), amely modul tőle a tranzakció jellegének megadását kéri (1770 lépés) és az eladó *B* pénztármodulján POS fizetés fogadása üzemmódot választ (1772 lépés). *B* kapcsolatmenedzser kapcsolatot létesít (1774 lépés), *A* kapcsolatmenedzser kapcsolatot létesít (1775 lépés), és így létrejön a biztonságtechnikailag védett kapcsolat *A* és *B* pénztármodulok között (1776 lépés). *B* modul összeg megadását kéri (1778 lépés), *B* fizet/vált funkció veszi az összeg adatot, és *A* modulhoz továbbítja 1782 lépésben. *A* modul vevőtől kéri az összeg jóváhagyását és az átutalandó pénz jellegének (pénz vagy hitel) valamint a bankjegyeknek kiválasztását (a megfelelő összeg összeállítását az *A* modulban tárolt bankjegyekből (1784 lépés). 1786 lépés: korrekt a kért összeg? Ha a kért összeg nem helyes, errős *A* fizet/vált funkció üzenetet küld *B* modulnak (1788, 1790 lépés). A *B* modul ekkor új összeg megadását kéri eladótól (gazda) (1792 lépés). 1794 lépés: Van új összeg? Ha eladó nem ad meg új összeget, a tranzakció megszakad (1796 lépés).

Ha az eladó által kért összeg helyes (azt a vevő elfogadta), akkor az *A* fizet/vált funkció veszi a pénz jellege és összege információt (1798 lépés), *A* bankjegykönyvtár ellenőrzi, van-e megfelelő pénzmennyiség a bankjegytárban (1800 lépés), vannak-e az összegnek megfelelő bankjegyek? (1802 lépés). Ha nem elég a pénz, akkor *A* modul új összeg, illetve új bankjegy kombináció megadására hívja fel vevőt (1804 lépés), és megnézi, van-e új összegadat beadás? (1806 lépés). Ha nincs újabb adat, akkor *A* fizet/vált funkció „elégtelen pénz" üzenetet küld *B*-nek (1808, 1890 lépés). *B* modul ekkor új összeg adatot kér az eladótól (1792 lépés). 1794 lépés: van megadva új összeg? Ha az eladó új összeget ad meg, a fizetési folyamat elölről kezdődik.

Ha *A* modul pénze elég a tranzakcióhoz, akkor *A* fizet/vált funkció a bankjegytárból a pénztárolóba teszi a megfelelő bankjegyeket (1810 lépés) és onnan átutalja *B* modulba (1812 lépés), majd lezárja a transzferkapcsolatot (1814 lépés).

A fentiekből kitűnik, hogy a POS fizetés egyszerű a vevő számára, mert ez egy az eladó (az átutalást vevő) által kezdeményezett fizetés. Általában a POS fizetés leginkább áruk, szolgáltatások ellenértékének megfizetésére alkalmas, míg az ügyfelek közötti STS fizetés egyének közötti fizetésre vagy számlák kifizetésére alkalmasabb.

Kredit (hitel)-megújítás kibocsátó banknál

A 13A. 13B. ábrán kredit (hitelpénz)-megújítás kibocsátó banknál protokoll folyamatábrája van feltüntetve. A példa főként arra vonatkozik, amikor egy hitelkérő ügyfél a már engedélyezett hitelkerete terhére kér hitelpénzbankjegyet a hitelpénzt kibocsátó banktól. Egy hitelkerethez hitelszámla (bankszámla) tartozik, amely bankszámla feltölthető egyetlen bankjeggyel vagy több bankjeggyel. Egy hitelkérőnek lehet több bankszámlája is. Megjegyzendő, hogy mindegyik bank, amelyik egy ügyfélnek engedélyezi bankszámlájának hitelpénzbankjegyekkel való feltöltését, a hitelpénzbankjegyek tekintetében kibocsátó banknak tekintendő. A kreditfrissítő tranzakció egy kreditbejelentkező eljárással indul *A* pénztármodul és a bank banki *B* pénztármodulja között (1854 lépés), amit most a 14. ábra alapján ismertetünk.

Kreditbejelentkezés

Kredit pénzkivétel célú bejelentkezési eljárás kezdődik, ha egy *A* pénztármodul tulajdonosa vagy bérlője úgy dönt, hogy megújítja hitelpénzállományát, és ennek érdekében bejelentkezik az *A* pénztármoduljánál (1876 lépés). Ilyen eset például ha *A* ügyfélnek a moduljában van ugyan kreditbankjegy, de ezt váltani, megnövelni vagy csökkenteni kívánja. A csökkentés egészen nulla összegig terjedhet. Egy másik eset, ha az ügyfél *A* pénztármoduljában nincs hitelbankjegy tárolva, ezért azt feltölteni szeretné. *A* modul *A* ügyféltől instrukciót kér tranzakcióra (1878 lépés). *A* ügyfél beadja a bankszámláról lehívni kívánt kreditösszeget és érintett bankszámlája adatait (1880 lépés). Ebben az alkalmazásban a kreditfrissítés összege megegyezik a lehívandó kreditösszeggel, amire *A* ügyfélnek épp szüksége van. *A* tranzakciós pénztármodul kapcsolat létesítését kezdeményezi a hitelt biztosító *B* bankkal. A kapcsolat EMS hálózaton jön létre, tehát hálózatra történő bejelentkezéssel (1882 lépés) indul. Miután *A* pénztármodul bejelentkezett a hálózatra, *A* modul és *B* bank között védett adatátviteli kapcsolat jön létre (1884 lépés). Az *A* pénztármodul azután kreditkérést továbbít a *B* banki pénztármodulhoz (1886 lépés) egy olyan eljárás során, amelyet az alábbiakban a 15A–15B. ábra alapján ismertetünk.

Hitelpénzkérés

A 15A–15B. ábrán hitelpénzkérés folyamatábrája van feltüntetve. A példában a feleket X és Y-nal jelöltük, de fél lehet bármely pénztármodul jellegű modul, amely banki (pénzkibocsátó) pénztármodullal lép kapcsolatba.

X bankjegykönyvtár, ha van kreditbankjegy a bankszámlán, a bankjegy összegét az *X* banki pénztármodullal közli (1897 lépés). *X* banki pénztármodul az *A* ügyfél által kért és a meglévő bankjegyek különbségéből nettó kreditkérelmet készít, amely kérelmet egy meghatározott számla alapján érvényesíteni szükséges (1898 lépés). A kreditkérelmet *X* banki pénztármodul *Y* bankhoz küldi, az üzenetbe belefoglalva a nettó kreditösszegen kívül a bankszámla számát és fejelését (1998 lépés), lefuttatva az üzenetküldő protokollt, amelyben az üzenet kódolással védetten kerül átvitelre (1900 lépés). A hitelpénzkérés a bankszámlaszámmal és fejeléssel együtt *Y* pénztármodulhoz jut, amely kezdeményezi a bankszámlaszám helyességének ellenőrzését (1902 lépés). A bankszámlaszám értékelését egy a 20. ábra szerinti, később ismertetendő eljárásban végezzük.

A bankszámla-információ helytállóságának megvizsgálása után, ha az rendben van, *Y* bank értékeli, van-e

elegendő kredit engedélyezve (1904 lépés). 1906 lépés: Van megfelelő, engedélyezett hitelkeret?

A hitelkeret megfelelősége esetén *Y* tranzakció funkció elfogadó üzenetet küld *X*-nek (1908 lépés) az üzenetküldő protokollt lefuttatva (1910 lépés). *X* pénztármodul veszi az elfogadó üzenetet (1912 lépés) a banki pénztármodullal fennálló kapcsolatában.

Ha nincs meg a szükséges összegű hitelengedély (15B. ábra), az ügyfél új hitelösszeg megadására kap felszólítást (1914–1918 lépések). Részletesebben: *Y* tranzakció funkció „elégtelen hitel" üzenetet küld *X*-nek (1914 lépés) az üzenetküldő protokoll lefuttatásával (1916 lépés), *A* ügyféltől *X* modulja új összeg megadását kéri (1918). 1920 lépés: van megadva új összeg? Ha az ügyfél új kért hitelpénzösszeget ad meg, azt az *X* modul *Y* bankhoz küldi (1922, 1924 lépések), a banki pénztármodul az összeget újraértékeli a tekintetben, hogy belefér-e a megnyitott hitelkeretbe (15A. ábra szerinti 1904 lépéstől kezdve). Ha az ügyfél nem ad meg újabb összeget, a tranzakció megszakad (1926 lépés). A hitelpénzkérés folyamatában, a 14. ábra szerinti folyamatábra szerinti *A* pénztármodul minden benne tárolt bankjegyet átküld *B* banki pénztármodulnak, tehát nemcsak a hitelpénzbankjegyet, hanem a pozitív értékű bankjegyeket is, függetlenül attól, hogy melyik korábbi tranzakcióból származtak (1888 lépés). Ha már nincs bankjegy az *A* tranzakciós pénztármodulban a hitelpénzkérés idején (1890 lépés: Van bankjegy *A* pénztármodulban?), akkor *A* pénztármodul nemleges üzenetet küld *B* pénztármodulnak (1892, 1894 lépések). Ha ekkor még van bankjegy az *A* pénztármodulban, akkor azt *A* pénztármodul átküldi *B* banki pénztármodulhoz a 8. ábra szerinti eljárás alkalmazásával (1896 lépés).

A 13. ábra szerinti folyamat 1854 lépésében hitelpénzkérést küld *A* ügyfél a kibocsátó *B* bankhoz *B* kibocsátó bank leellenőrzi, hogy minden hitelpénz- és nem hitelpénzbankjegy átkerült-e hozzá az *A* modulból (1856 lépés). 1858 lépés: összes bankjegy átadva? Ha a banknak átadott bankjegyek valóban az *A* tranzakciós pénztármodulból származnak, akkor *B* bank a könyvelésén átvezeti a változásokat (1860 lépés). Akkor is, ha nem volt átadandó bankjegy az *A* modulban, és akkor is, ha az 1860 lépésben történt lekönyvelés után nem maradt bankjegy az *A* modulban, kapcsolat létesül *B* banki pénztármodul és *B* pénzformátum-generátor között (1862 lépés). A *B* bank frissíti a hitelkeretet (1864 lépés) hozzáadva a bankjegyet (ha ilyen van) a hitelkerethez, így az igénybe vehető teljes hitelösszeget számolja ki, és ebből vonja le a kért hitelpénz összegét. Ha nincs szükség sem hitelpénz sem más bankjegy előállítására, mert az engedélyezett hitelkeret állása nulla és pozitív értékű bankjegy átutalására sem került sor, a pénztármodulok lezárják a tranzakciós kapcsolataikat (1875 lépés) a 10. ábra szerinti eljárás (1865–1875 lépések) alkalmazásával. Ha szükség van bankjegy (kredit- vagy debitbankjegy) előállítására, mert a kért hitelpénzösszeg nem nulla és/vagy bankjegyek transzfere történt a kérési folyamatban, akkor a kibocsátó *B* banki pénztármodul a *B* pénzformátum-generátortól meghatározott bankjegy előállítását kéri (1866 lépés). Az előállított bankjegyet vagy bankjegyeket a pénzformátum-generátor *B* banki pénztármodulhoz továbbítja (1868 lépés), a *B* banki pénztármodul pedig az új bankjegyet vagy bankjegyeket *A* modulba továbbítja (1870 lépés) a 8. ábra szerinti bankjegy-átutalási eljárás alkalmazásával. Ezután a kérésben és tranzakcióban részt vevő modulok lezárják a kapcsolataikat a 10. ábra szerinti folyamatban. A kapcsolatlezárások sorát az a tranzakciós pénztármodul kezdi, amelyik a *B* banki pénztármodullal kapcsolatban állt (1872 lépés). Ezután a *B* banki pénztármodul és a *B* pénzformátum-generátor közötti kapcsolat zárul le (1874 lépés). Ezzel a hitelpénzkérés folyamata lezárult a kibocsátó bank részéről.

Kibocsátottpénz-vizsgáló (egyeztető) rendszer

A kibocsátott bankjegyeket ellenőrizni célszerű esetleges duplikálások, hamisítások kiszűrése érdekében (16., 17. ábrák). A kibocsátottpénz-vizsgáló rendszer egy kibocsátott pénz mesterfájlra alapozva minden bankjegy számára egy bankjegy transzferfát készít, amely tükrözi a bankjegy eddigi transzfereinek teljes történetét.

A 16. ábrán egy bankjegytranszfer-történelem, azaz a bankjegymodulok közti (vízszintes koordináta irány), példakénti transzferei vannak ábrázolva idő sorrendben (függőleges koordináta irány). A 16. ábra szerinti fejlécen az alábbi megnevezések találhatók: Date/mine=dátum/időpont (nap:óra:perc), 1(MG)=pénzformátum-generátor, 2 (teller)=banki pénztármodul, 3,4,5,6 tranzakciós pénztármodulok. A fejléc szerinti 1–6 számok modulazonosítók. A függőleges sorban például 1:00:00 egy dátum/idő adat. A nyilak különböző transzferműveleteket jelölnek, így Create=bankjegy előállítás az 1 pénzformátum-generátorban, Withdraw=bankjegykivét, Pay=kifizetés, Deposit=bankszámlára-helyezés. A 16. ábrán szemléltetve vannak a bankjegy $ érték változásai is.

A 16. ábra szerinti bankjegytranszfer-történelemnek megfelelő pénzmegjelenítő transzferfa van ábrázolva a 17. ábrán. Az ábrán alkalmazott jelölések: SEQ=sorszám, TR=átutalás vevője, $ összeg (érték). A példában 1 pénzformátum-generátor pénz egy elektronikus megjelenítőjét (elektronikus 2300 bankjegy) hozza létre. A 2300 bankjegynek törzsadatmezői és transzferadatmezői vannak, amelyeket jelöltünk a 17. ábrán, a 2300 bankjegynek továbbá bizonylat- és szignómezői is vannak, amelyek feltüntetésétől eltekintettünk az átláthatóság kedvéért. A törzsadatmezők tartalmaznak egy bankjegy-azonosítót (például N 12), a kibocsátó pénzformátum-generátor azonosítóját (például MG1), a kibocsátó bank azonosítóját (Bank Name), a kibocsátás dátumát (1:00:00 issued), a lejárat dátumát (12:00:00 expires), a bankjegy monetáris értékét és pénzegységét ($50). Más törzsadatmezők (mint például a pénz jellege: hitelpénz) nincsenek a példában feltüntetve. A dátum/idő adat formája az ábrázolthoz képest (nap:óra:perc) eltérő is lehet.

A pénzmegjelenítő transzferek adatmezői transzferrekordokat (2306–2328 transzferfeljegyzés) tartalmaznak, amely transzferrekordok mindegyike tartalmazza az utalást fogadó (TR) azonosítóját, a transzfer dátum/idő adatát és a transzfer összegét ($) és előnyösen mindegyiknek van egy sorszáma (SEQ). A transzfer sor-

számát a bankjegy vagy bankjegyrész mindegyik átutalója bejegyzi a bankjegykönyvtárába, mindegyik transzfert követően. Átalában a transzfer azonosításához elegendő a transzfer dátum/idő adatát és sorszámát megadni. Előállhat azonban bankjegyduplikálás, ha például a transzferek között időigazítás történik és ugyanolyan összeget, ugyanaz a modul még egyszer kap. Ennek elkerülését, illetve felfedezését segíti a transzfersorszám (SEQ) alkalmazása. A transzfersorszám egy adott bankjegy élete során mindegyik következő transzfernél emelkedik. Ha egy kibocsátású pénzmegjelenítőhöz két egyforma transzfersorszám van fűzve, az duplikálás egyértelmű jele.

Amikor egy pénz elektronikus új megjelenítője (új 2300 bankjegy) a banki pénztármodulba (Teller 2) kerül, egy első 2302 transzferfeljegyzés készül, amelyet a bankjegytranszferek adatmezőjébe beillesztünk. Ez a 2302 transzferfeljegyzés tartalmaz egy transzfersorszámot (SEQ1), egy átutalást fogadó azonosítót (TR2), a transzfer időpontját (1:00:00 és a transzfer összegét ($50). Az áttekinthetőség kedvéért mindegyik transzfer után csak az utolsó transzfer rekordját tüntettük fel, de a korábbi transzferrekordok is a bankjegyhez fűzve maradnak. Ilyen okból nem tüntettük fel a 17. ábrán a transzferek össz-számát sem, amit ugyancsak tartalmaznak a transzferek adatmezői. Az MG 1 pénzformátum-generátorban készült 2300 bankjegy most a kibocsátó Teller 2 banki pénztármodulban van, ahonnan a 3 tranzakciós pénztármodul fogja lehívni. Az $50 bankjegy lehívásának részeként a 2 banki pénztármodul újabb 2304 transzferfeljegyzést fűz a bankjegyhez, pontosabban a 2302 transzferfeljegyzéssel ellátott bankjegy adatmezőinek másolatához. Ez a 2304 transzferfeljegyzés tárolódik a bankjegyet lehívó 3 tranzakciós pénztármodulban is. Megjegyezzük, hogy a 17. ábra szerinti bankjegy transzferfa minden ága egy-egy a bankjegyhez újonnan hozzáfűzött transzferfeljegyzésnek (transzferrekordnak) felel meg.

1:00:05 időpontban a 3 tranzakciós pénztármodul $10 dollárt fizet 2306 transzferfeljegyzéssel a 4 tranzakciós pénztármodulnak. 1:01:00 időpontban a 3 tranzakciós pénztármodul $10 dollárt fizet 2308 transzferfeljegyzéssel az 5 tranzakciós pénztármodulnak. 3:08:01 időpontban a 3 tranzakciós pénztármodul $25 dollárt fizet 2310 transzferfeljegyzéssel az 5 tranzakciós pénztármodulnak. 4:11:08 időpontban a 3 tranzakciós pénztármodul $5 dollárt fizet 2312 transzferfeljegyzéssel a 6 tranzakciós pénztármodulnak.

2:00:01 időpontban a 4 tranzakciós pénztármodul $5 dollárt utal át 2314 transzferfeljegyzéssel a 6 tranzakciós pénztármodulnak. 2:01:07 időpontban a 4 tranzakciós pénztármodul további $5 dollárt utal át 2315 transzferfeljegyzéssel a 6 tranzakciós pénztármodulnak, amely 6 modul 3:07:05 időpontban $5 dollárt utal át 2321 transzferfeljegyzéssel a 3 tranzakciós pénztármodulnak.

2:00:06 időpontban az 5 tranzakciós pénztármodul az egész $10 dollárt átutalja 2316 transzferfeljegyzéssel a 3 tranzakciós pénztármodulnak. A 3:08:01 időpontban a 3 tranzakciós pénztármodultól kapott $25 dollárból az 5 tranzakciós pénztármodul 3:09:12 időpontban kifizet 6 tranzakciós pénztármodulnak $20 dollárt 2318 transzferfeljegyzés készítése mellett és a maradék $5 dollárt elhelyezi a bank Teller 2 pénztármoduljában a bankszámláján 4:12:05 időpontban, 2320 tranzakciós feljegyzéssel.

4:10:00 időpontban a 6 tranzakciós pénztármodul $10 dollárt utal át 2322 transzferfeljegyzéssel az 5 tranzakciós pénztármodulnak. 5:00:06 időpontban a 6 tranzakciós pénztármodul a maradék $10 dollárt átutalja 2324 transzferfeljegyzéssel a 3 tranzakciós pénztármodulnak.

A találmány szerint előnyösen minden egy tranzakciós pénztármodultól banki pénztármodul felé irányuló tranzakció során nemcsak az átutalni kívánt, hanem a modulban tárolt minden bankjegyet átküldünk a bankba lejáratának frissítése céljából. Ebből következik, hogy a 2320 tranzakciós feljegyzésnek megfelelő lépésben, ahol $5 dollárt a bankban helyezünk el, az 5 tranzakciós pénztármodulból nemcsak az $5 dollár összeget küldjük át a bankba, hanem automatikusan és egy másik 2326 transzferfeljegyzéssel minden benne tárolt bankjegyet is, szimultán az $5 átutalásával. Ezután tehát egy (ha 3 modulban nem volt hitelpénzbankjegy) $5 értékű új bankjegyet állít elő az 1 pénzformátum-generátor, amit 3 transzferpénztármodul kap meg a kibocsátó Teller 2 banktól, megfelelő transzferfeljegyzés kíséretében. A modulokban tárolt bankjegyek lejártának frissítése tehát a bankkal végzett minden pénzmozgással járó művelettel (bankbetét elhelyezése, pénz kivétele bankszámláról) megtörténik, és ugyanekkor megtörténik a kibocsátott (forgalomban lévő) bankjegyek felülvizsgálata is.

5:00:10 időpontban a 3 tranzakciós pénztármodul $10 dollárt letétbe helyez 2328 transzferfeljegyzéssel a Teller 2 banki pénztármodulban. Ezzel egyidejűleg, automatikusan megtörténik a 3 tranzakciós pénztármodulban tárolt más bankjegyek (így a 2316 és 2321 transzferfeljegyzés szerinti pénzek) bankhoz történő átadása is. Válaszul a kibocsátó Teller 2 bank visszaküld a 3 tranzakciós pénztármodulnak egy új bankjegyet, amelynek értéke a modulnak visszaadandó bankjegyek összértéke (15$).

Ebben az időpontban már csak a 6 tranzakciós pénztármodulban van az eredeti 2300 bankjegyből (2312 és 2314 transzferfeljegyzésnek megfelelő) maradék, minden más bankjegyrész ebből van származtatva. Ha ezután a 6 tranzakciós pénztármodul a bankból pénzt vételez vagy ott elhelyez, már nem marad eredeti rész forgalomban a 2300 bankjegyből, annak minden részét kivonta már forgalomból a kibocsátó bank. A bankjegy lejáratának dátuma tehát egy időkeret, amelyen belül a bankjegynek el kell tűnnie a forgalomból.

A pénzmegjelenítő transzferfa a bankjegy teljes bevonásáig épül, tovább nem. Ha bekerül a forgalomba egy hamis bankjegy, annak nem egyezik a bankjegy-törzse az eredeti 2300 bankjegy törzsével. Ha a bankjegy valamely részösszege duplikálódott, akkor a duplikálódás utáni transzferek összege nem egyezik, hanem megnő a helyeshez képest. Amikor például az 5:00:06 időpontban a 6 tranzakciós pénztármodul a maradék 10$ dollárt

átutalja 2324 transzferfeljegyzéssel a 3 tranzakciós pénztármodulnak, a 10$ utalása helyett 20$ utalása történik, akkor a későbbi transzfernél (2318 transzferfeljegyzés) az összeg $20 helyett $30 lenne, ami jelezné, hogy a 6 transzfer-pénztármodulban duplikálódott a bankjegy.

Pénztármodul hozzáférése bankszámlához

A 18A–18C. ábrán „pénztármodul hozzáférése bankszámlához" protokolljának folyamatábrája van feltüntetve. A folyamat azzal kezdődik, hogy 1928 lépésben az ügyfél egy ügyfélkiszolgáló szolgálat megbízottjához (CSR) fordul, igazolja személyazonosságát és kéri, hogy az kapcsolja össze egy tranzakciós pénztármodulon át egy banknál vezetett bankszámlájával. Az ügyintéző a 1930 lépésben a kérést beadja az ügyfelet kiszolgáló *A* gazdamodulba (CSMHA), az ügyfelet kiszolgáló gazdamodul (CSMHA) a banktól lekéri (1932 lépés) és beszerzi (1934 lépés) az ügyfél bankszámláira vonatkozó bankinformációt. Ezután az ügyfél és a megbízott ügyintéző értékelik a bankinformációt, az előfizető kijelöli azt a bankszámláját, amelyikkel kapcsolatot kíván létesíteni (1936 lépés). Az ügyfél és az ügyfélkiszolgáló gazda ügyintéző közreműködésével az ügyfél *B* pénztármodulja és az ügyfélkiszolgáló modul (CSMA) között kapcsolat jön létre (1938–1946 lépések). Bővebben: az ügyfél kéri, hogy *B* pénztármodulját kössék össze a bankszámlájával (1938 lépés), *B* modul kapcsolatmenedzsere kapcsolatot létesít (1940 lépés), ugyanekkor a megbízott ügyintéző (CSR) az *A* ügyfélkiszolgáló modulon kér összekapcsolást a bankszámlával (1942 lépés) és az *A* ügyfélkiszolgáló modul kapcsolatmenedzsere kapcsolatot létesít (1944 lépés), amely lépések eredményeképp egy 1946 lépésben létrejön a kapcsolat az *A* ügyfélkiszolgáló modul és a *B* tranzakciós pénztármodul között (1946 lépés). Egy az *A* ügyfélkiszolgáló modul gazdájához intézett kérésre (1948 lépés) a gazda megküldi a bankinformációt az *A* ügyfélkiszolgáló modulnak (1950 lépés), az *A* ügyfélkiszolgáló modul veszi az információt és annak alapján bankszámlafejelést készít (1952 lépés). *A* közös kulcs adó ezután szignálja a bankszámlafejelést (1954 lépés), *A* bankszámlafejelő a szignált bankszámlafejelést tartalmazó üzenetet küld *B* pénztármodulnak (1956, 1958 lépés). *B* biztonságőr veszi az üzenetet, (1960 lépés), *B* közös kulcs adó leellenőrzi az abban foglalt digitális szignót (1962 lépés). Ha a szignó nem érvényes, a kapcsolat megszakad (1966 lépés).

Ha a szignó érvényes, akkor *B* modul a bankszámlafejelést *A* gazdához küldi, hogy az ügyfél ott értékelhesse (1964 lépés). 1967 lépés: bankszámlafejelés jóváhagyva? Ha az ügyfél nem erősíti meg a bankszámlafejelést, a tranzakció megszakad. Ha az ügyfél megerősíti a bankszámlafejelést, *B* biztonságőr a bankszámlafejeléshez ügyfélkiszolgáló modul bizonylatot fűz (1968 lépés). *B* modul ellenőrzi, nincs-e egy az új bankszámlafejeléssel megegyező bankszámlafejelés a számlavezető banknál (1970 lépés), 1971 lépés: van a bankban az új fejeléssel egyező bankszámla? Ha ilyen már létezik, akkor azt felülírja *B* pénztármodul (1972 lépés), ha nincs egyező fejelésű bankszámla, akkor *B* pénztármodul az új fejelést beírja bankszámla listájára (1976 lépés). Ezután a kapcsolat lezárul (1974 lépés).

Pénztármodul hozzáférésének megújítása

A 19A–19C. ábrán „pénztármodul bankszámlához történő hozzáférésének megújítása" protokoll folyamatábrája van feltüntetve. A folyamat azzal kezdődik, hogy az ügyfél bejelentkezik *A* tranzakciós pénztármoduljánál (1978 lépés) és válaszul az *A* modul a tranzakció jellegének megadását kéri (1980 lépés). Ügyfél a bankszámlájához való hozzáférés visszaállítását kéri *A* modulon, számlavezető *B* bankjához tartozó *B* vevőkiszolgáló modultól (1982 lépés). *A* tranzakciós pénztármodul lefuttatja a 6. ábra szerinti bejelentkezés hálózatra protokollt (1984 lépés), és létrejön a kapcsolat *A* tranzakciós pénztármodul és *B* bank vevőkiszolgáló modulja között (1986 lépés). *A* pénztármodul ezután megküldi a bankszámlák fejléseit *B* bank vevőkiszolgáló moduljának (1988, 1990 lépés). *B* bankszámlafejelő funkciója veszi az üzenetet (1992 lépés), *B* biztonságőr értékeli a vevőkiszolgáló modul bizonylatát és a bankszámlafejelések szignóját (1994 lépés). 1995 lépés: bizonylat és szignó érvényes? Ha a bizonylat vagy a szignó nem érvényes, akkor az ügyfélkiszolgáló modul megszakítja a tranzakciót (2000 lépés). Ha a bizonylat érvényes, akkor *B* banki gazda a bankszámlák fejléséből vett bankszámlaszámokat megküldi az ügyfélkiszolgáló modul gazdájának (1996 lépés), aki megnézi, hogy mindegyik bankszámla aktív-e (1998 lépés), 2001 lépés: minden bankszámla aktív? Ha a bankszámlák valamelyike lejárt, akkor a *B* ügyfélkiszolgáló modul gazdája megszüntető üzenetet küld *A* modulnak egy megszüntető eljárás lefuttatásával (2010' lépés).

Ha mindegyik bankszámla aktív, akkor a gazda ügyfélkiszolgáló modul felélesztő instrukciót küld az ügyfélkiszolgáló modulnak (2002 lépés), *B* bankszámlafejelő funkciója veszi az üzenetet és a számlainformációból bankszámlafejelést készít (2004 lépés). *B* közös kulcs adó szignálja a bankszámlafejelést (2006 lépés) és *B* bankszámlafejelő funkciója üzenetet állít össze a bankszámlafejelésből és szignóból (2008 lépés), az üzenetet *A* tranzakciós pénztármodulnak küldi (2010 lépés). *A* közös kulcs adó veszi az üzenetet és értékeli annak szignóját (2012 lépés), 2013 lépés: érvényes szignó? Ha a szignó nem érvényes, *A* tranzakciós pénztármodul megszakítja a tranzakciót (2018 lépés). Ha a szignó érvényes, *A* modul az ügyfélkiszolgáló modul bizonylatát fűzi a bankszámlafejeléshez (2014 lépés) és *A* tranzakciós pénztármodul lezárja a tranzakciót (2016 lépés).

Bankszámlaszám értékelése

A találmány szerinti egyik részmegoldásban, amelyben az ügyfél is rendelkezik a fent ismertetett ügyfélkiszolgáló modullal, a bankszámlaszám értékelése a 20. ábra szerinti folyamatban történhet. Ebben a folyamatban *Y* biztonságőr veszi a számlaszám és fejelés üzenetét, együtt az ügyfél ügyfélkiszolgáló moduljának bizonylatával, majd értékeli az ügyfélkiszolgáló modul bizonylatát (2020 lépés). Ha a bizonylat érvénytelen, a tranzakció a két pénztármodul között megszakad (2028 lépés).

Ha a bizonylat érvényes, akkor *Y* biztonságőr átadja a bankszámlafejelést *Y* közös kulcs adónak, hogy az ér-

tékelje annak szignóját (2022 lépés). 2023 lépés: szignó érvényes? Egy érvénytelen szignó észlelése hatására *Y* biztonságőr informálja a kapcsolatmenedzsert arról, hogy a fejelés érvénytelen (2026 lépés), és a két pénztármodul közötti kapcsolat megszakad (2028 lépés).

Ha a szignó érvényesnek bizonyul, akkor *Y* bankhoz funkció a megkapott számlaszámot a bank on-line számítógép rendszeréhez továbbítja (2024 lépés). Inaktív bankszámla észlelésekor az *Y* biztonságőr erről informálja az inaktív számla kapcsolatmenedzserét (2030 lépés) és megszakítja a tranzakciót (2028 lépés). Egy aktív bankszámla a bankszámlaszám-értékelő folyamatot tovább lépteti. Amint a fenti ismertetésből kitűnik, a bankszámlaszám-értékelő folyamat jelentősen leegyszerűsödött a banki pénztármodul számára ahhoz képest, amikor nem volt közbeiktatva folyamatba ügyféloldali ügyfélkiszolgáló modul.

Elveszett pénz visszakövetelése

Amint azt már említettük, az elektronikus pénz képes elveszni a tranzakciós folyamatokban az alábbi okok miatt: (1) a pénztármodul megsérül, és nem működik tovább, (2) a pénztármodult az ügyfél elveszíti, vagy azt ellopják, (3) a tranzakció lezárása féloldalas. Egy pénzrendszer hatásos működtetésének fontos feltétele, hogy az ügyfelek biztonságban tudják a pénzrendszerbe helyezett pénzüket, bizalommal legyenek a pénzrendszer iránt. Ehhez szükséges az, hogy a pénzrendszerben, a pénzrendszer hibájából elveszett pénzüket visszakaphassák. A tranzakciós pénztármodul elektronikája meghibásodásának lehetősége nem zárható ki, és ez vélhetően nagyobb valószínűséggel vezethet az ügyfélnél lévő pénztármodulban tárolt pénz elvesztéséhez, mint a papírpénz fizikai tönkremenetelének valószínűsége. A rendszer hibájából elveszett pénz visszaadásánál sokkal problémásabb az elvesztett vagy ellopott tranzakciós pénztármodulban tárolt pénz megmentése és visszaadása. Az erre irányuló igény sokkal nagyobb követelményeket támaszt a rendszerrel szemben, és biztonságos megoldás csökkentheti az ügyfelek elővigyázatosságát a moduljuk megőrzésében.

A találmány mindkét esetre nyújt megoldást, amely lehetővé teszi az elveszett pénz visszaszolgáltatását az ügyfélnek. A fenti (1) és (2) esetben ennek feltétele, hogy az ügyfél időnként készítsen elveszettbankjegykövetelést, (21A–21B. ábra), amelyet a tranzakciós modulján kívül tárol. Pénzelvesztés esetén ezt a követelést eljuttatja a kibocsátó bankhoz (22A–22E. ábra). A követelés tartalmazza a tranzakciós pénztármodul tartalmának legutóbb rögzített állapotát. A (tranzakciós pénztármodulban tárolt és) visszakövetelt bankjegyek adatait érvényesíteni szükséges a bank(ok)hoz küldés előtt. A kibocsátó bank egy ideig kivár, és figyeli, forgalomban vannak-e az elveszett bankjegyek, majd visszatéríti a bankjegyeknek megfelelő pénzt.

A (3) esetben, amelyben a pénztármodul és az ügyfélkiszolgáló modul közötti tranzakció féloldalas lezárása miatt következett be a pénz elvesztése, de a pénztármodul még működőképes (22A–22E. ábrák), az elveszettpénz-követelés az (1) és (2) esethez hasonlóan egy kibocsátottpénz-vizsgáló rendszerhez kerül, amely összehasonlítja a követelést a pénzrendszerben lévő pénzekkel. A kibocsátó bank kockázatmentesen kártalaníthatja az ügyfelet, mert minden, a pénzforgalomba visszakerülő bankjegy ellenőrizva van hamisítás vagy duplikálás tekintetében, emellett ismert az ügyfél is.

Ezeket az eljárásokat az alábbiakban részletesen ismertetjük a 21A–21B. és a 22A–22E. ábrák alapján.

Elveszettpénz-követelés készítése

A 21A. ábrán egy elveszettpénz-követelés készítésének folyamata van szemléltetve. A folyamat azzal kezdődik, hogy az *A* ügyfél bejelentkezik a tranzakciós pénztármoduljánál (2032 lépés). *A* tranzakciós pénztármodul üzemmód megadását kéri az ügyféltől (2034 lépés). Ügyfél elveszett pénz követelés készítése üzemmódot választja az *A* tranzakciós pénztármodulon (2036 lépés).

Ekkor számos lépés történik az *A* tranzakciós pénztármodulban, amellyel nyugalmi állapotokat teremtünk a modulban, hogy felmérhető legyen annak tartalma, a benne tárolt bankjegyek és meghiúsult tranzakciók adatai. Így *A* tranzakciós pénztármodulban az *A* bankjegykönyvtár a tartalmának másolatához követelés sorszámot társít, és pakettmenedzserhez továbbítja (2038 lépés), *A* bankjegytár a szignált és bizonylatolt bankjegyek másolatát a pakettmenedzserhez küldi (2040 lépés), *A* Tran Log átadja pakettmenedzsernek a meghiúsult (és eddig még nem követelt) kapcsolatok adatait (a meghiúsuláskor készített transzferfeljegyzéseket) (2042 lépés).

A közös kulcs adó ezután az *A* tranzakciós pénztármodul egyedi kulcsával szignálja a követelés sorszámát, a bankjegykönyvtár másolatát és a meghiúsult kapcsolatok adatait a pakettmenedzsernél (2044 lépés) és *A* pakettmenedzser szignálja az összegyűjtött adatcsomagot, ilymódon létrehozva a pakettet (2046 lépés). A pakettet ezután kódolják az *A* közös kulccsal (2048 lépés), majd *A* közös kulcs adó a kódolt követeléshez követelésleírást fűz, amely követelésleírás tartalmazza a követelés sorszámát, a követelés teljes összegét és az *A* tranzakciós pénztármodul bizonylatát (2050 lépés). Az *A* tranzakciós pénztármodul most az így teljes követelést a gazdájához továbbítja (2052 lépés), amely gazda a követelést az *A* tranzakciós pénztármodultól független helyen eltárolja jövőbeni felhasználás céljából (2054 lépés).

Elveszett pénz visszakövetelése

A 22A–22E. ábrán elveszett pénz visszakövetelése protokoll folyamatábrái vannak feltüntetve. A folyamat akkor kezdődik, amikor az ügyfél az ügyfélkiszolgáló megbízott képviselőhöz fordul, kérve, hogy készítsen elveszettpénz-követelést számára. Az ügyfél ekkor igazolja személyazonosságát (2056 lépés). Az ügyfélkiszolgáló képviselő (CSR) az előfizető azonosító adatai a gazda *A* ügyfélkiszolgáló modulba (CSMH) beadja (2058 lépés), és megállapítja az elvesztés okát (kapcsolathiba vagy modul elvesztése, tönkremenetele) (2060 lépés). 2061 lépés: kapcsolathiba? Ha az elvesztés oka kapcsolathiba és az ügyfél modulja épen megvan), és az ügyfél a tranzakciós pénztármodulján át történő lekérést választotta, a képviselő pedig ezt elfogadta, a tranzakciós pénztármodul *B* kapcsolatmenedzsere és az ügyfélkiszolgáló modul (CSM) *A* kapcsolatmenedzsere az ügyfélkiszol-

gáló képviselővel együttműködve (a gazda ügyfélkiszolgáló modulon (HCSM) át) védett kapcsolatot hoznak létre az *A* ügyfélkiszolgáló modul (CSM) és *B* tranzakciós pénztármodul között. (2062-2070 lépések). Részletesebben: a 2062 lépésben ügyfél a saját tranzakciós pénztármodulján kezdeményezi az elveszett pénz visszakövetelését, a megbízott képviselő elfogadja a követelést és intézkedik (2064 lépés), *A* kapcsolatmenedzser kapcsolatot hoz létre (2066 lépés), *B* kapcsolatmenedzser kapcsolatot hoz létre (2068 lépés), a 2070 lépésben létrejön a kapcsolat *A* ügyfélkiszolgáló modul (CSM) és *B* pénztármodul között.

Ha létrejött a védett kapcsolat, a képviselő *A* modulja az ügyfél azonosító adatait kéri gazdájától (2072 lépés), a gazda ügyfélkiszolgáló modul (HCSMA) válaszol a kérésre, az ügyfél adatait tartalmazó üzenetben (2074). *A* elveszettpénz-visszakövetelő funkció veszi az üzenetet és *B* pénztármodultól kéri a követelés megküldését (2076 lépés). 2078 lépés: üzenetküldés *AΨB*.

B Tran Log veszi az üzenetet és előhívja azon hibás transzfer rekordjait, amelyekből kifolyólag korábban még nem követeltek vissza pénzt (2080 lépés). Ha nincsenek ilyen rekordok, akkor a tranzakció megszakad (2383 lépés). Ha van ilyen rekord, akkor a *B* modul kijelzi ezek adatait (dátum, időpont, összeg) az ügyfélnek (2082 lépés), aki ezekből kiválasztja azokat, amelyeket visszakövetelni szándékozik (2084 lépés). Például az ügyfél nem kíván visszakövetelni olyan tételeket, amelyek sorsa közben más úton már rendeződött. *B* Tran Log minden kiválasztott hibás transzferfeljegyzésből üzenetet készít az *A* ügyfélkiszolgáló modul számára (2086 lépés), és elküldi az üzenetet (2088 lépés).

A elveszettpénz-követelés funkció veszi az információt és tudomásul vevő üzenetet küld a követelés azonosítójával, mint jövőbeni hivatkozási jellel (2090 lépés). 2092 lépés: üzenet továbbítása *BΨA.B* Tran Log veszi az üzenetet, és mindegyik transzferrekordot kiegészíti a követelés azonosítójával, dátum/idő adatával (2094). Ezután *B* lezárja a tranzakciót (2096 lépés).

Miután a tranzakciót lezáró lépéssor befejeződött, az *A* elveszettpénz-követelés funkció a követelést átformálja a kibocsátottpénz-vizsgáló rendszer (MIIS) számára (2098 lépés) és megküldi az *A* ügyfélkiszolgáló modul gazdájának (2100 lépés). Az *A* ügyfélkiszolgáló modul gazdája veszi a követelést és továbbítja a kibocsátottpénz-vizsgáló rendszerhez (MIIS).

Visszatérve a 2060 lépéshez, amelyben a pénz elvesztésének okát határoztuk meg, ha az elvesztést nem kapcsolathiba okozta (hanem például az ügyfél tranzakciós pénztármoduljának elvesztése), akkor az ügyfél az ügyfélkiszolgáló képviselőhöz fordul és választhat, hogy milyen úton nyújtja be elveszettpénz-követelését. *B* gazdának hozzáférése van mindegyik ügyfél – elveszett pénz követelés készítése eljárásban (21. ábra) készült és a tranzakciós pénztármodulon kívül tárolt – elveszettpénz-követeléséhez. Az ügyfélkiszolgáló képviselő a pénztármodul gazdájától fogadja el az elveszettpénz-követelést (2104 lépés), vagy a pénztármodul gazdájától (2106 lépés). Mindkét esetben a gazda hozza létre a szükséges kapcsolatot (2108 lépés).

Ezután az ügyféloldali *B* gazda elküldi a követelést a pénztármodul bizonylatával együtt az ügyfélkiszolgáló modul *A* gazdájának (CSMHA) (2110 lépés). 2112 lépés: üzenetküldés. *A* elveszettpénz-követelés funkció veszi a követelést (2114 lépés), és *A* közös kulcs adó értékeli a pénztármodul bizonylatát (CertM) (2116 lépés). 2117 lépés: bizonylat érvényes?

Ha a pénztármodul bizonylat érvénytelen, akkor *A* gazdához funkció üzenetet küld az ügyfélkiszolgáló modul *A* gazdájának (CSMHA), jelezve, hogy a követelés el van utasítva (2120 lépés), és az ügyfélkiszolgáló modul *A* gazdája az üzenetet az ügyféloldali *B* gazdához továbbítja, ezzel az eljárás sikertelenül befejeződik (2121 lépés).

Ha a pénztármodul-bizonylat érvényes, akkor *A* közös kulcs adó dekódolja a követelés üzenetet, és megvizsgál benne minden bankjegy- és szignóadatot (2118 lépés). Ha a vizsgált adatok bármelyike érvénytelen, (2119 lépés: érvényes?) akkor a folyamat a 2120, 2121 lépésekkel lezárul. Ha a vizsgált adatok mindegyike érvényes, akkor *A* elveszettpénz-követelés funkció vizsgálja a transzferösszegek konzisztenciáját és transzfertörténetét (2122 lépés). 2123 lépés: korrekt? Ha valamilyen inkonzisztenciát állapít meg, a folyamat a 2120, 2121 lépésekkel zárul.

Ha az összegek végig konzisztensek, akkor az *A* elveszettpénz-követelés funkció a kibocsátottpénz-vizsgáló rendszer (MIIS) számára követelést és követelésazonosítót készít (2124 lépés), *A* gazda a követelést és követelésazonosítót *A* ügyfélkiszolgáló modul gazdájához továbbítja (2126 lépés). Az ügyfélkiszolgáló modul gazdája veszi a követelést és a követelés azonosítót az ügyféloldai *B* gazdához, a követelést a kibocsátottpénz-vizsgáló rendszerhez továbbítja (2128 lépés). Ezzel az elveszettpénz-visszakövetelés folyamata lezárult.

SZABADALMI IGÉNYPONTOK

1. Eljárás pénznemek közötti átváltásra, első idegen pénznemű pénz ügyfél tranzakciós pénztármoduljában tárolt elektronikus megjelenítője és második idegen pénznemű pénz tulajdonos második pénztármoduljában tárolt elektronikus megjelenítője között, *azzal jellemezve,* hogy

a) az első tranzakciós pénztármodul (1186) és második pénztármodul (1188) között rejtjelezéssel biztosított kapcsolatot hozunk létre,

b) az ügyfél az első tranzakciós (1184) pénztármoduljában beadja az első pénznemben eladni kívánt – első – pénzösszeget,

c) leellenőrizzük, hogy az első tranzakciós (1186) pénztármodulban van-e tárolva a tranzakcióhoz szükséges mennyiségű elektronikus pénzmegjelenítő,

d) az első tranzakciós (1186) pénztármodulból rejtjelezéssel biztosított kapcsolatban átküldjük az első pénzösszegadatot a második pénztármodulba (1188),

e) a második pénztármodul (1188) tulajdonosától átváltási árfolyamot vagy a második pénznemben megadott – második – összegadatot kérünk,

f) leellenőrizzük, hogy a másoik pénztármodulban (1188) van-e tárolva a tranzakcióhoz szükséges mennyiségű elektronikus pénzmegjelenítő,

g) a második pénztármodulból (1188) üzenetet küldünk az első, tranzakciós pénztármodulba (1186) rejtjelezéssel biztosított kapcsolatban, közölve az átváltási arányt és/vagy a második összeget,

h) az első ügyfél elfogadja az átváltási arányt és/vagy a második összeget,

i) az első tranzakciós pénztármodulból (1186) rejtjelezéssel biztosított kapcsolatban átküldjük az első pénzösszegnek megfelelő, első pénznemű elektronikus pénzmegjelenítőt a második pénztármodulba,

j) a második pénztármodulból (1188) rejtjelezéssel biztosított kapcsolatban átküldjük a második pénzösszegnek megfelelő, második pénznemű elektronikus pénzmegjelenítőt az első, tranzakciós pénztármodulba (1186),

k) az első, tranzakciós pénztármodul (1186) átadja, a második pénztármodul (1188) átveszi az első pénznemű, első összegű pénzmegjelenítőt, a második pénztármodul (1188) átadja, az első, tranzakciós pénztármodul átveszi a második pénznemű, második összegű pénzmegjelenítőt, előre meg nem határozott sorrendben.

2. Az 1. igénypont szeirnti eljárás, *azzal jellemezve,* hogy a k) lépésben

a) az első és a második pénztármodul (1186, 1188) számára felosztunk egy közös, bináris értéket, annak első vagy második értékét választva az egyik vagy másik pénztármodul (1186, 1188) számára,

b) az első, tranzakciós pénztármodul (1186) visszafejtést megengedő módon, feltételesen bevezeti bináris értéktől függően vagy az első pénznemű pénzmegjelenítő átadását vagy a második pénznemű pénzmegjelenítő fogadását,

c) az első tranzakciós pénztármodulból (1186) üzenetet küldünk a második pénztármodulnak (1188) arról, hogy a feltételes tranzakció be van vezetve,

d) a második tranzakciós pénztármodul (1186) visszafejtést megengedő módon, feltételesen bevezeti bináris értéktől függően vagy a második pénznemű pénzmegjelenítő átadását vagy az első pénznemű pénzmegjelenítő fogadását,

e) a második tranzakciós pénztármodul (1188), ha a közös véletlen száma első értékű, kezdeményezi az első tranzakciós pénztármodulnál (1186) a tranzakció folytatását

f) az első tranzakciós pénztármodul (1186) válaszul a második tranzakciós pénztármodul (1188) üzenetére a feltételes átutalást feltétel nélkülivé teszi, és kezdeményezi befejező protokoll lefuttatását, amelyben az első tranzakciós pénztármodul (1186) visszavonhatatlanná teszi első pénznemű átutalását és a második tranzakciós pénztármodul (1188) is visszavonhatatlanná teszi második pénznemű átutalását,

g) a második tranzakciós pénztármodul (1188), ha a közös véletlen száma a második értékű, a feltételes átutalást feltétel nélkülivé teszi, és kezdeményezi befejező protokoll lefuttatását, amelyben a második tranzakciós pénztármodul (1188) visszavonhatatlanná teszi második pénznemű átutalását és az első tranzakciós pénztármodul (1186) is visszavonhatatlanná teszi első pénznemű átutalását.

3. A 2. igénypont szerinti eljárás, *azzal jellemezve,* hogy a közös véletlen számot a rejtjelesen kódolt kapcsolat létrehozása során, kapcsolatkulcsként hozzuk létre.

4. Az 1. igénypont szerinti eljárás, *azzal jellemezve,* hogy a két tranzakciós pénztármodul (1186, 1188) között folyamatban lévő pénzátutalást befejező, egy adott pénztármodul (1186, 1188) által kezdeményezett protokoll lépései az alábbiak:

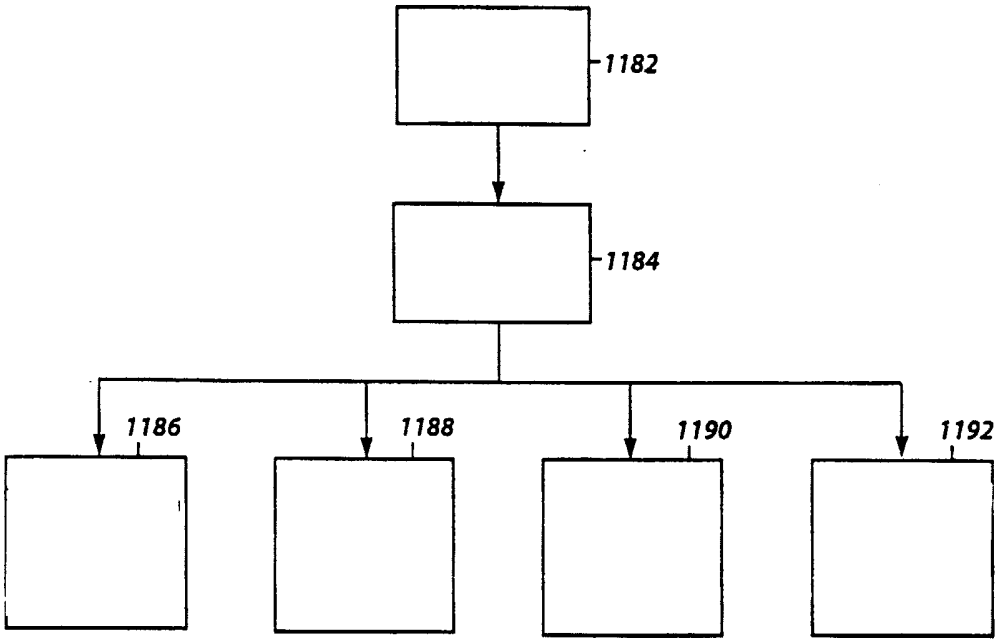
a befejező protokollt kezdeményező pénztármodulból (1186) „befejezésre kész" üzenetet küldünk a másik pénztármodulba (1188)

a másik pénztármodulból (1188) válaszként tudomásul vevő üzenetet küldünk a kezdeményező pénztármodulba (1186),

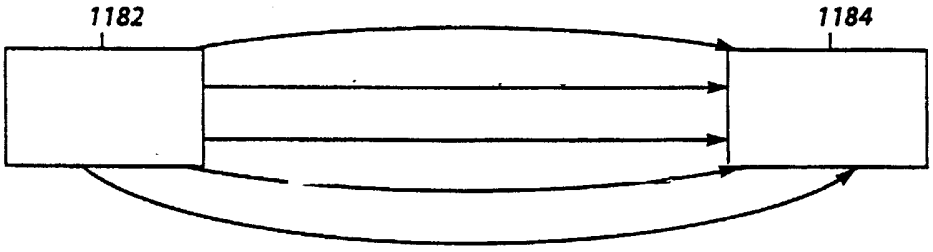
a kezdeményező pénztármodul (1186) visszafejthetetlenné teszi a folyamatban lévő pénztranszfer műveleteit, és így véglegesíti a pénz átutalását,

a másik pénztármodul (1188) is visszafejthetetlenné teszi a folyamatban lévő pénztranszfer műveleteit.

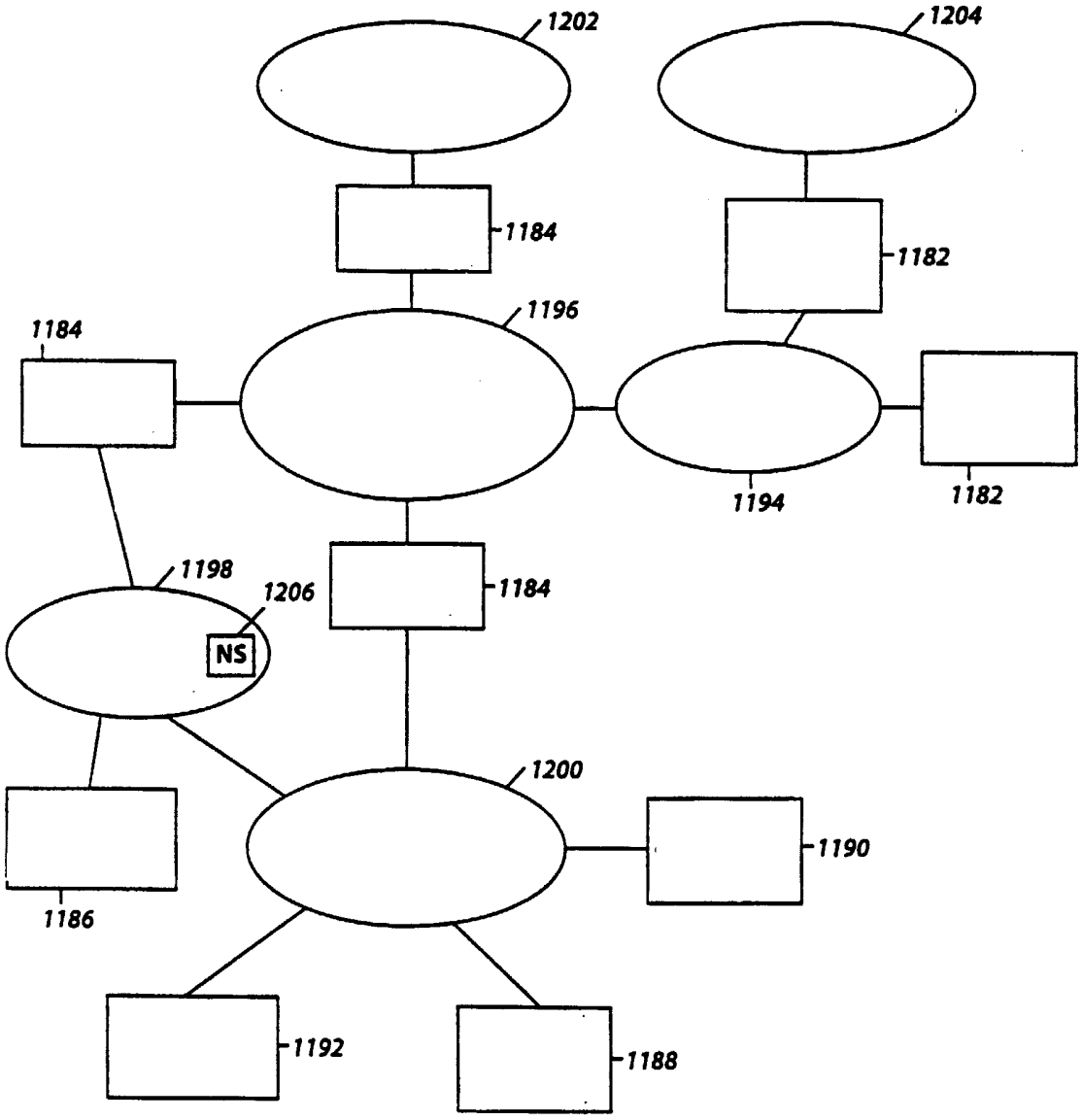
5. Az 1. igénypont szerinti eljárás, *azzal jellemezve,* hogy a b) lépésben az első ügyfél az átváltandó, első összeget bankjegyenként adja meg.



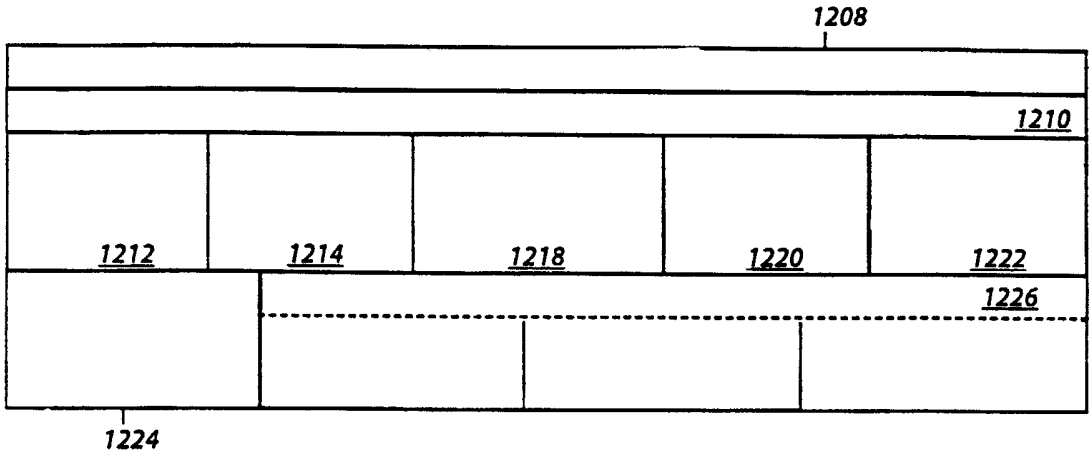
1A. ábra



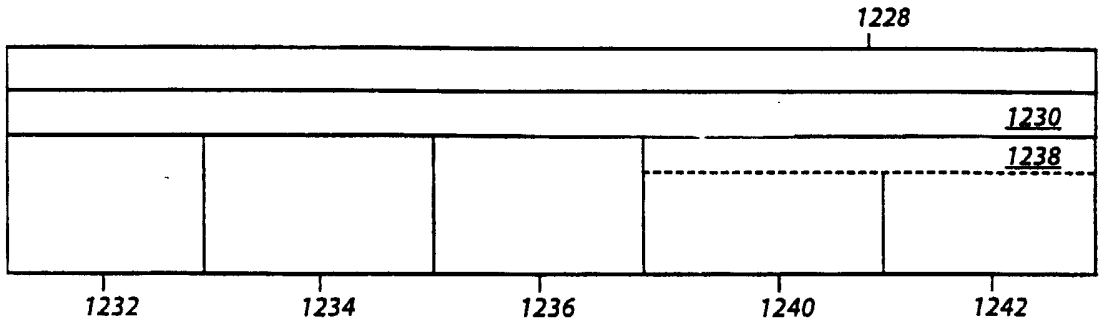
1B. ábra


1202
1204
1184
1182
1196
1184
1194
1182
1198
1206
1184
NS
1200
1190
1186
1192
1188

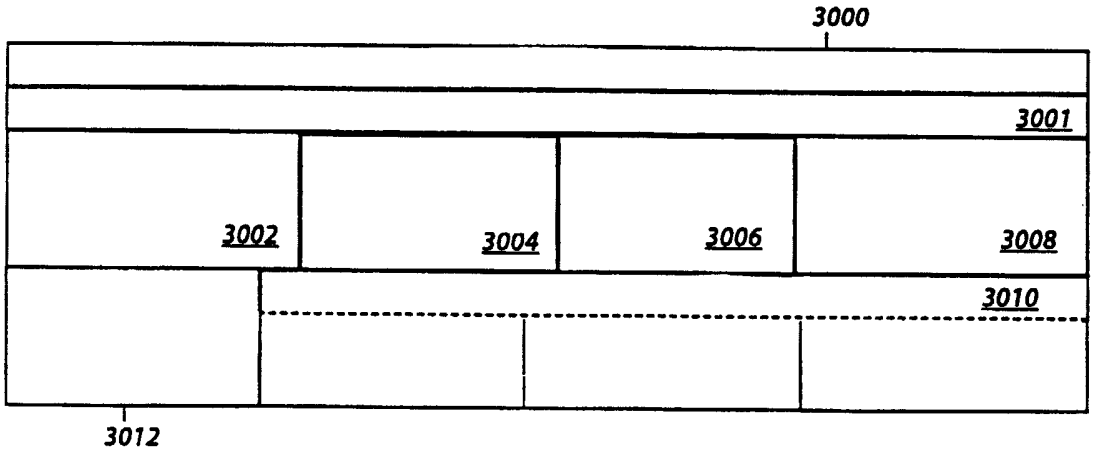
2. ábra



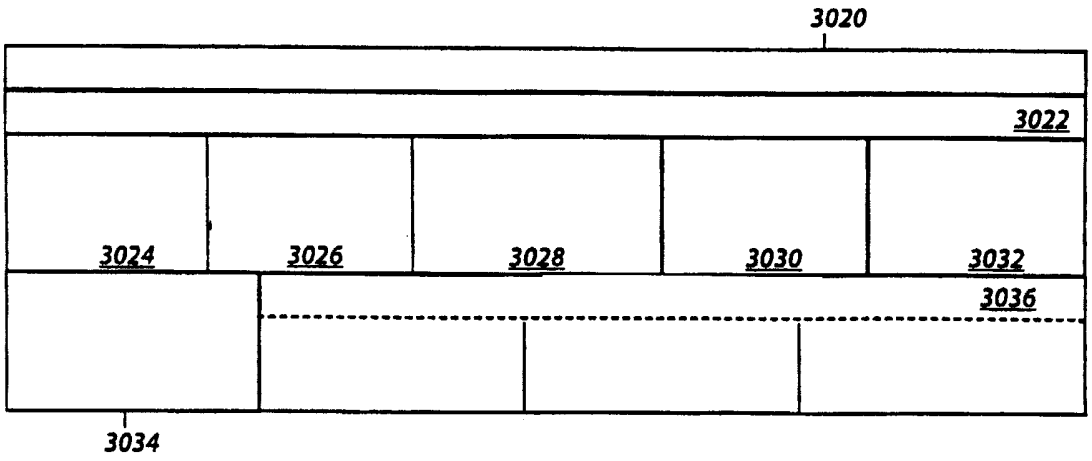
3A. ábra



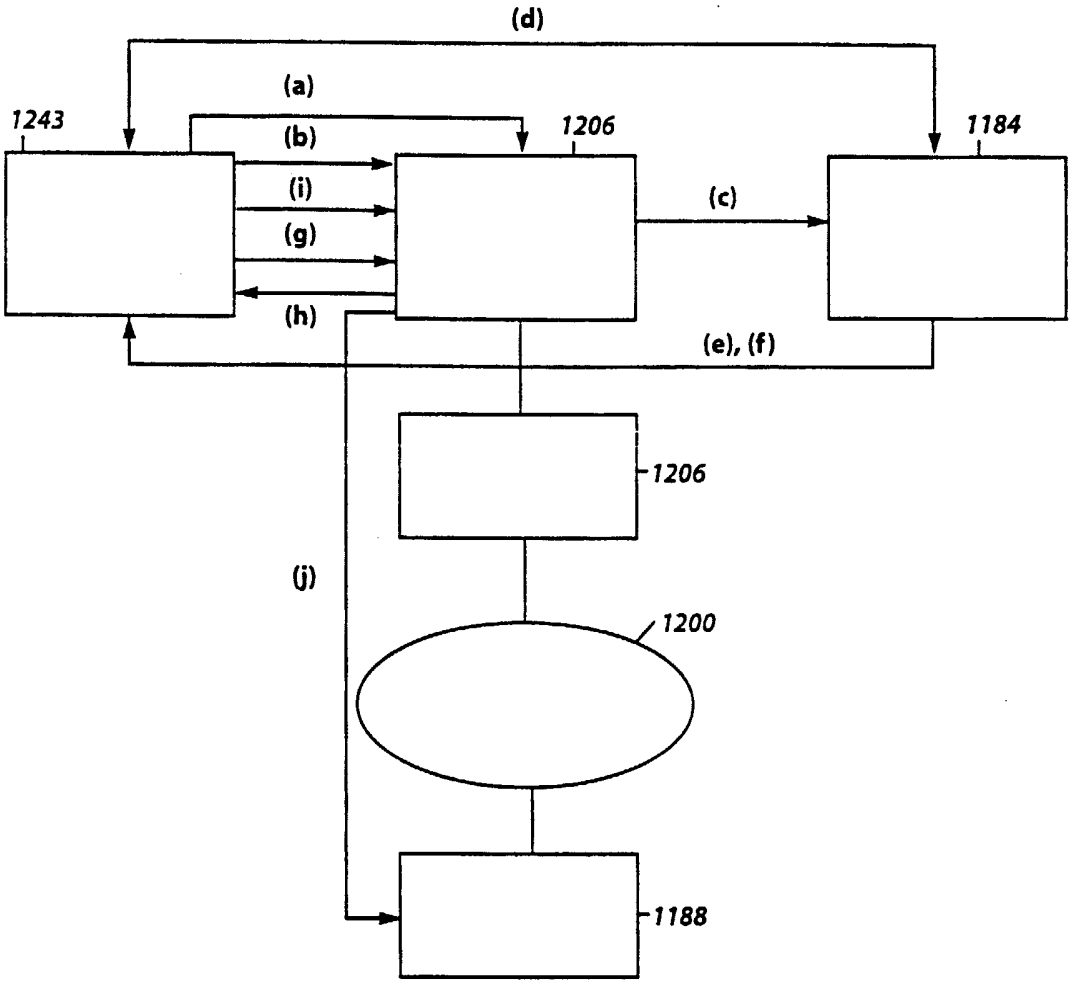
3B. ábra



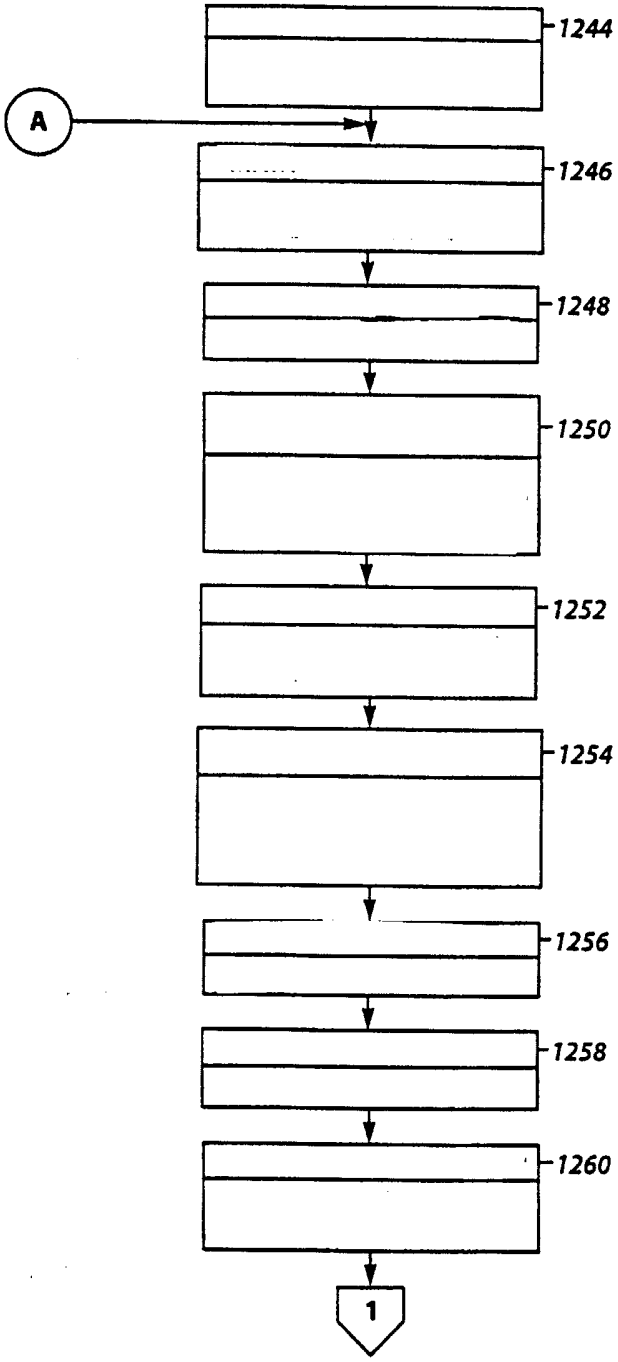
4A. ábra



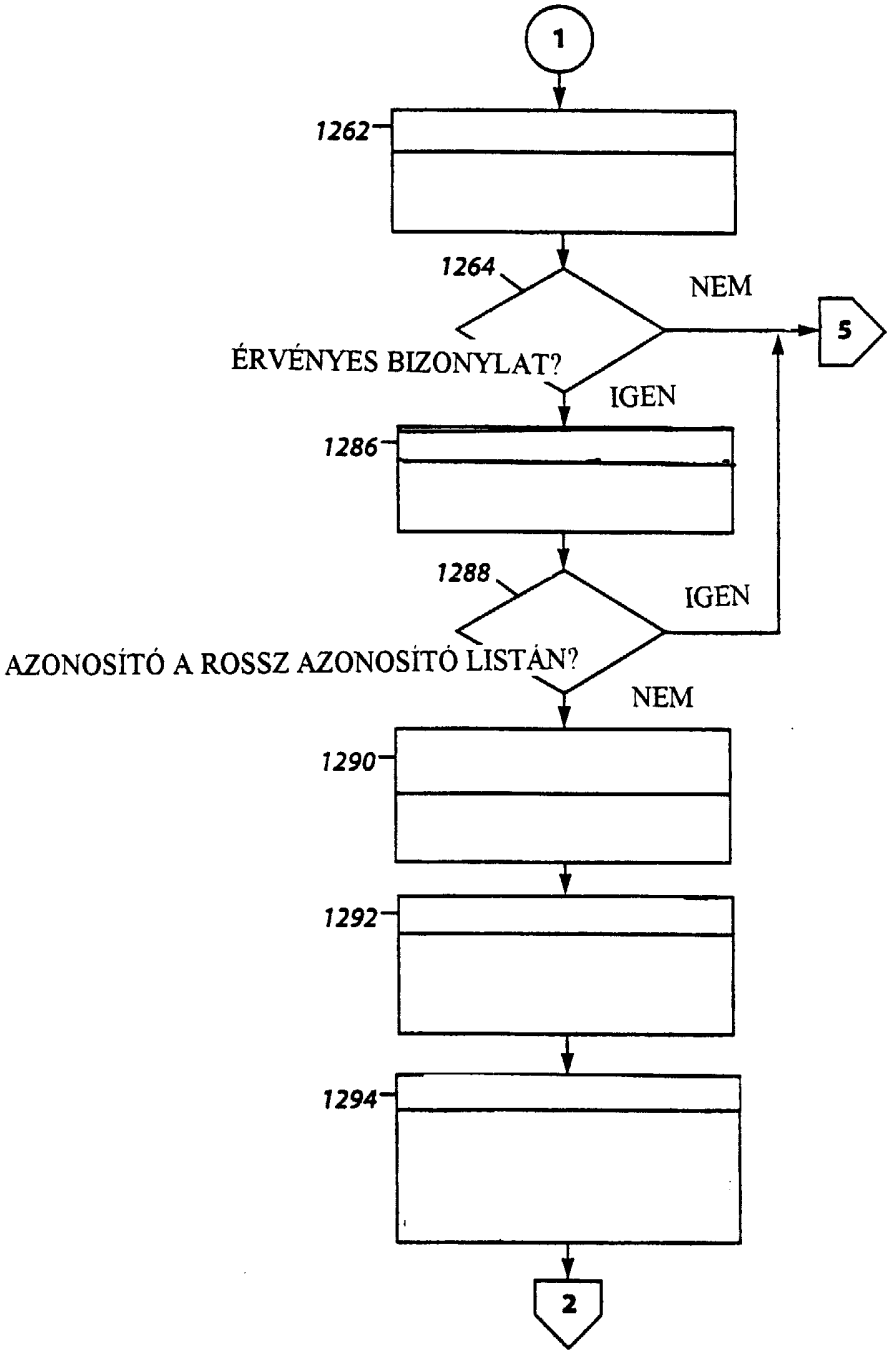
4B. ábra



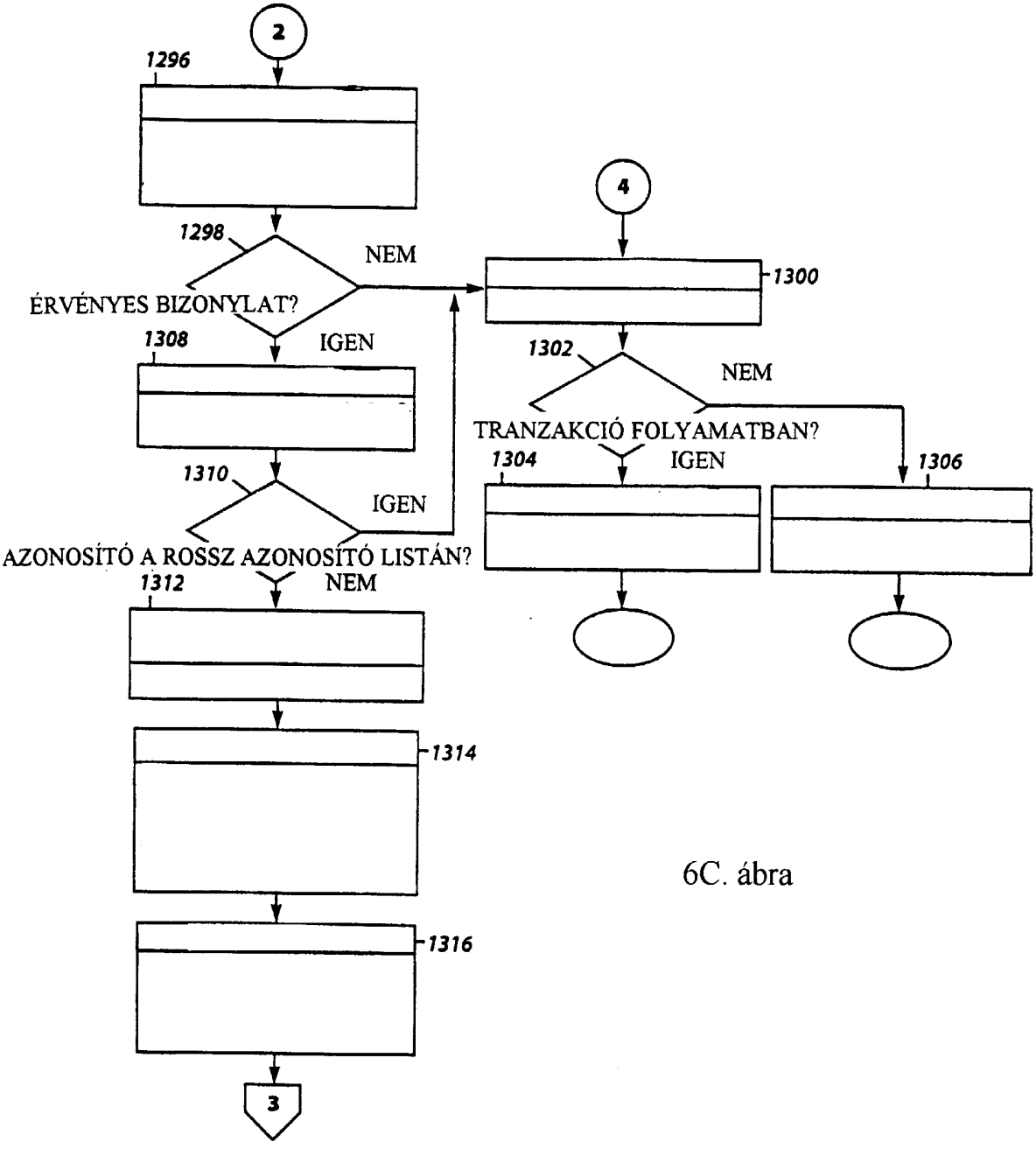
5. ábra



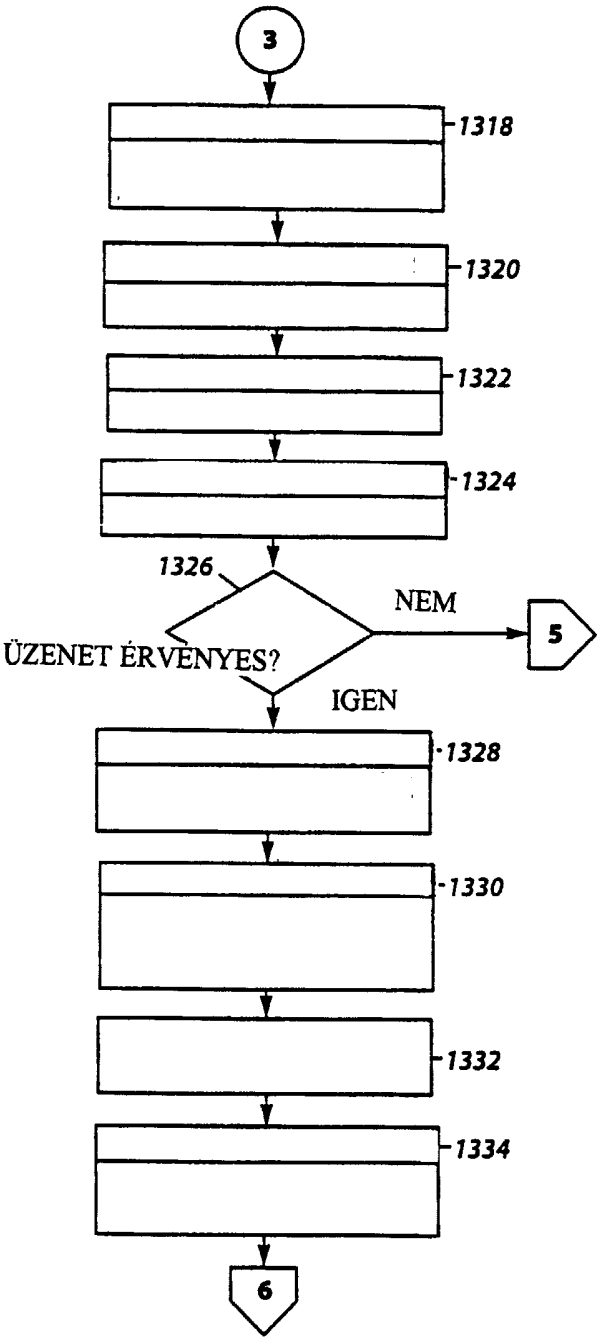
6A. ábra


1
1262
1264
NEM
5
ÉRVÉNYES BIZONYLAT?
IGEN
1286
1288
IGEN
AZONOSÍTÓ A ROSSZ AZONOSÍTÓ LISTÁN?
NEM
1290
1292
1294
2

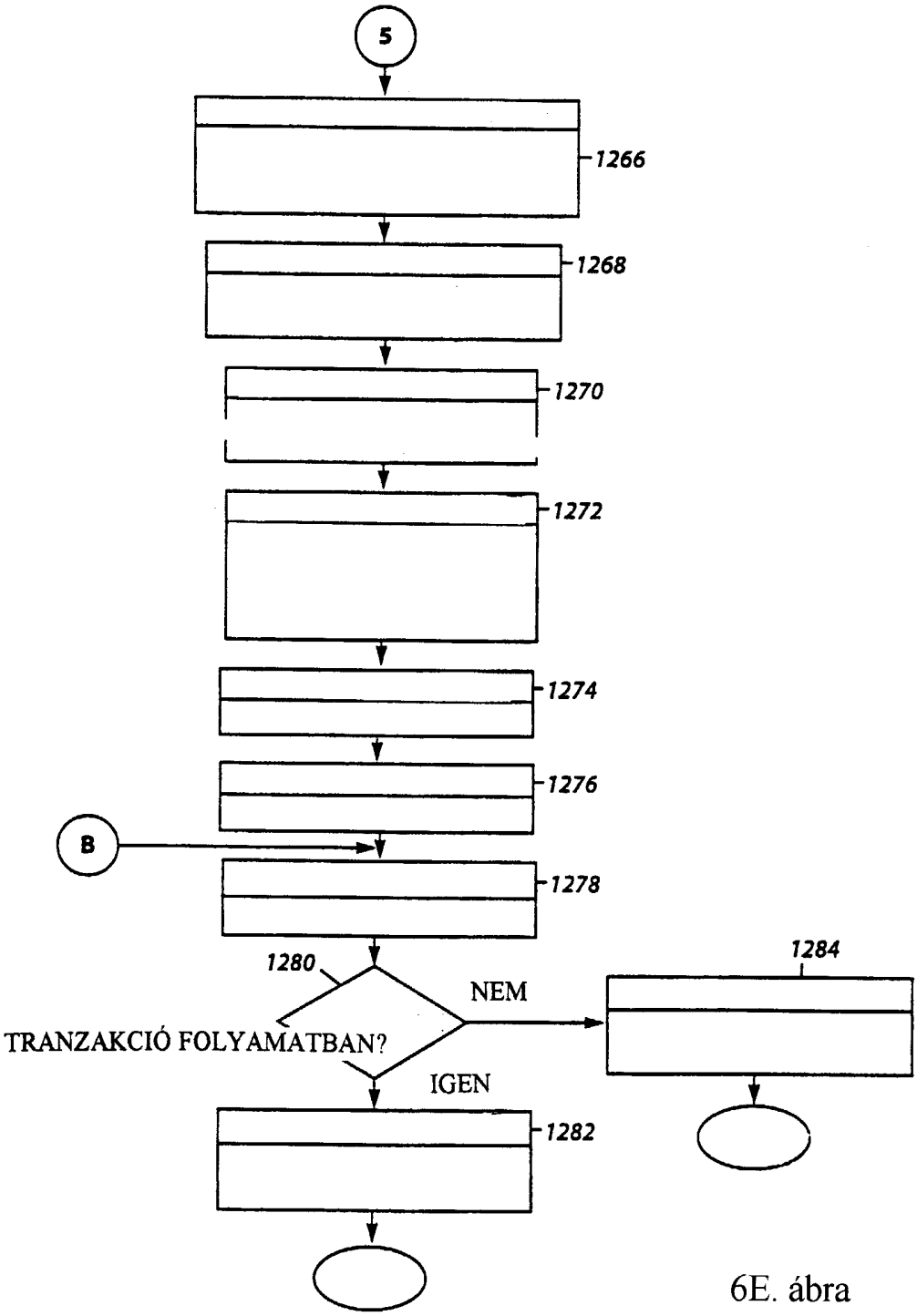
6B. ábra


2
1296
1298
ÉRVÉNYES BIZONYLAT?
NEM
IGEN
1308
1310
AZONOSÍTÓ A ROSSZ AZONOSÍTÓ LISTÁN?
IGEN
NEM
1312
1314
1316
3
4
1300
1302
TRANZAKCIÓ FOLYAMATBAN?
NEM
IGEN
1304
1306

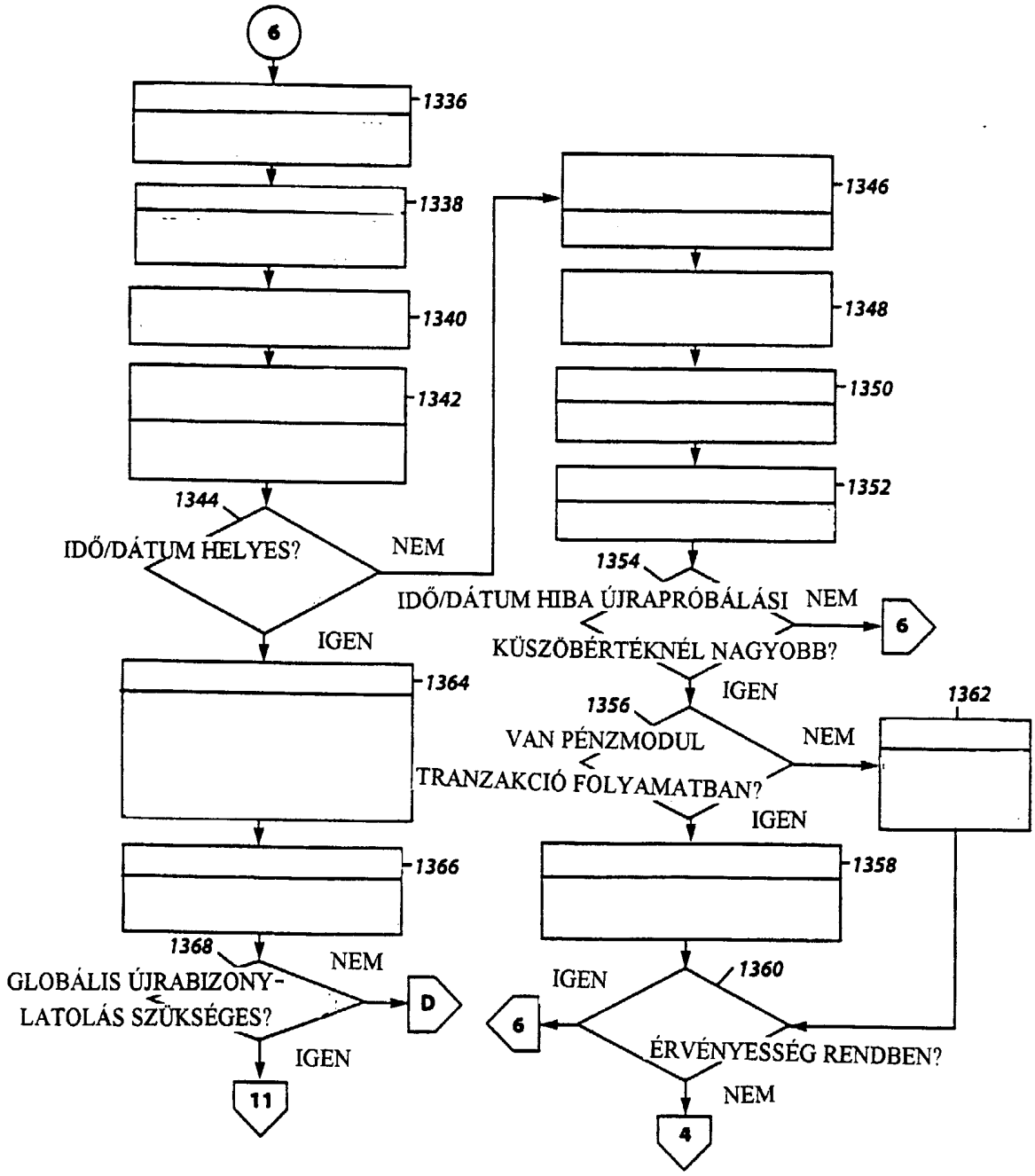
6C. ábra


3
1318
1320
1322
1324
1326
ÜZENET ÉRVÉNYES?
NEM
5
IGEN
1328
1330
1332
1334
6

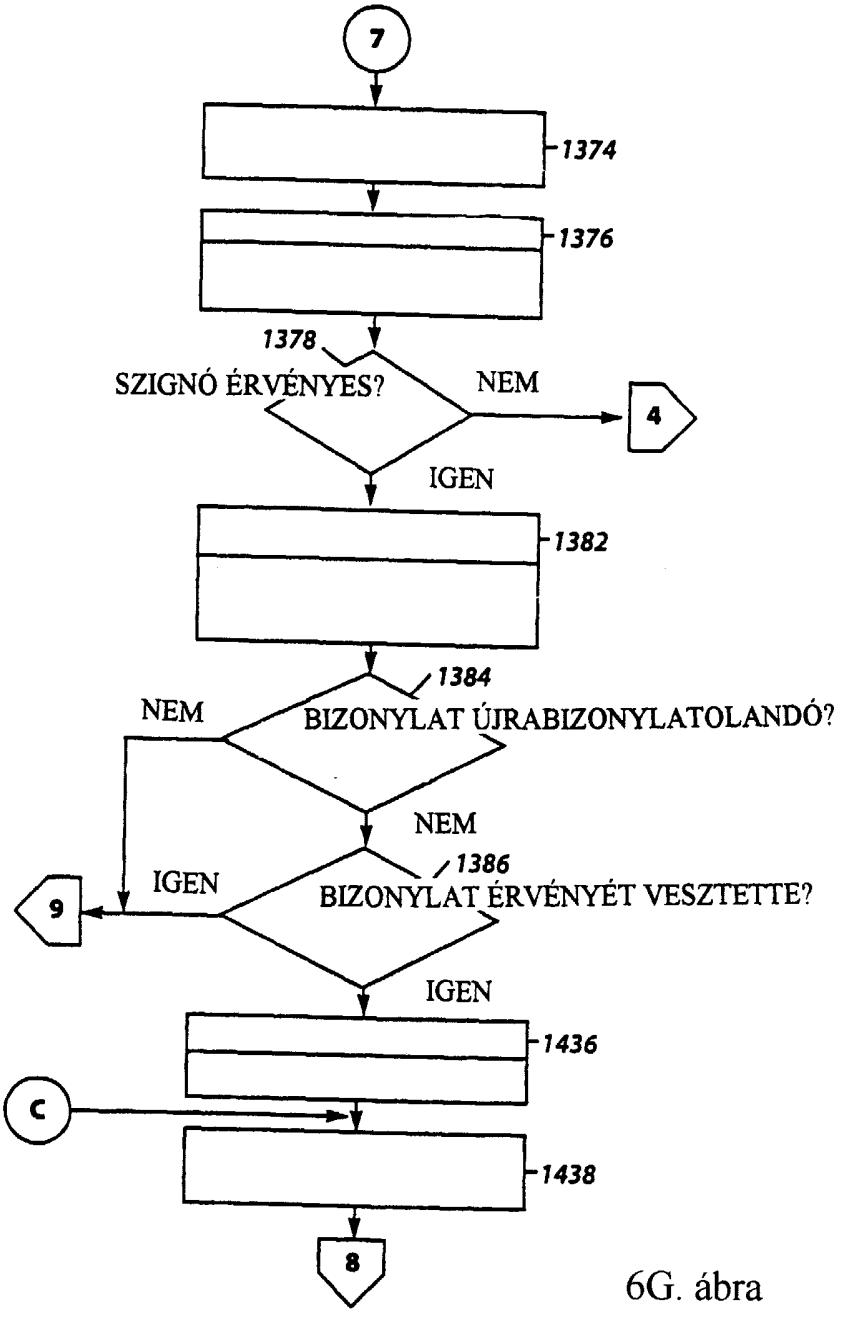
6D. ábra


5
1266
1268
1270
1272
1274
1276
B
1278
1280
TRANZAKCIÓ FOLYAMATBAN?
NEM
IGEN
1284
1282

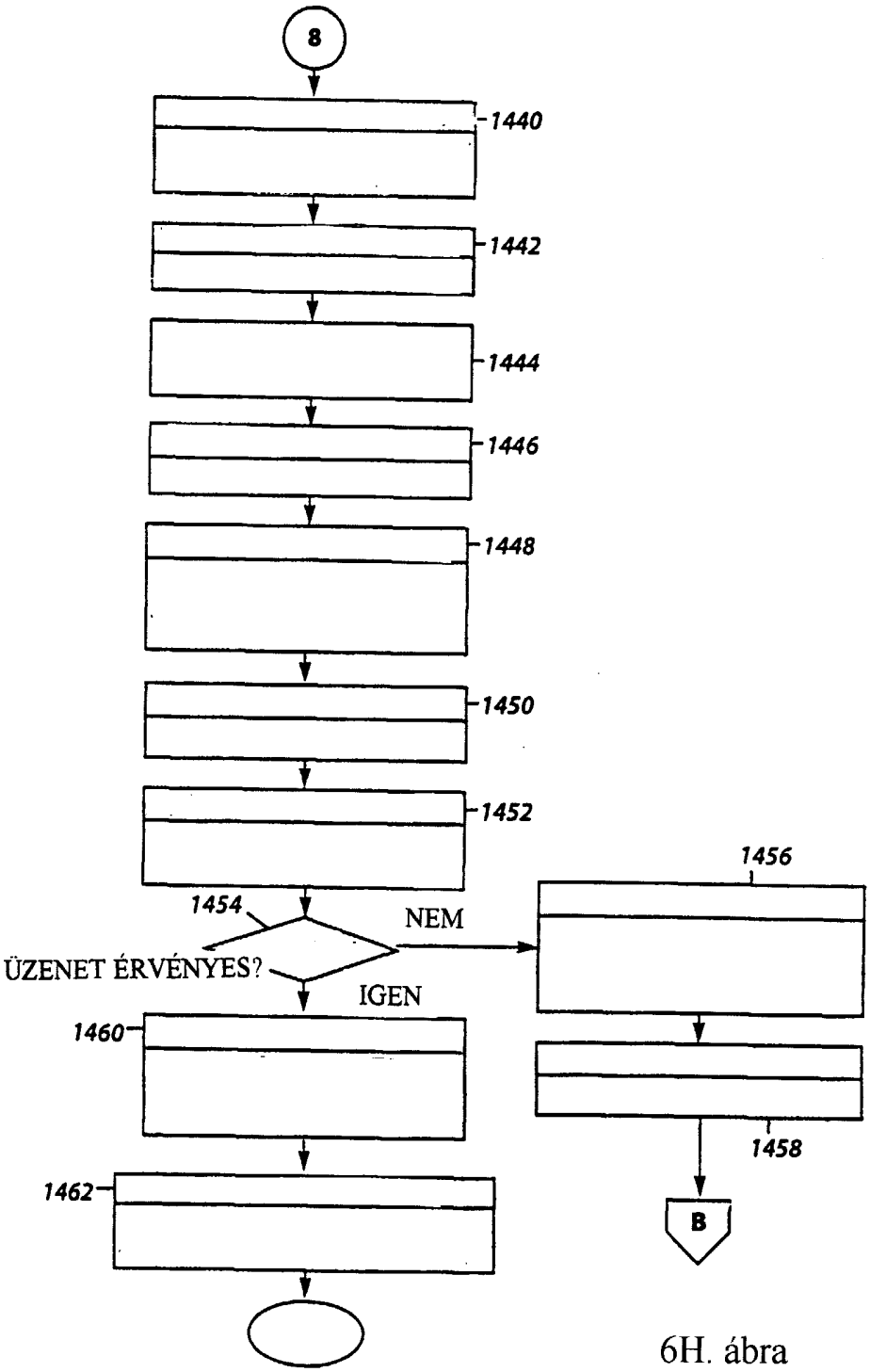
6E. ábra


6
1336
1338
1340
1342
1344
IDŐ/DÁTUM HELYES?
NEM
IGEN
1364
1366
1368
GLOBÁLIS ÚJRABIZONY-
LATOLÁS SZÜKSÉGES?
NEM
D
IGEN
11
1346
1348
1350
1352
1354
IDŐ/DÁTUM HIBA ÚJRAPRÓBÁLÁSI
KÜSZÖBÉRTÉKNÉL NAGYOBB?
NEM
6
IGEN
1356
VAN PÉNZMODUL
TRANZAKCIÓ FOLYAMATBAN?
NEM
1362
IGEN
1358
1360
IGEN
6
ÉRVÉNYESSÉG RENDBEN?
NEM
4

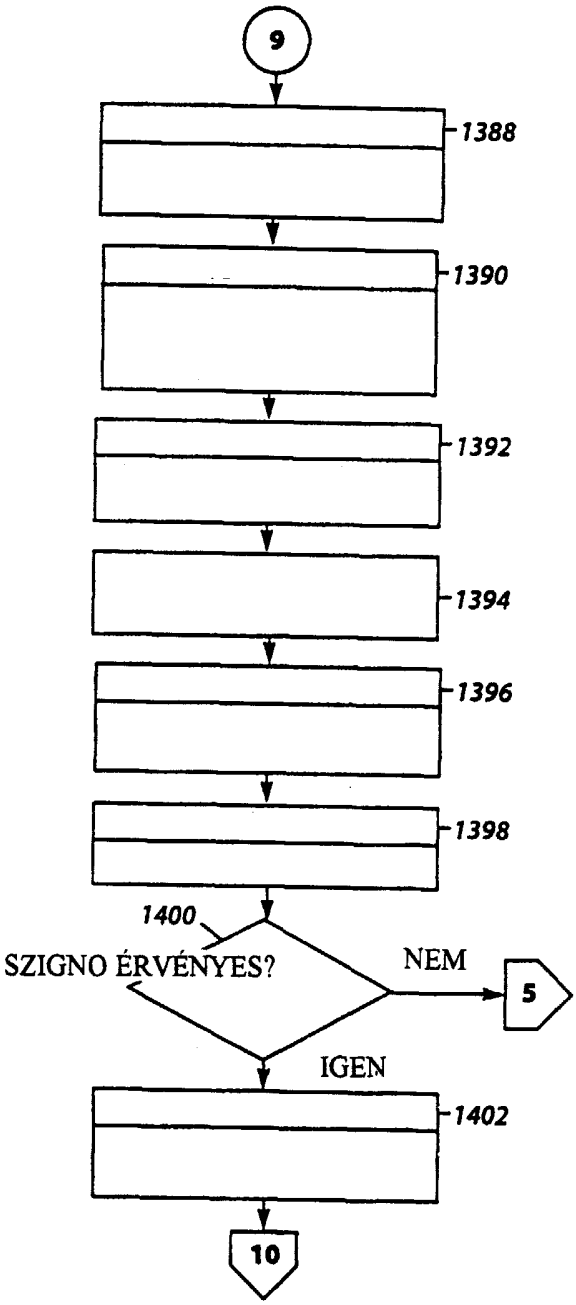
6F. ábra


7
1374
1376
1378
SZIGNÓ ÉRVÉNYES?
NEM
4
IGEN
1382
1384
NEM
BIZONYLAT ÚJRABIZONYLATOLANDÓ?
NEM
1386
IGEN
9
BIZONYLAT ÉRVÉNYÉT VESZTETTE?
IGEN
1436
C
1438
8

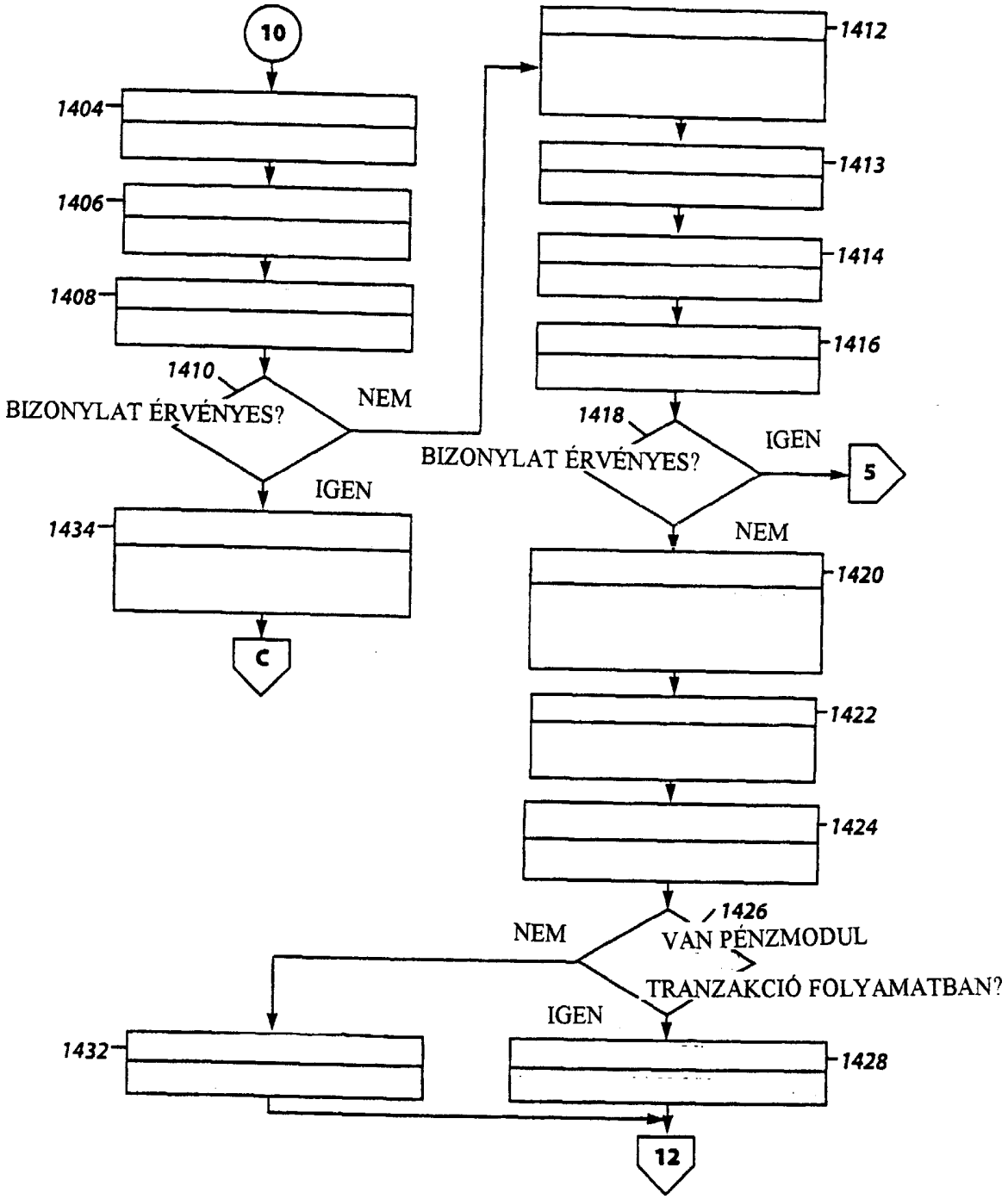
6G. ábra


8
1440
1442
1444
1446
1448
1450
1452
1454
ÜZENET ÉRVÉNYES?
NEM
IGEN
1456
1458
1460
1462
B

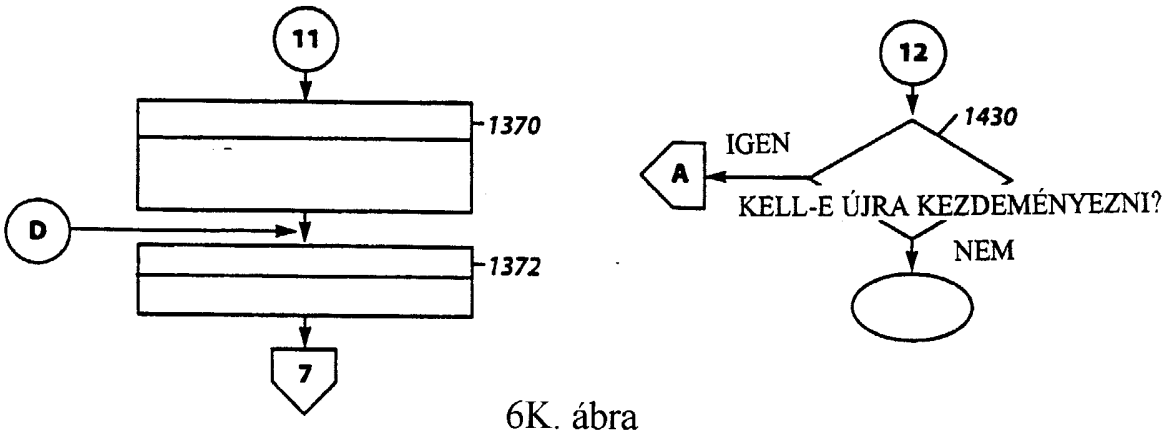
6H. ábra


9
1388
1390
1392
1394
1396
1398
1400
SZIGNO ÉRVÉNYES?
NEM
5
IGEN
1402
10

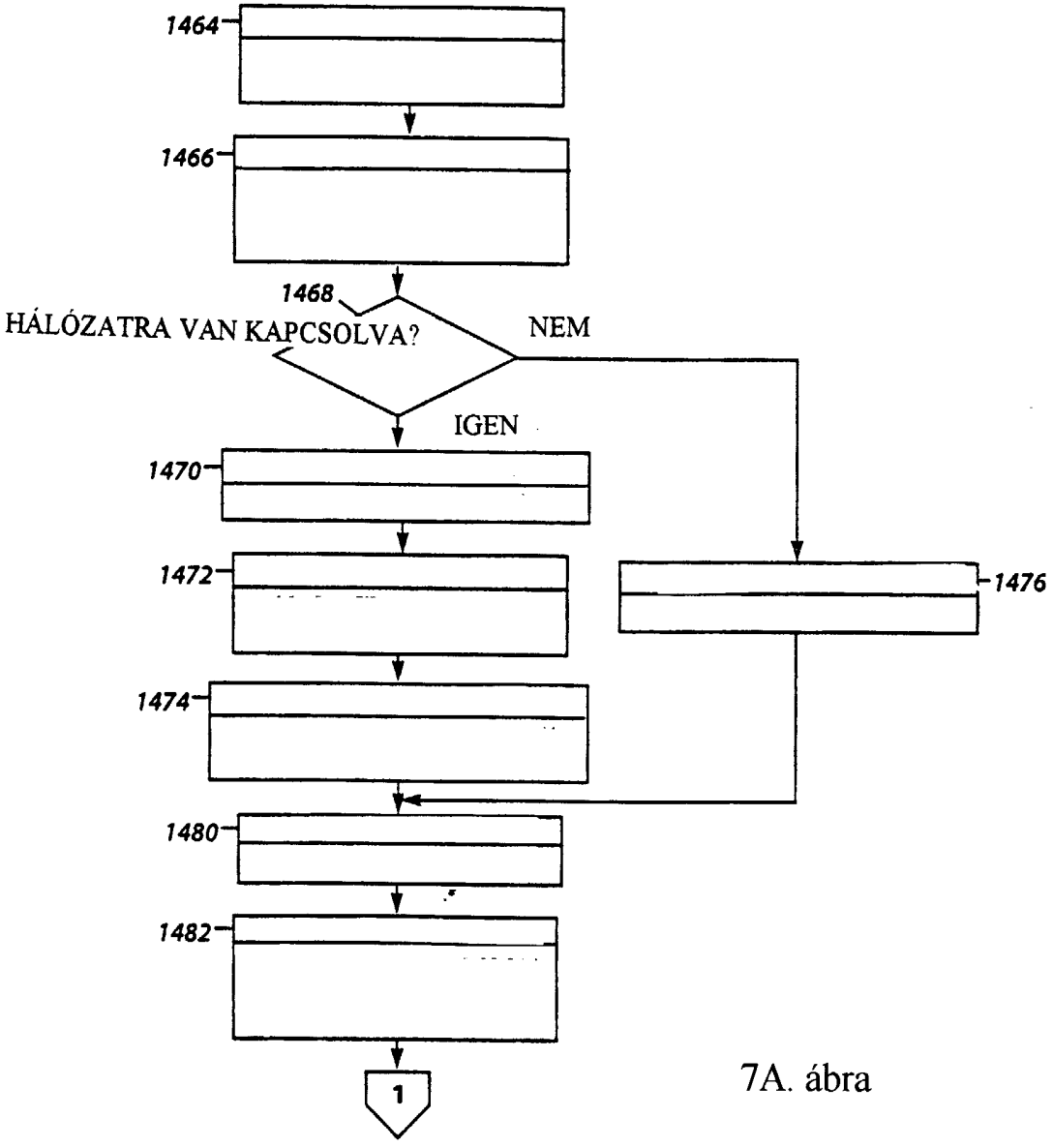
6I. ábra


10
1404
1406
1408
1410
BIZONYLAT ÉRVÉNYES?
NEM
IGEN
1434
C
1412
1413
1414
1416
1418
BIZONYLAT ÉRVÉNYES?
IGEN
5
NEM
1420
1422
1424
1426
NEM
VAN PÉNZMODUL
TRANZAKCIÓ FOLYAMATBAN?
IGEN
1432
1428
12

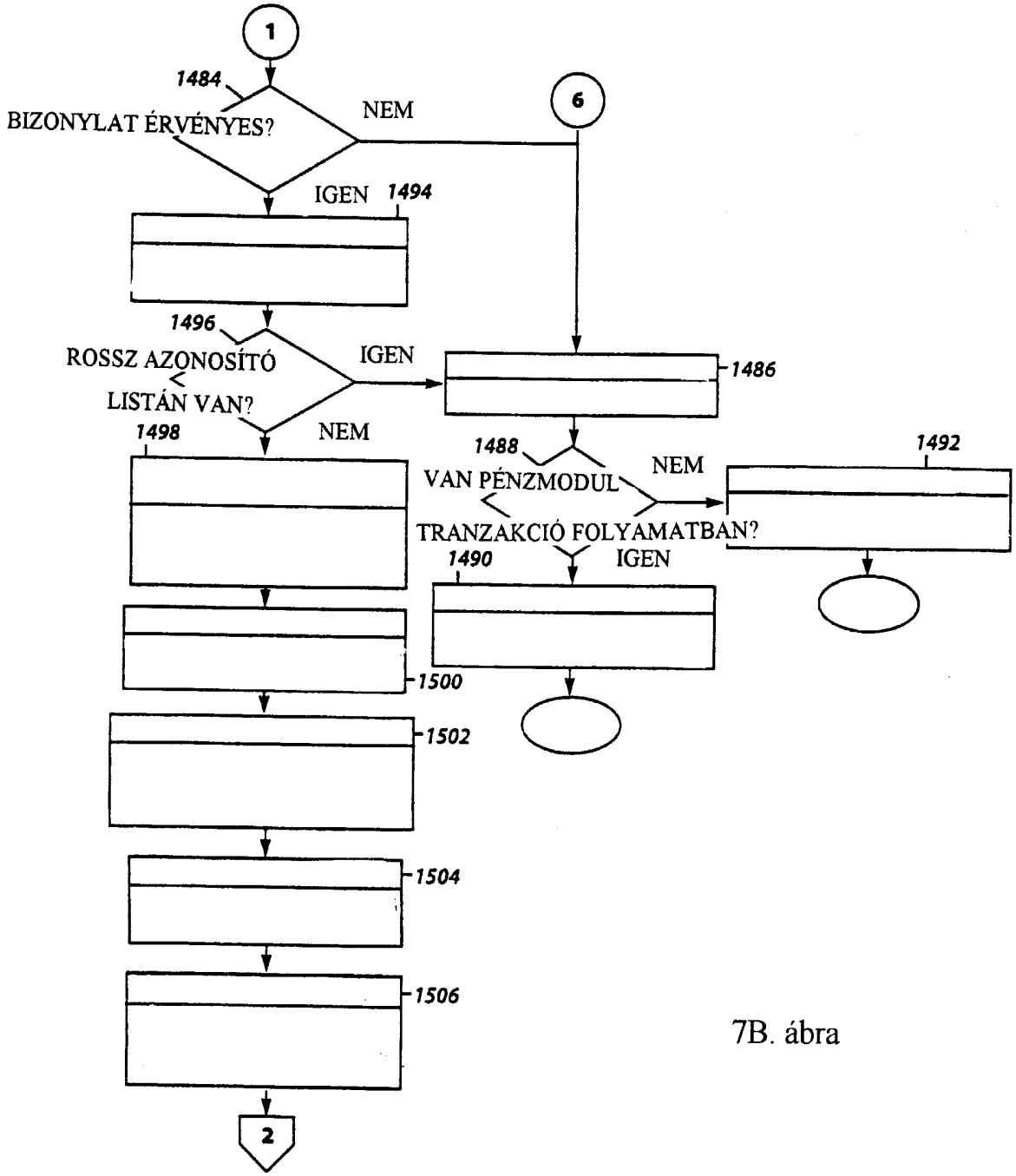
6J. ábra



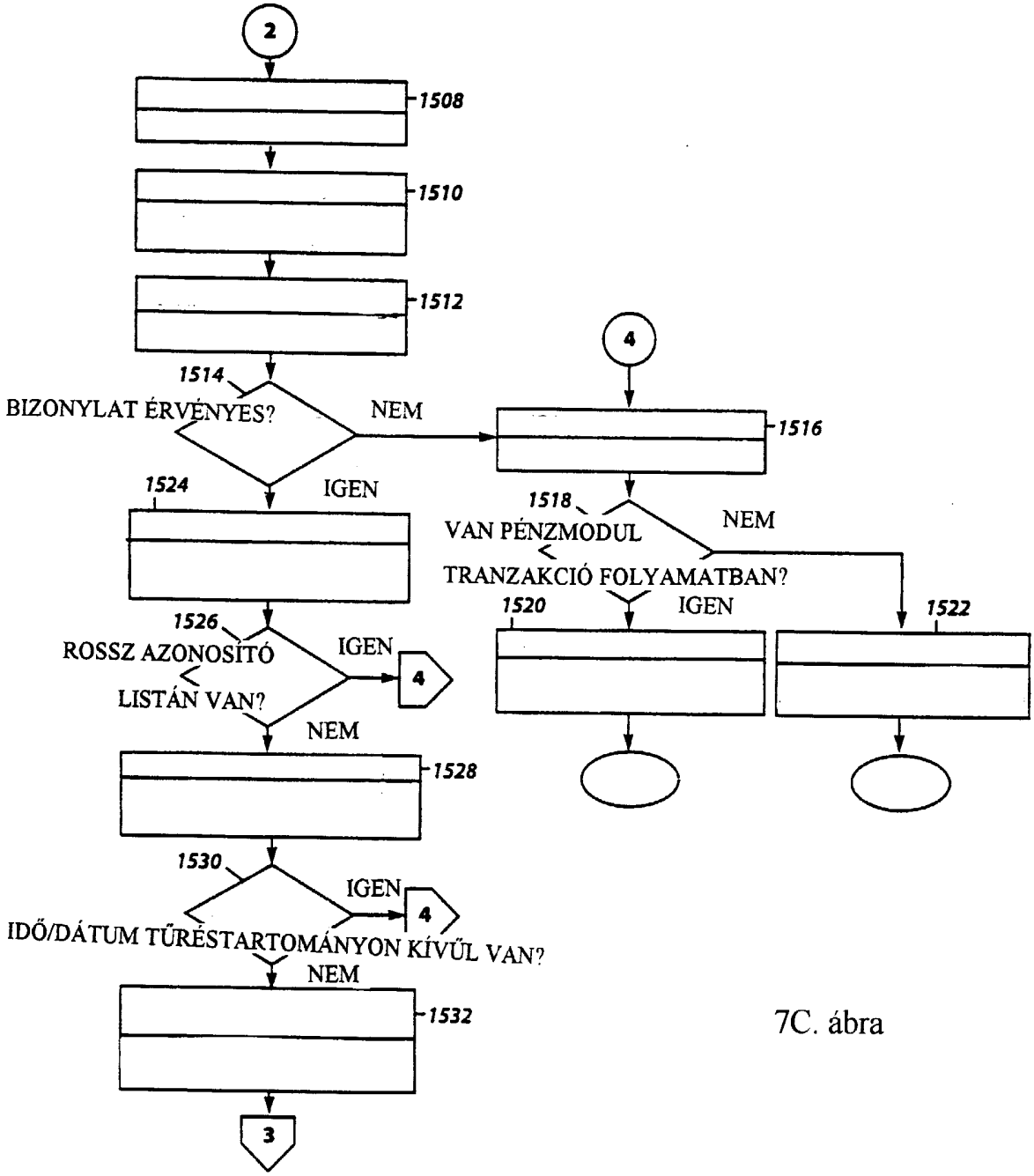
6K. ábra


1464
1466
1468
HÁLÓZATRA VAN KAPCSOLVA?
NEM
IGEN
1470
1472
1474
1476
1480
1482
1

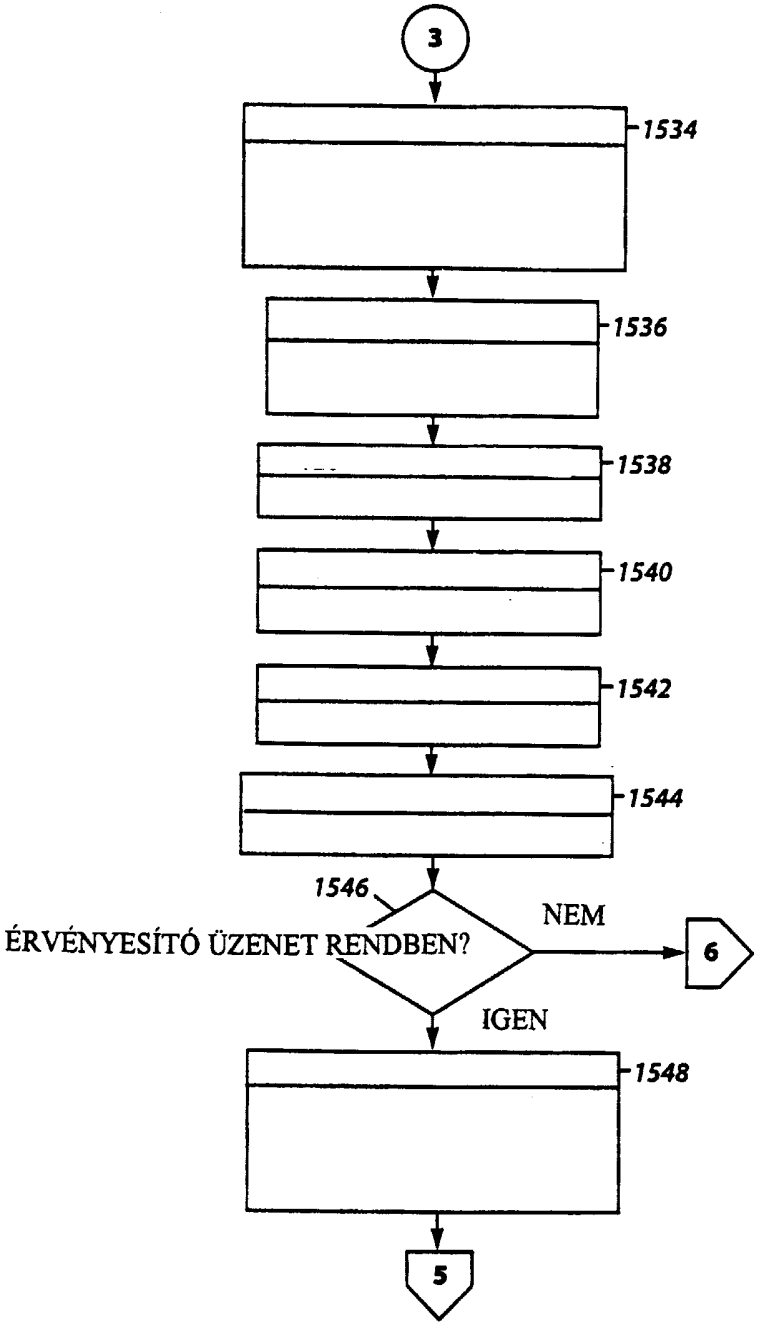
7A. ábra


1
1484
BIZONYLAT ÉRVÉNYES?
NEM
6
IGEN
1494
1496
ROSSZ AZONOSÍTÓ
LISTÁN VAN?
IGEN
1486
1498
NEM
1488
VAN PÉNZMODUL
NEM
1492
TRANZAKCIÓ FOLYAMATBAN?
1490
IGEN
1500
1502
1504
1506
2

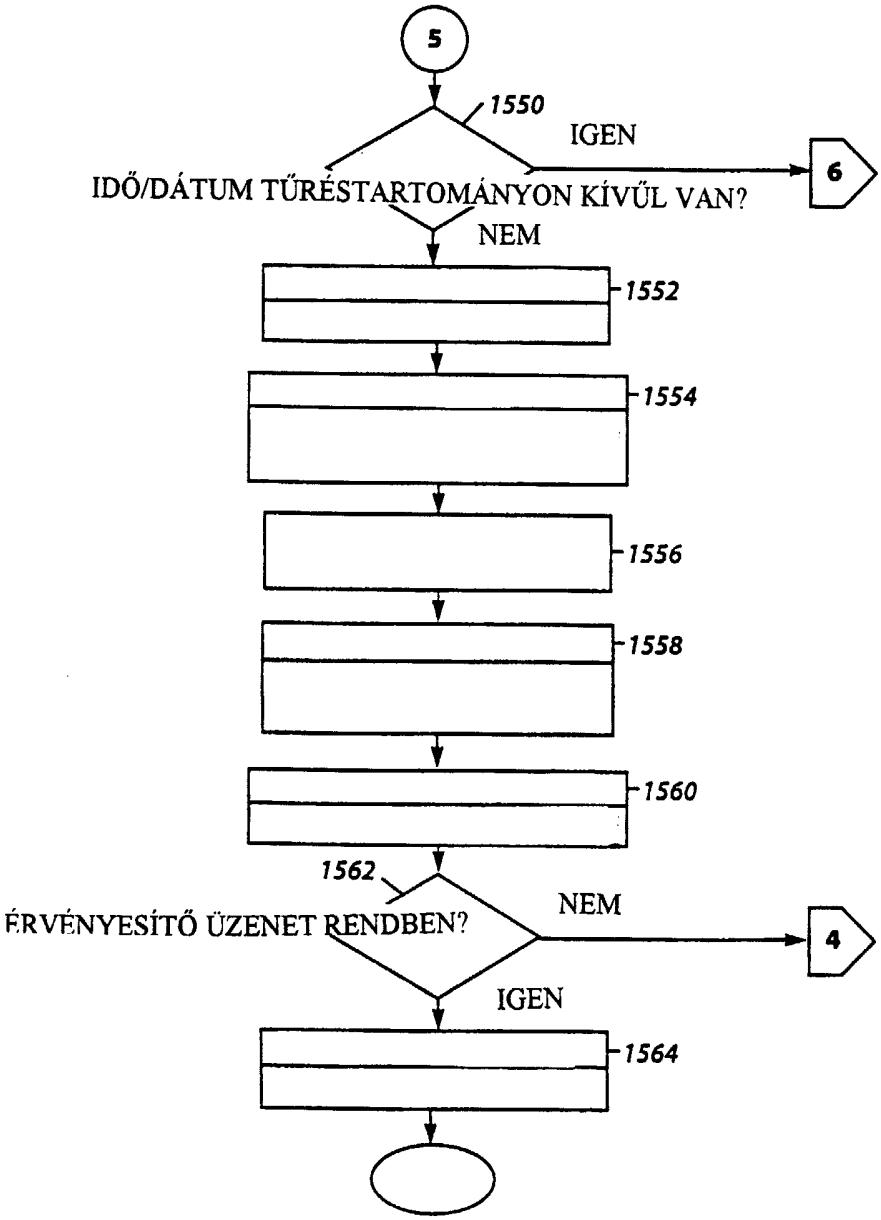
7B. ábra


2
1508
1510
1512
1514
BIZONYLAT ÉRVÉNYES?
NEM
IGEN
4
1516
1518
VAN PÉNZMODUL TRANZAKCIÓ FOLYAMATBAN?
NEM
IGEN
1520
1522
1524
1526
ROSSZ AZONOSÍTÓ LISTÁN VAN?
IGEN
4
NEM
1528
1530
IGEN
4
IDŐ/DÁTUM TŰRÉSTARTOMÁNYON KÍVÜL VAN?
NEM
1532
3

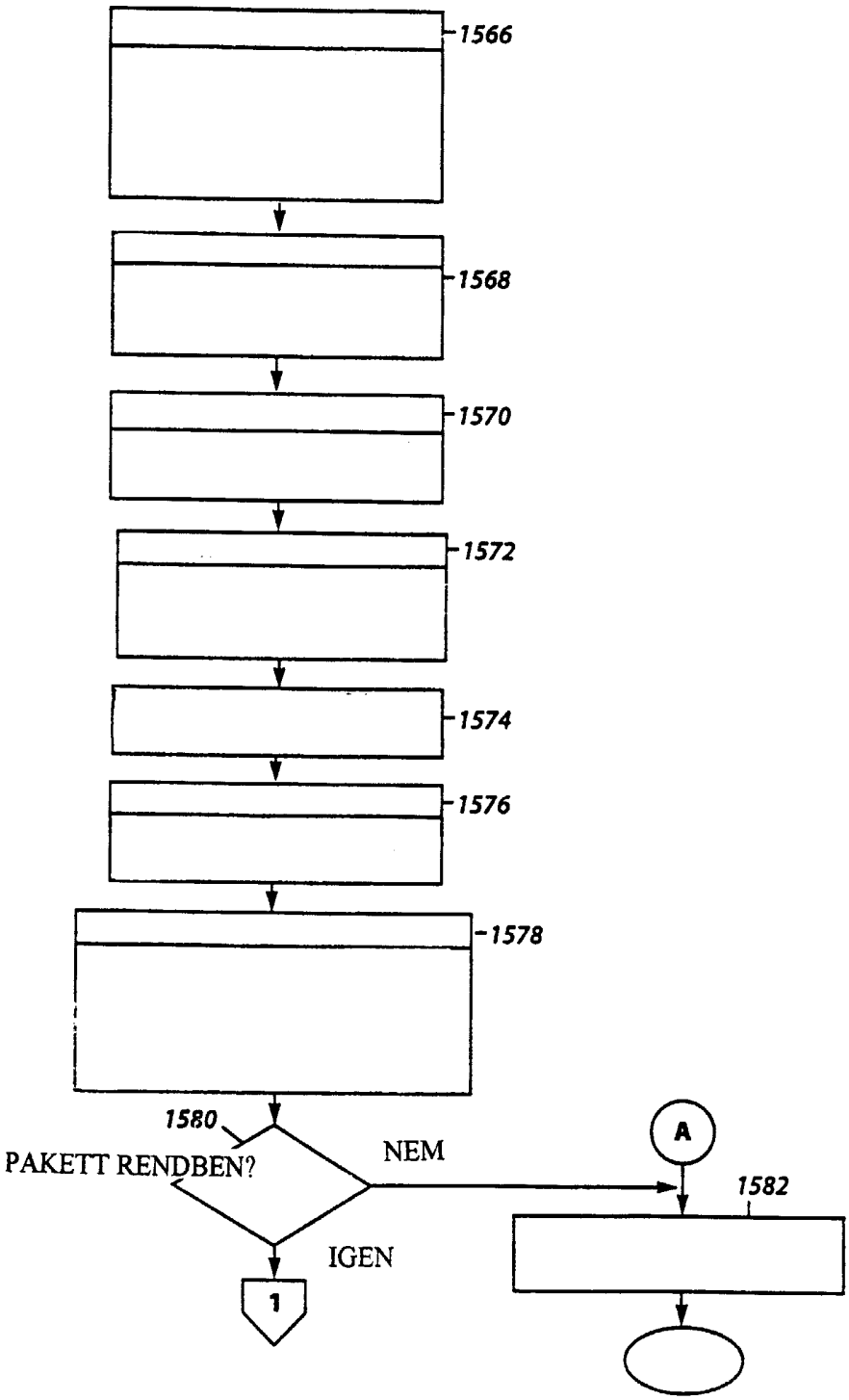
7C. ábra


3
1534
1536
1538
1540
1542
1544
1546
ÉRVÉNYESÍTŐ ÜZENET RENDBEN?
NEM
6
IGEN
1548
5

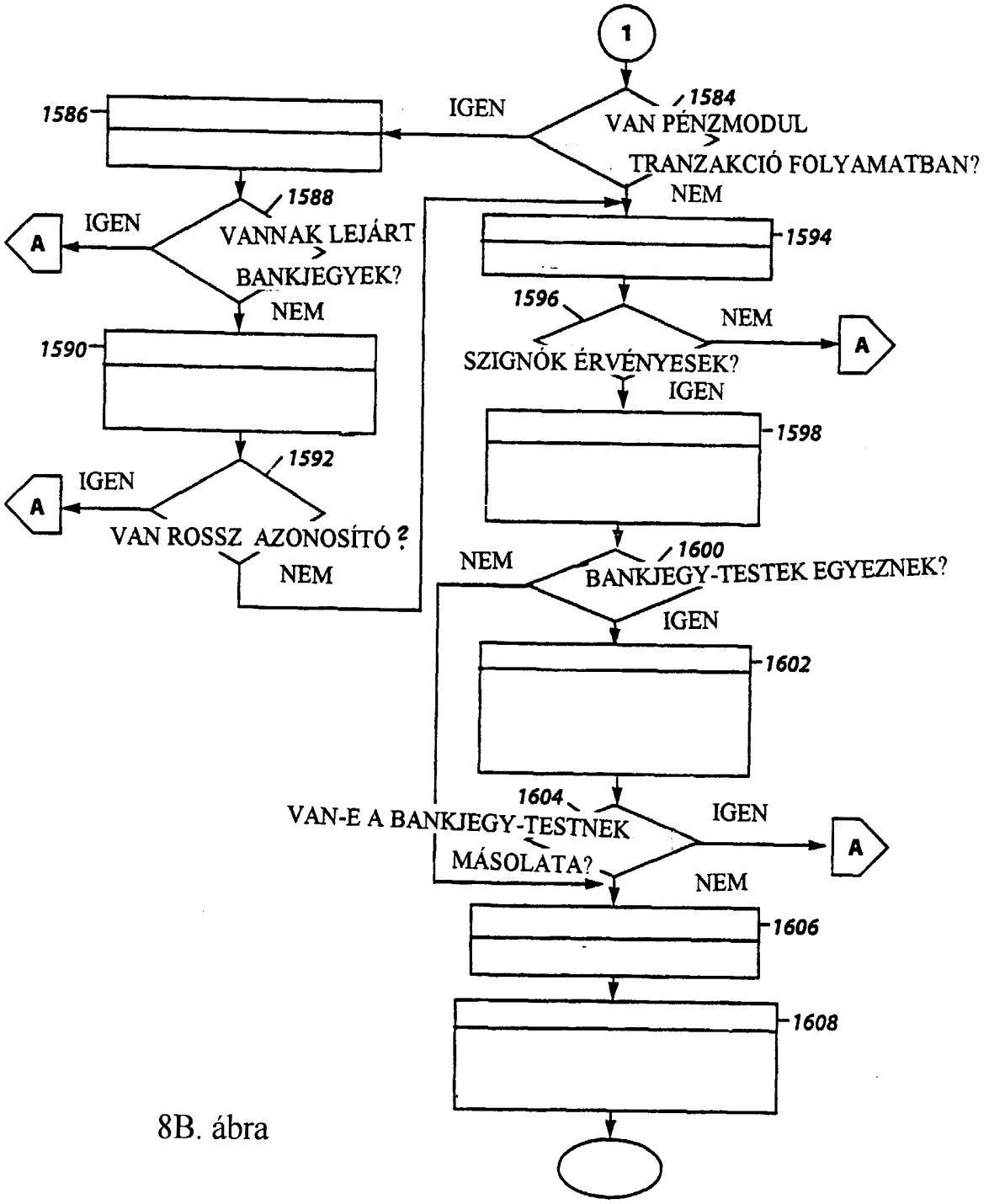
7D. ábra


5
1550
IGEN
6
IDŐ/DÁTUM TŰRÉSTARTOMÁNYON KÍVŰL VAN?
NEM
1552
1554
1556
1558
1560
1562
ÉRVÉNYESÍTŐ ÜZENET RENDBEN?
NEM
4
IGEN
1564

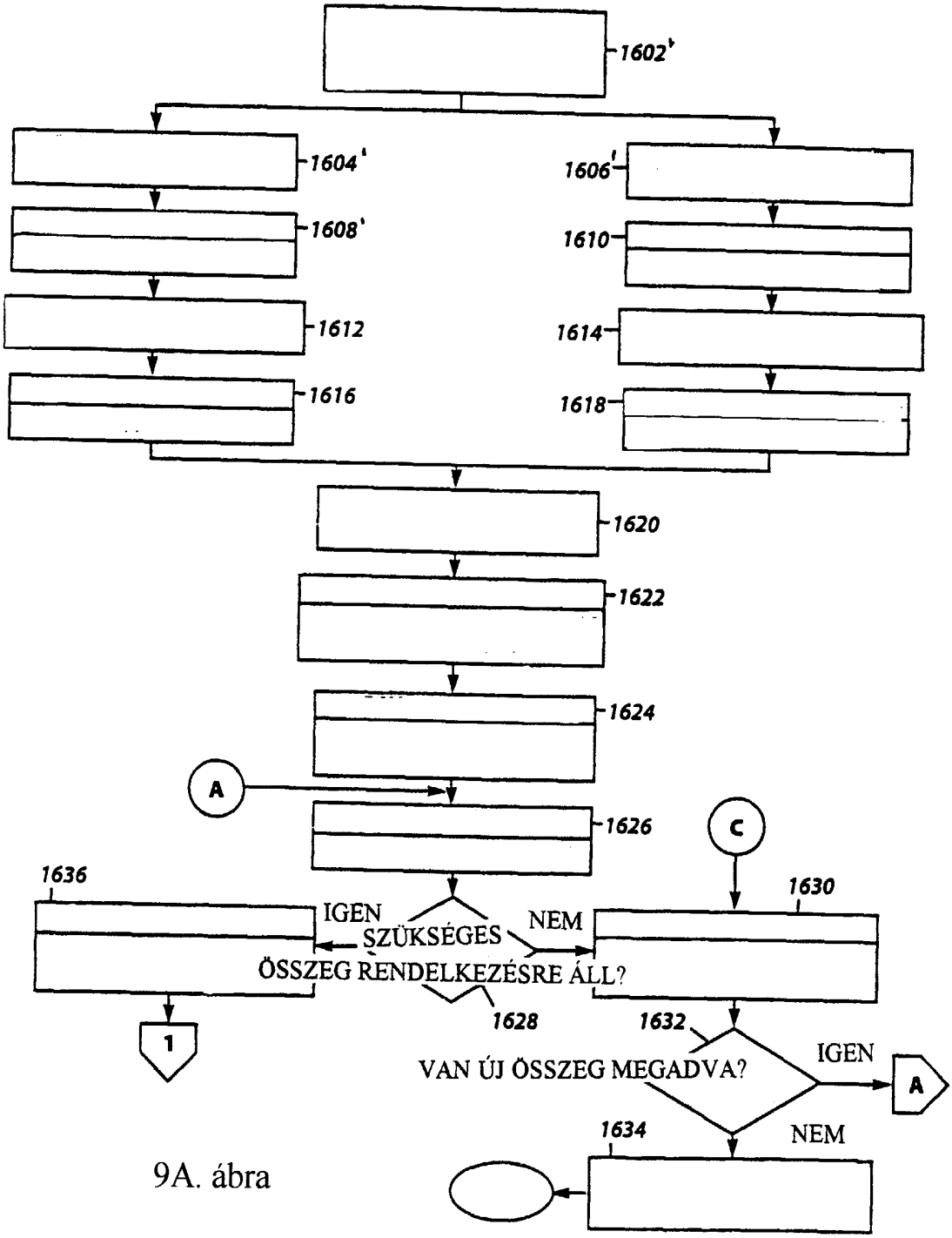
7E. ábra


1566
1568
1570
1572
1574
1576
1578
1580
PAKETT RENDBEN?
NEM
IGEN
A
1582
1

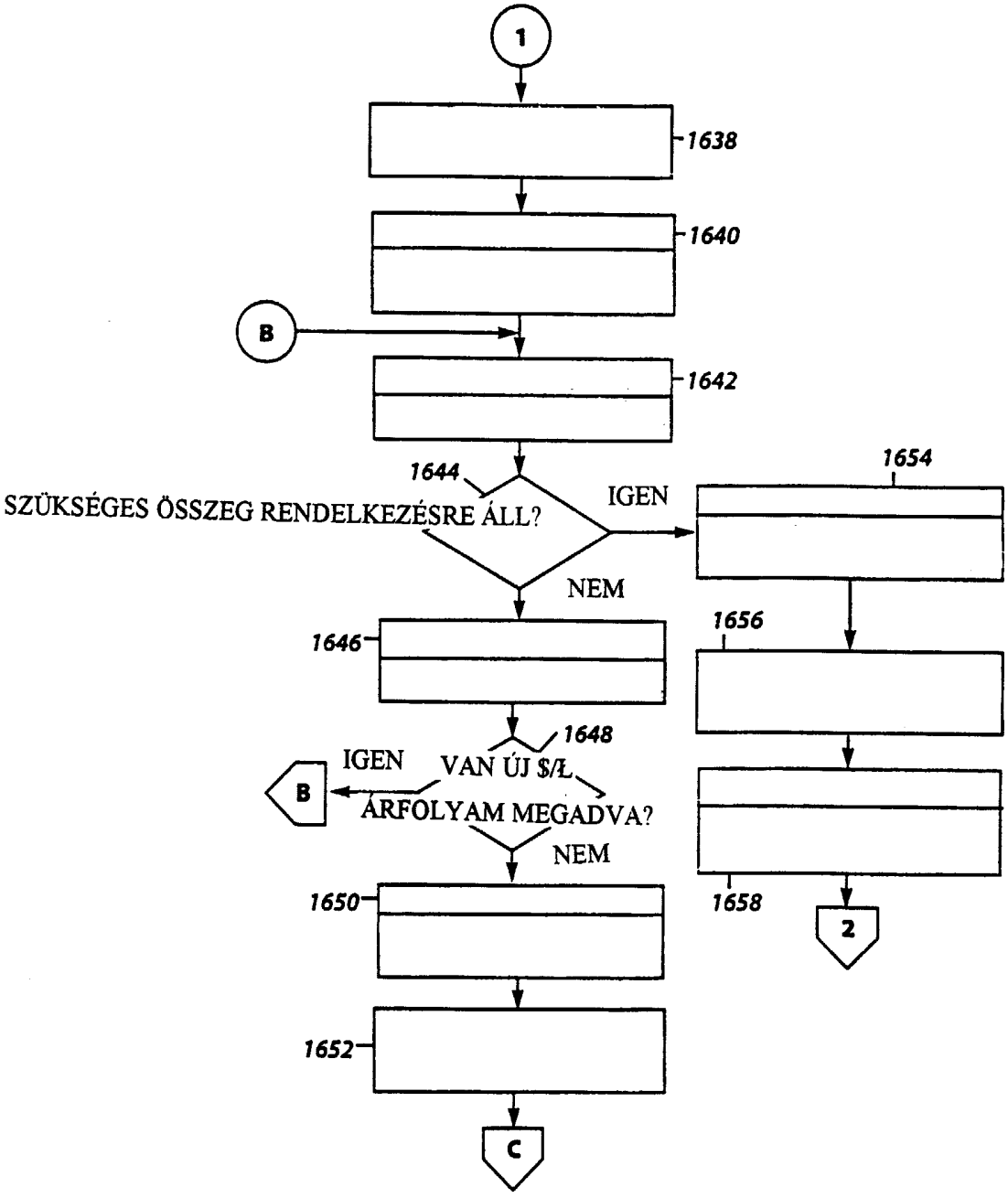
8A. ábra


1
1584
VAN PÉNZMODUL
TRANZAKCIÓ FOLYAMATBAN?
IGEN
1586
NEM
1588
VANNAK LEJÁRT
BANKJEGYEK?
IGEN
A
NEM
1590
1592
VAN ROSSZ AZONOSÍTÓ ?
IGEN
A
NEM
1594
1596
SZIGNÓK ÉRVÉNYESEK?
NEM
A
IGEN
1598
1600
BANKJEGY-TESTEK EGYEZNEK?
NEM
IGEN
1602
1604
VAN-E A BANKJEGY-TESTNEK
MÁSOLATA?
IGEN
A
NEM
1606
1608

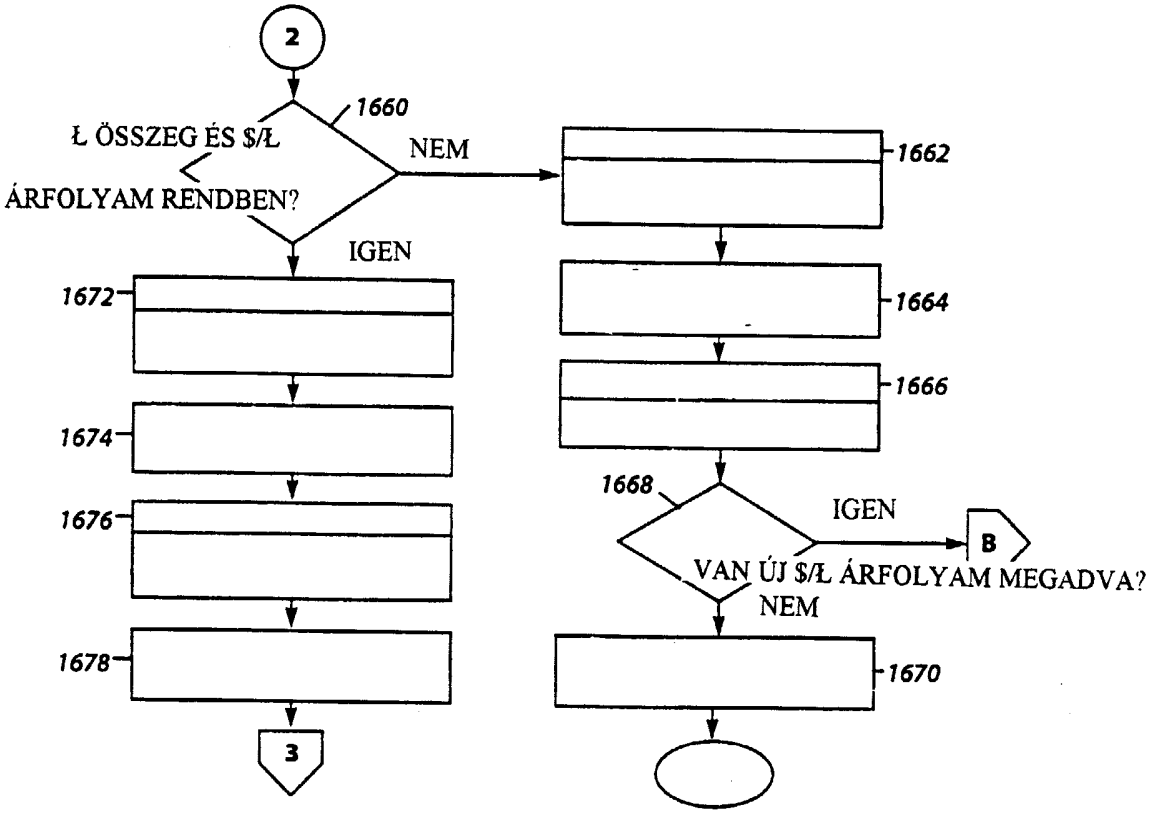
8B. ábra


1602'
1604'
1606'
1608'
1610
1612
1614
1616
1618
1620
1622
1624
A
1626
C
1636
1630
IGEN
NEM
SZÜKSÉGES
ÖSSZEG RENDELKEZÉSRE ÁLL?
1628
1632
1
VAN ÚJ ÖSSZEG MEGADVA?
IGEN
A
1634
NEM

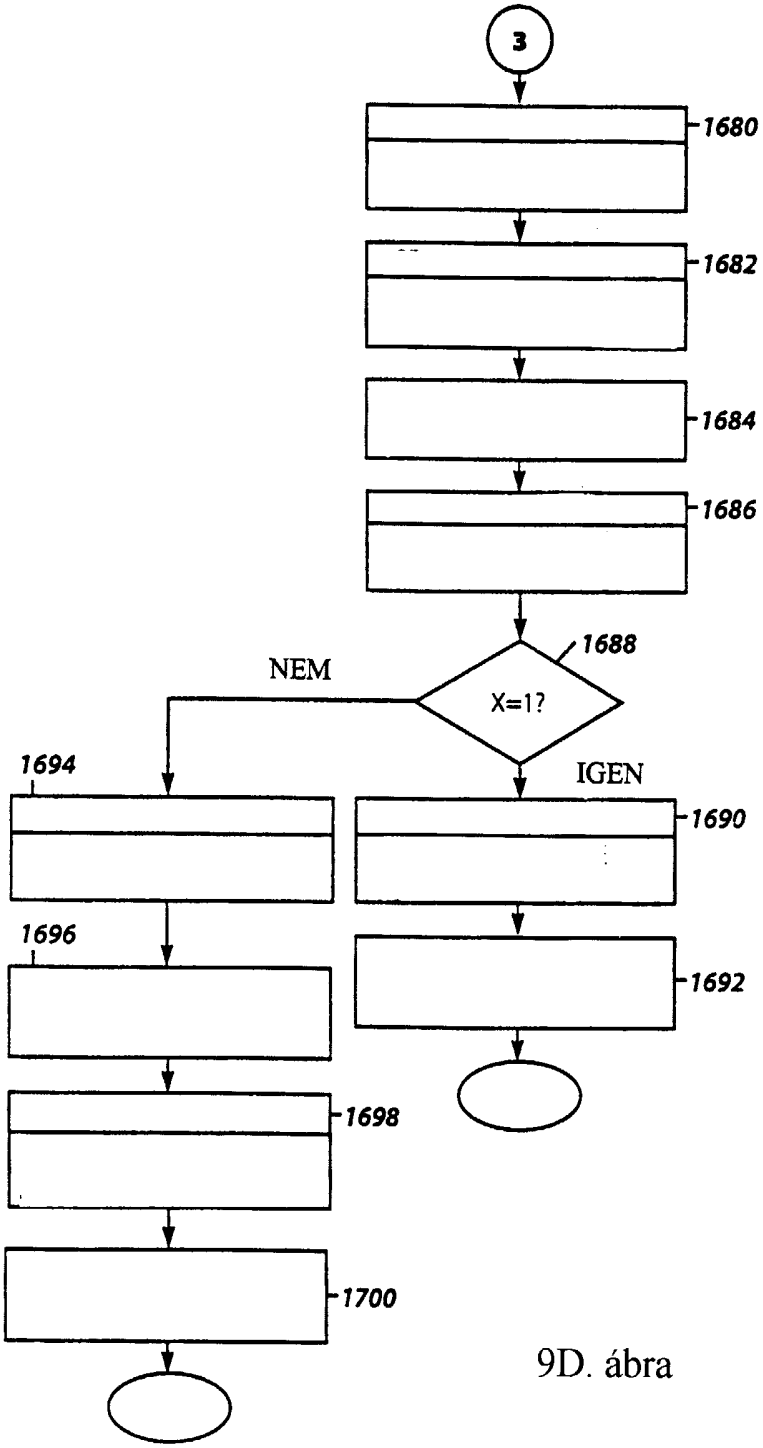
9A. ábra


1
1638
1640
B
1642
1644
SZÜKSÉGES ÖSSZEG RENDELKEZÉSRE ÁLL?
IGEN
1654
NEM
1646
1656
1648
IGEN
VAN ÚJ $/Ł
B
ÁRFOLYAM MEGADVA?
NEM
1650
1658
2
1652
C

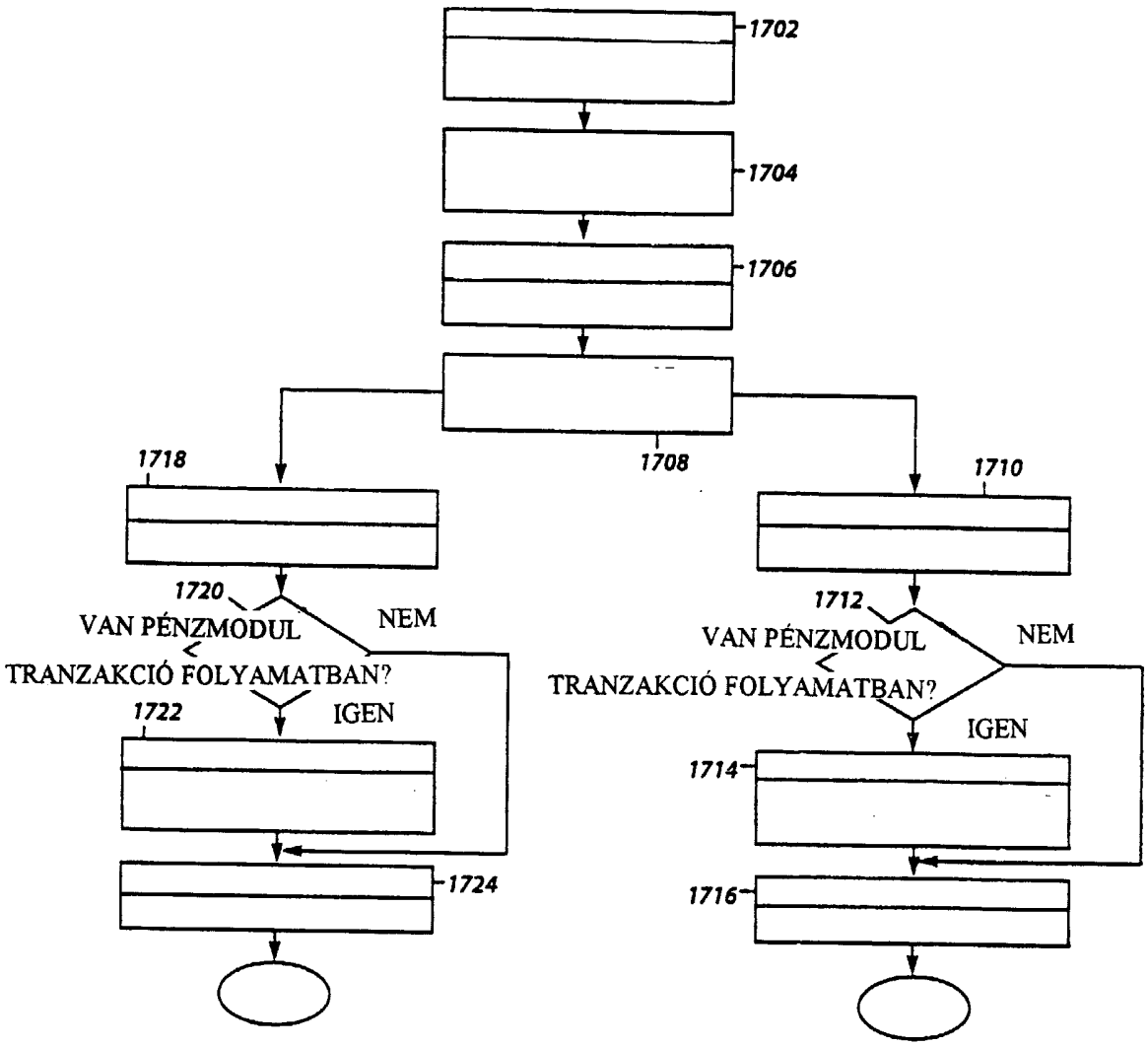
9B. ábra


2
1660
Ł ÖSSZEG ÉS $/Ł ÁRFOLYAM RENDBEN?
NEM
IGEN
1662
1664
1666
1668
IGEN
B
VAN ÚJ $/Ł ÁRFOLYAM MEGADVA?
NEM
1670
1672
1674
1676
1678
3

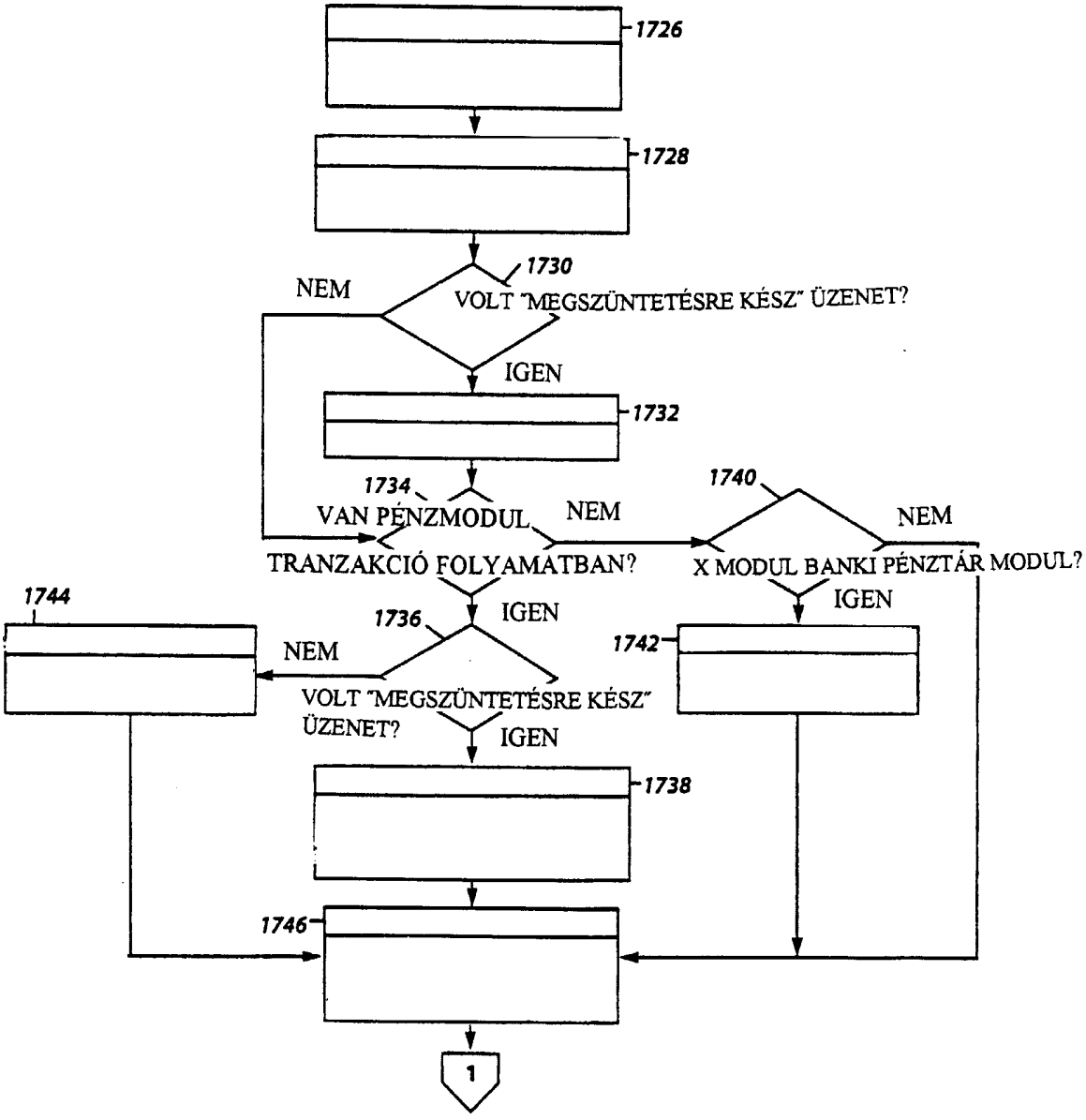
9C. ábra


3
1680
1682
1684
1686
1688
X=1?
NEM
IGEN
1694
1690
1696
1692
1698
1700

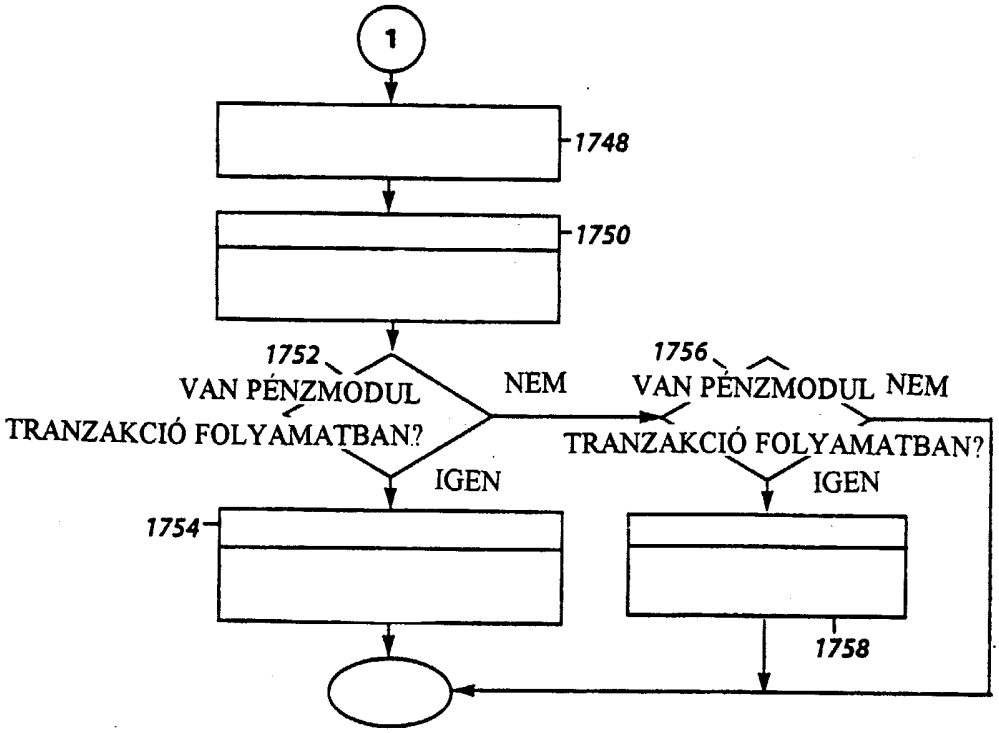
9D. ábra


1702
1704
1706
1708
1710
1712
VAN PÉNZMODUL
TRANZAKCIÓ FOLYAMATBAN?
NEM
IGEN
1714
1716
1718
1720
VAN PÉNZMODUL
TRANZAKCIÓ FOLYAMATBAN?
NEM
1722
IGEN
1724

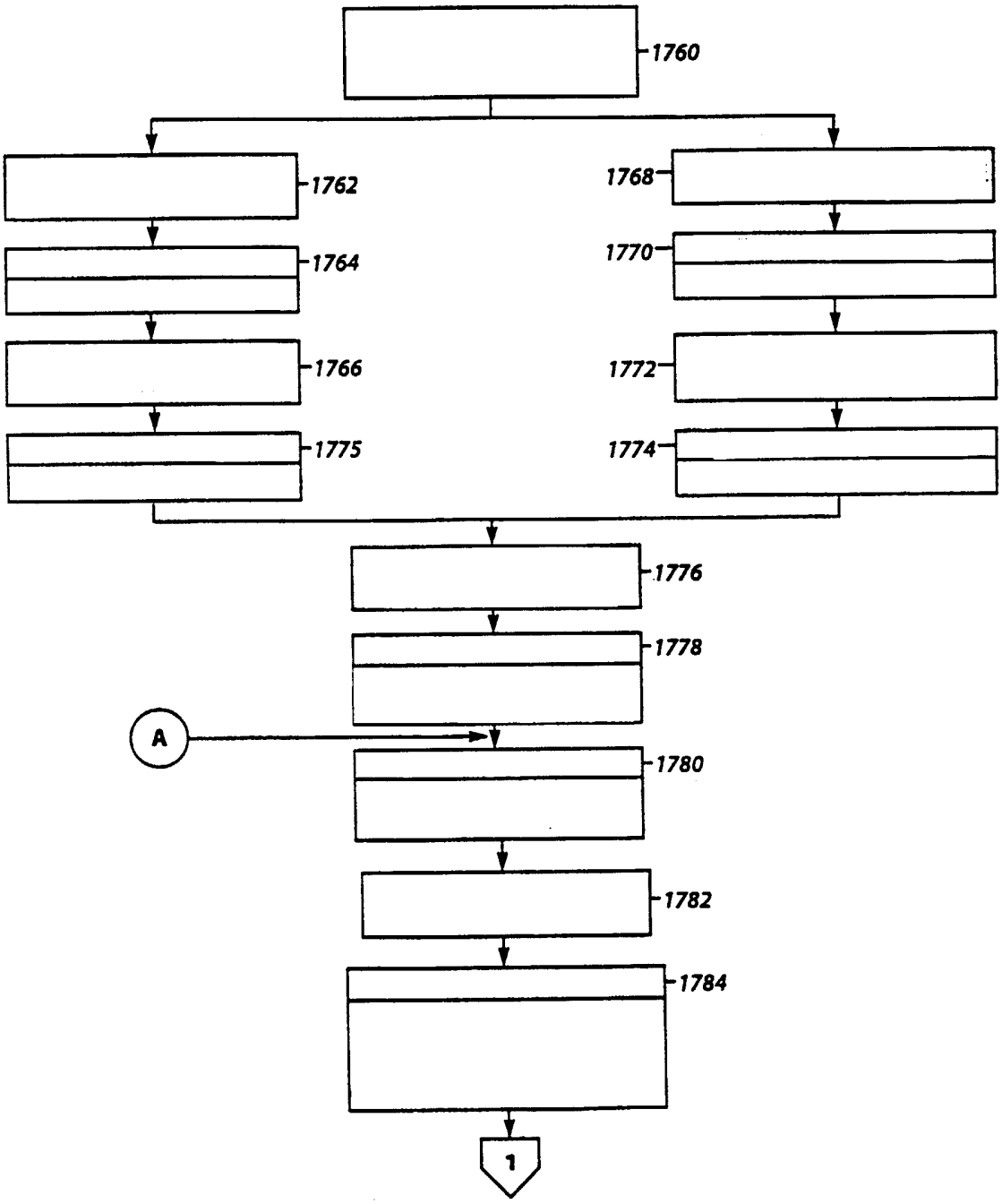
10. ábra


1726
1728
1730
NEM
VOLT "MEGSZÜNTETÉSRE KÉSZ" ÜZENET?
IGEN
1732
1734
VAN PÉNZMODUL
TRANZAKCIÓ FOLYAMATBAN?
NEM
1740
NEM
X MODUL BANKI PÉNZTÁR MODUL?
IGEN
1744
1736
NEM
VOLT "MEGSZÜNTETÉSRE KÉSZ" ÜZENET?
IGEN
1742
1738
1746
1

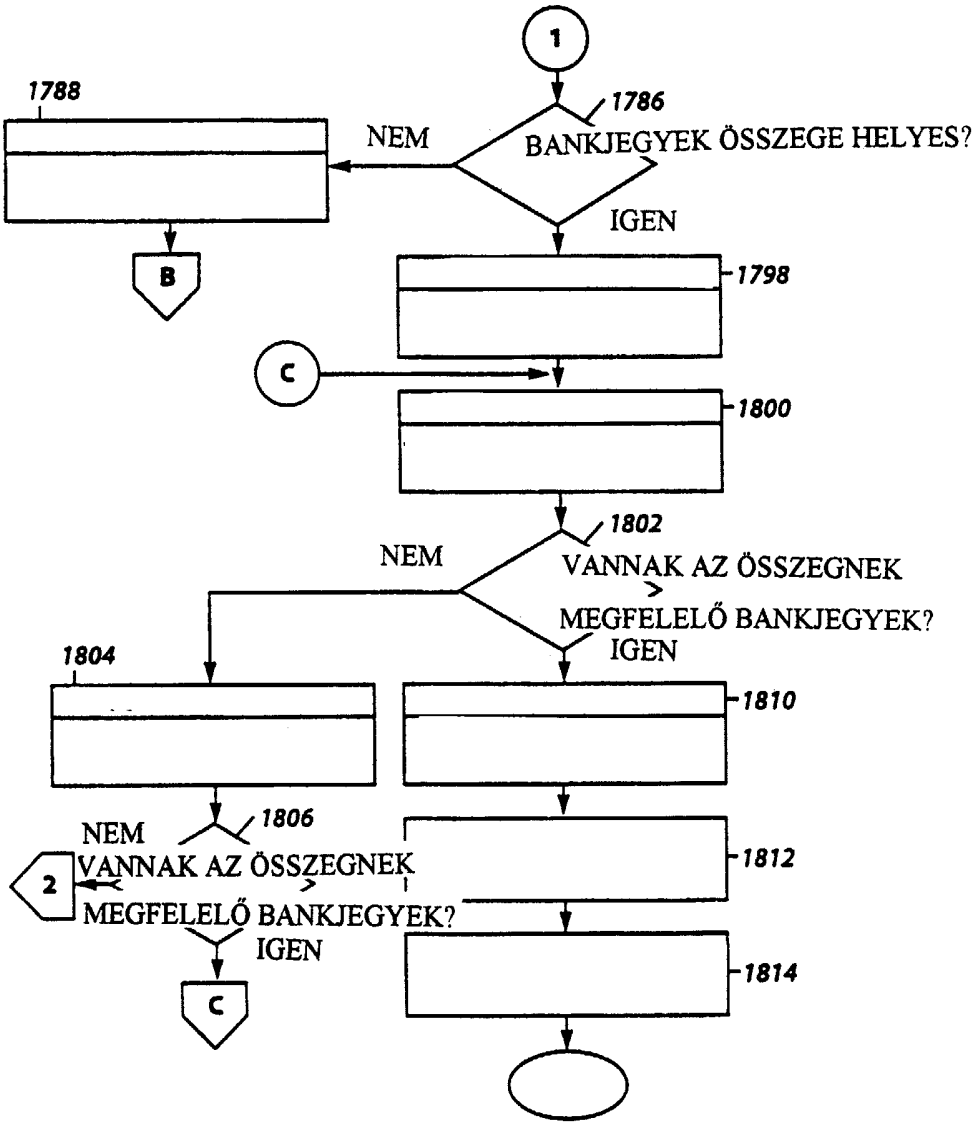
11A. ábra


1
1748
1750
1752
VAN PÉNZMODUL
TRANZAKCIÓ FOLYAMATBAN?
NEM
IGEN
1754
1756
VAN PÉNZMODUL
TRANZAKCIÓ FOLYAMATBAN?
NEM
IGEN
1758

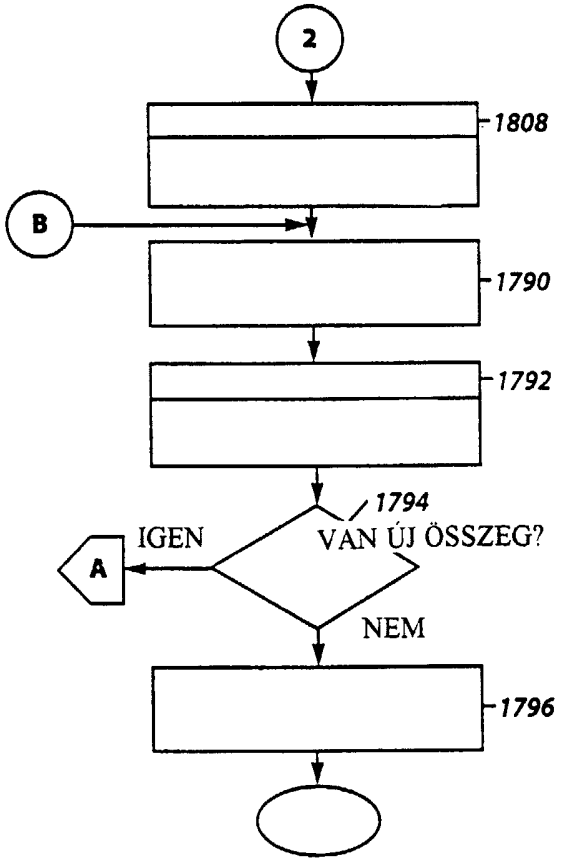
11B. ábra


1760
1762
1764
1766
1775
1768
1770
1772
1774
1776
1778
A
1780
1782
1784
1

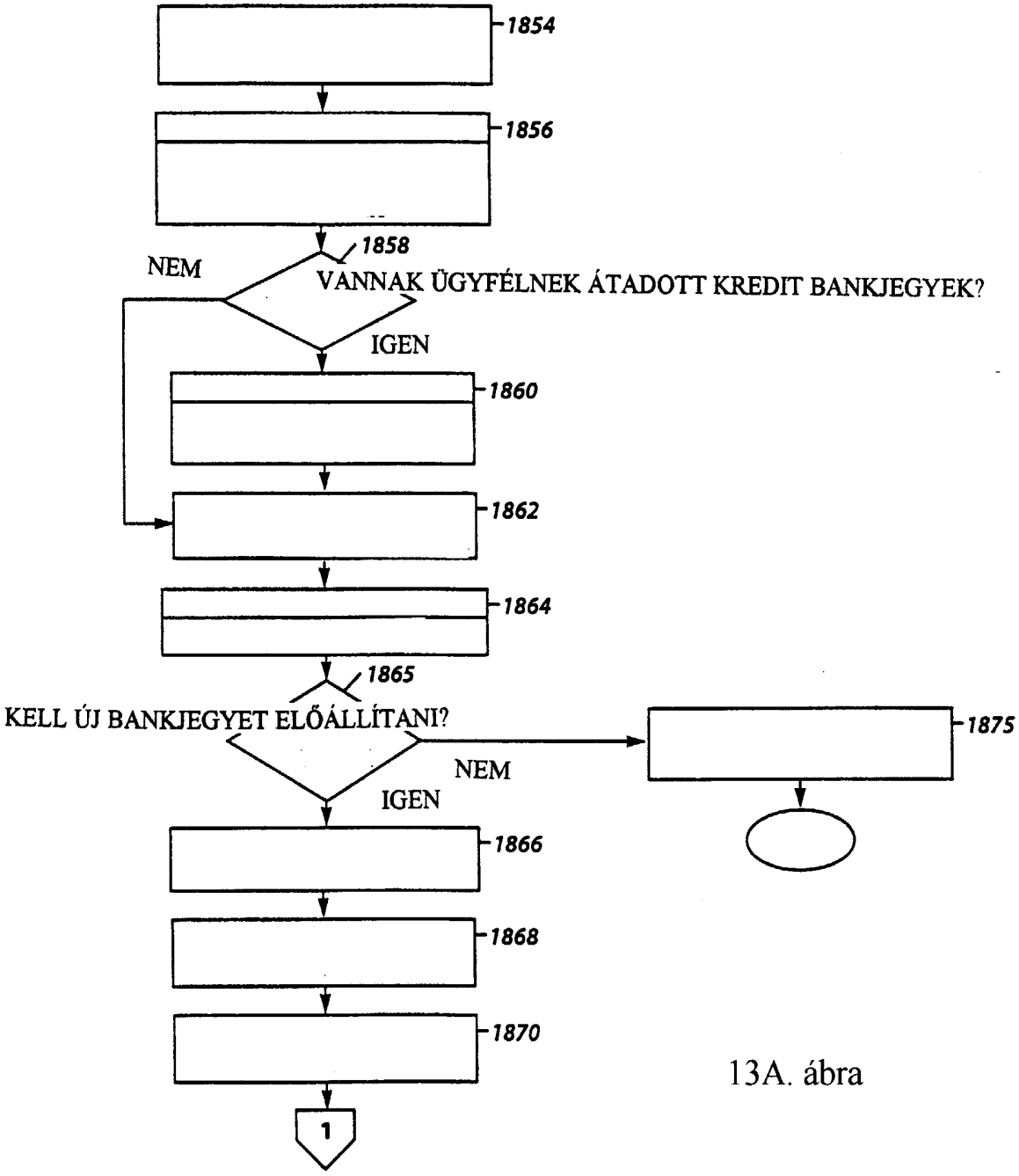
12A. ábra


1
1788
1786
NEM
BANKJEGYEK ÖSSZEGE HELYES?
IGEN
B
1798
C
1800
1802
NEM
VANNAK AZ ÖSSZEGNEK
MEGFELELŐ BANKJEGYEK?
IGEN
1804
1810
NEM
1806
VANNAK AZ ÖSSZEGNEK
2
MEGFELELŐ BANKJEGYEK?
IGEN
1812
1814
C

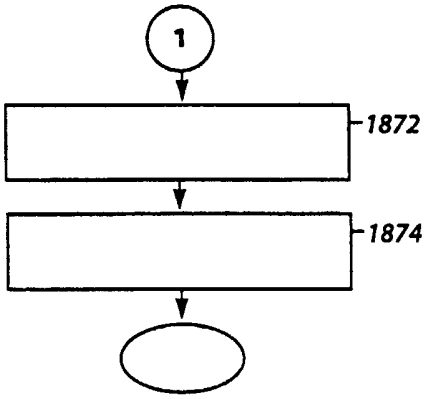
12B. ábra



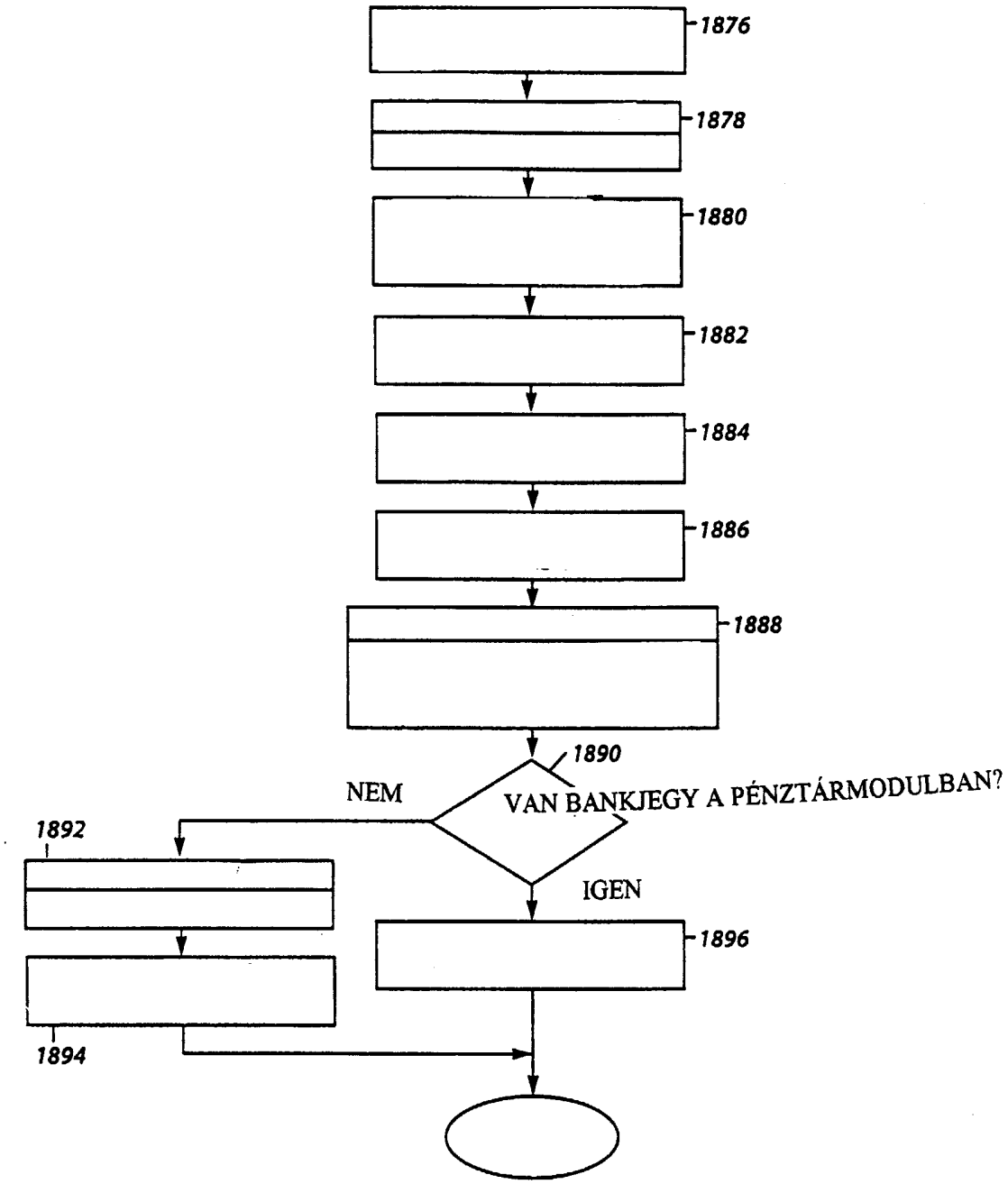
12C. ábra


1854
1856
1858
NEM
VANNAK ÜGYFÉLNEK ÁTADOTT KREDIT BANKJEGYEK?
IGEN
1860
1862
1864
1865
KELL ÚJ BANKJEGYET ELŐÁLLÍTANI?
NEM
IGEN
1875
1866
1868
1870
1

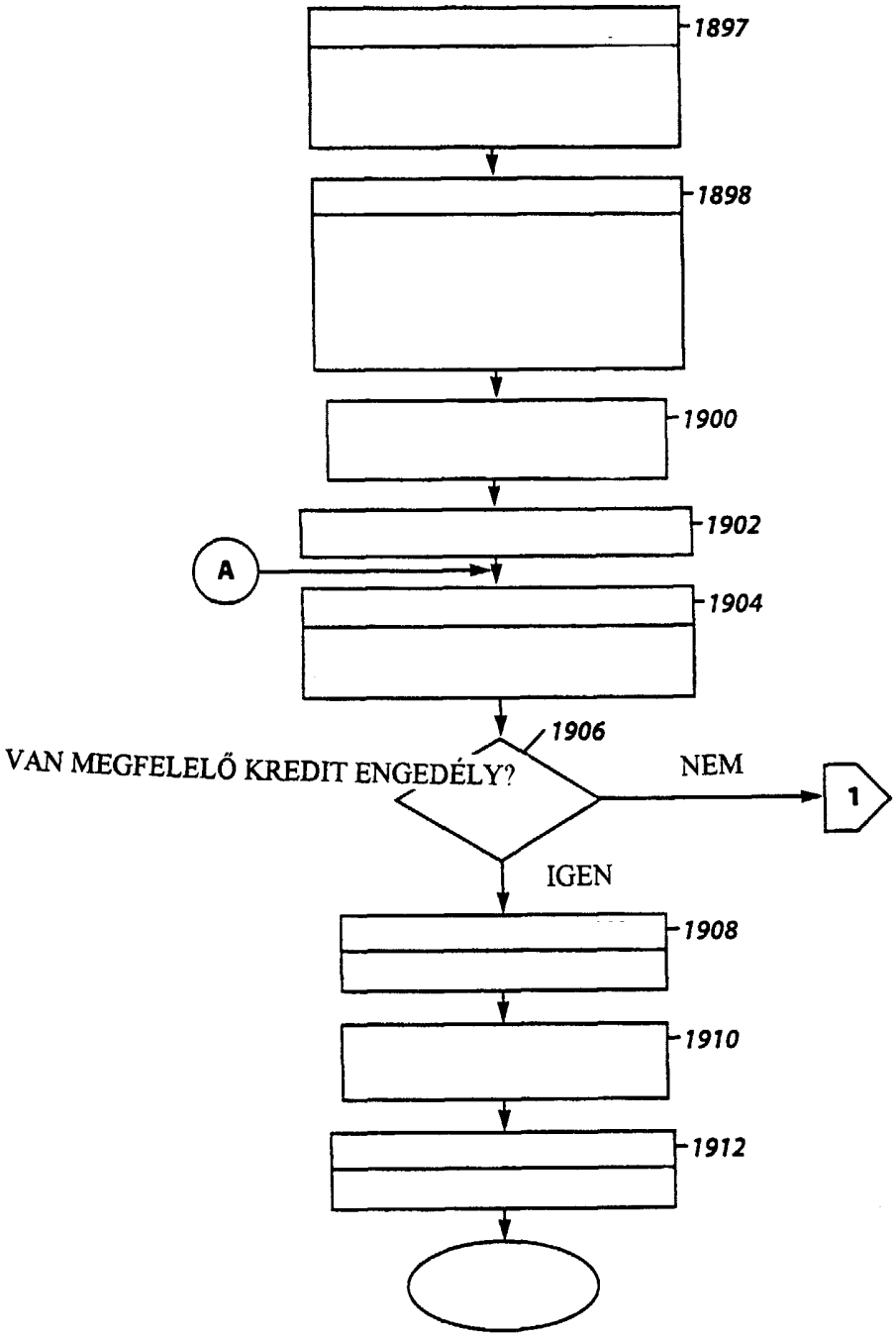
13A. ábra



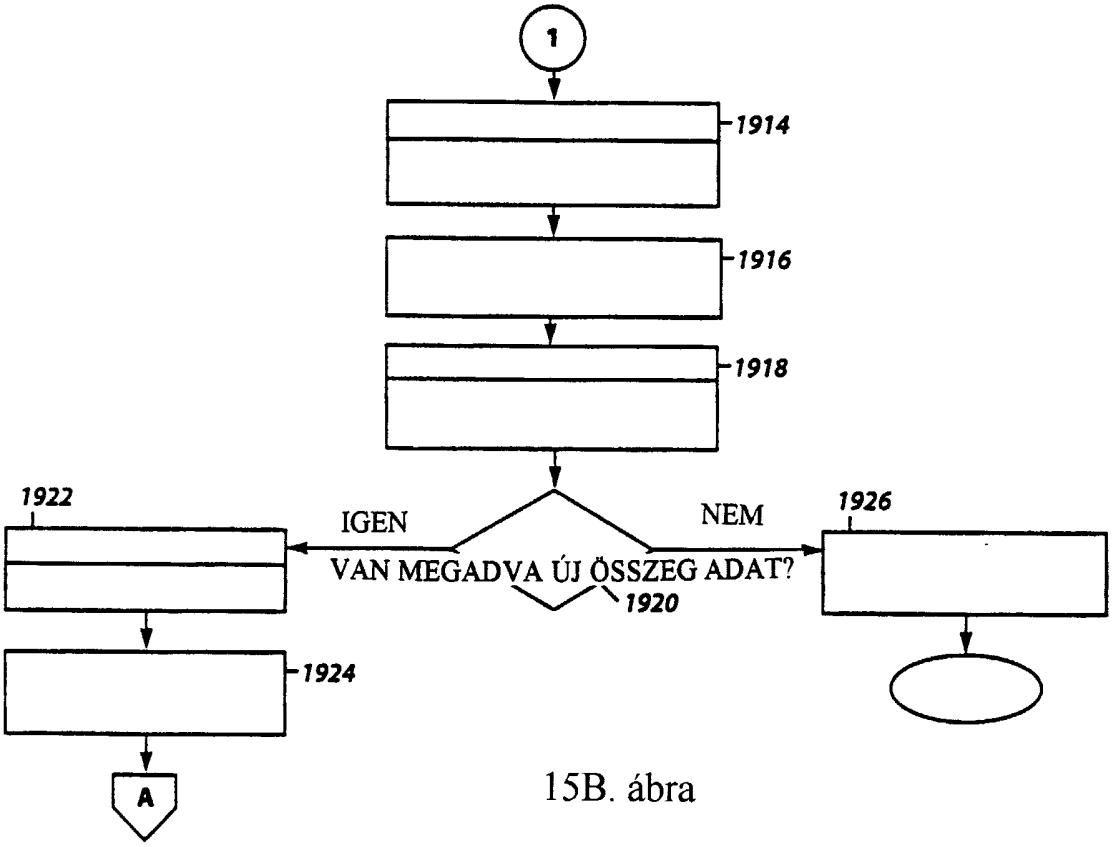
13B. ábra


1876
1878
1880
1882
1884
1886
1888
1890
NEM
VAN BANKJEGY A PÉNZTÁRMODULBAN?
IGEN
1892
1894
1896

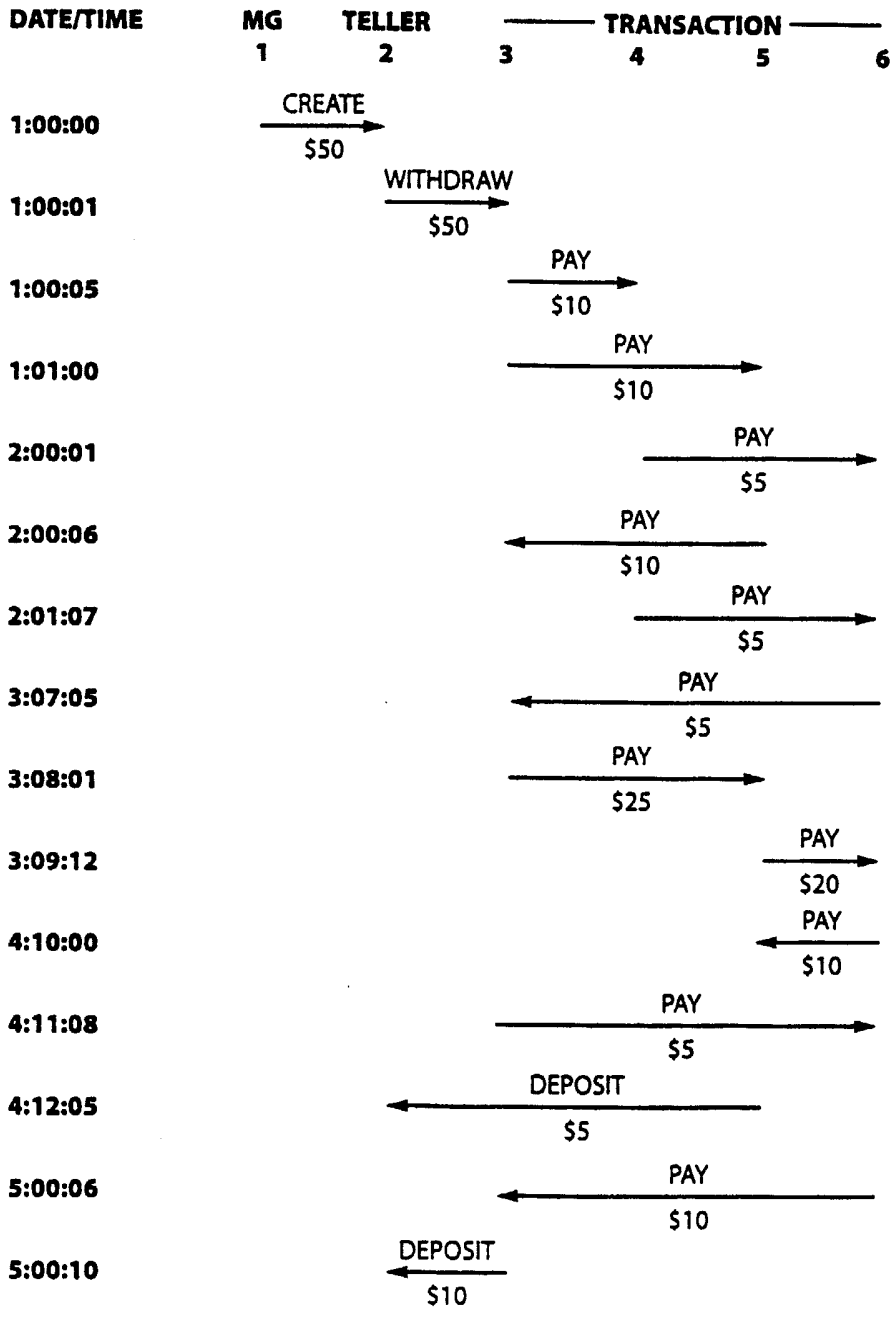
14. ábra


1897
1898
1900
1902
A
1904
1906
VAN MEGFELELŐ KREDIT ENGEDÉLY?
NEM
1
IGEN
1908
1910
1912

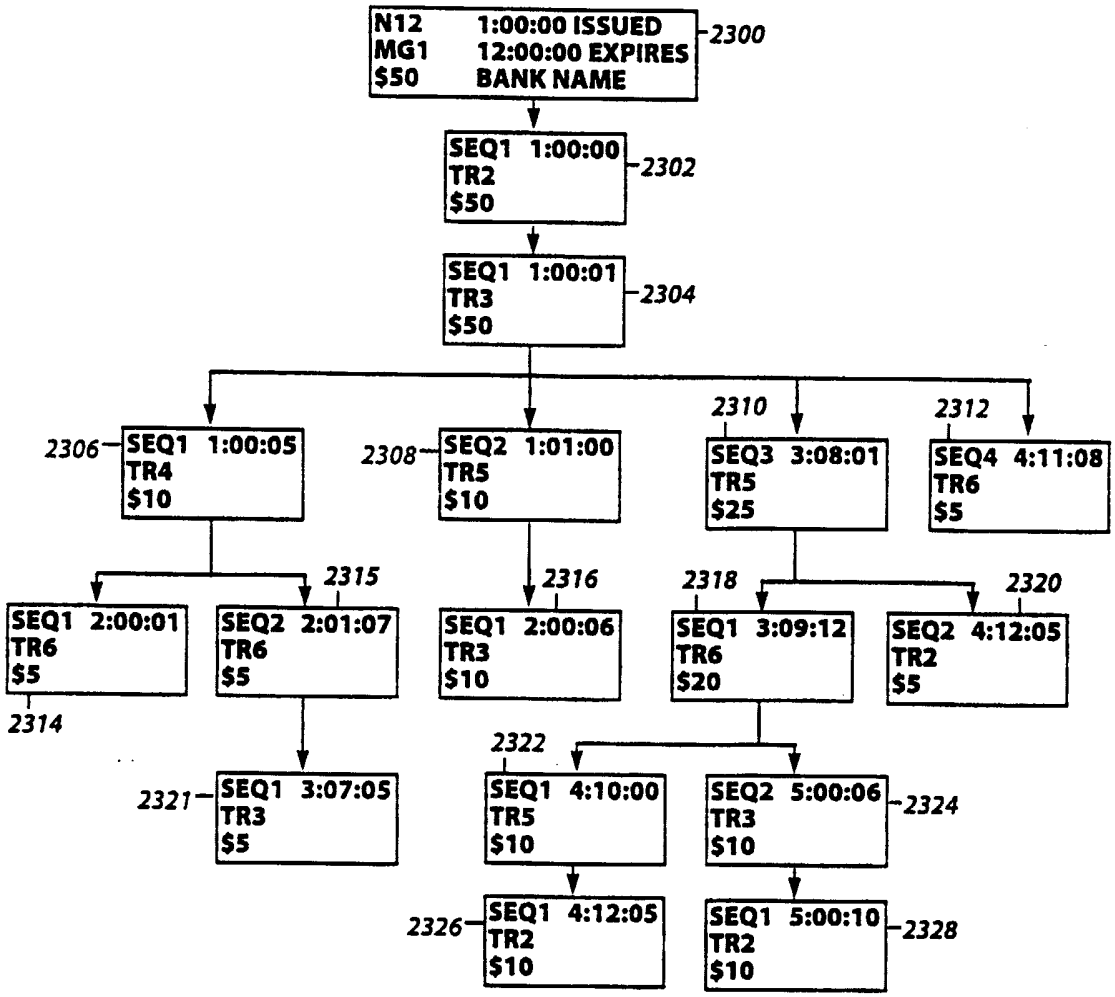
15A. ábra


1
1914
1916
1918
1922
IGEN
NEM
1926
VAN MEGADVA ÚJ ÖSSZEG ADAT?
1920
1924
A

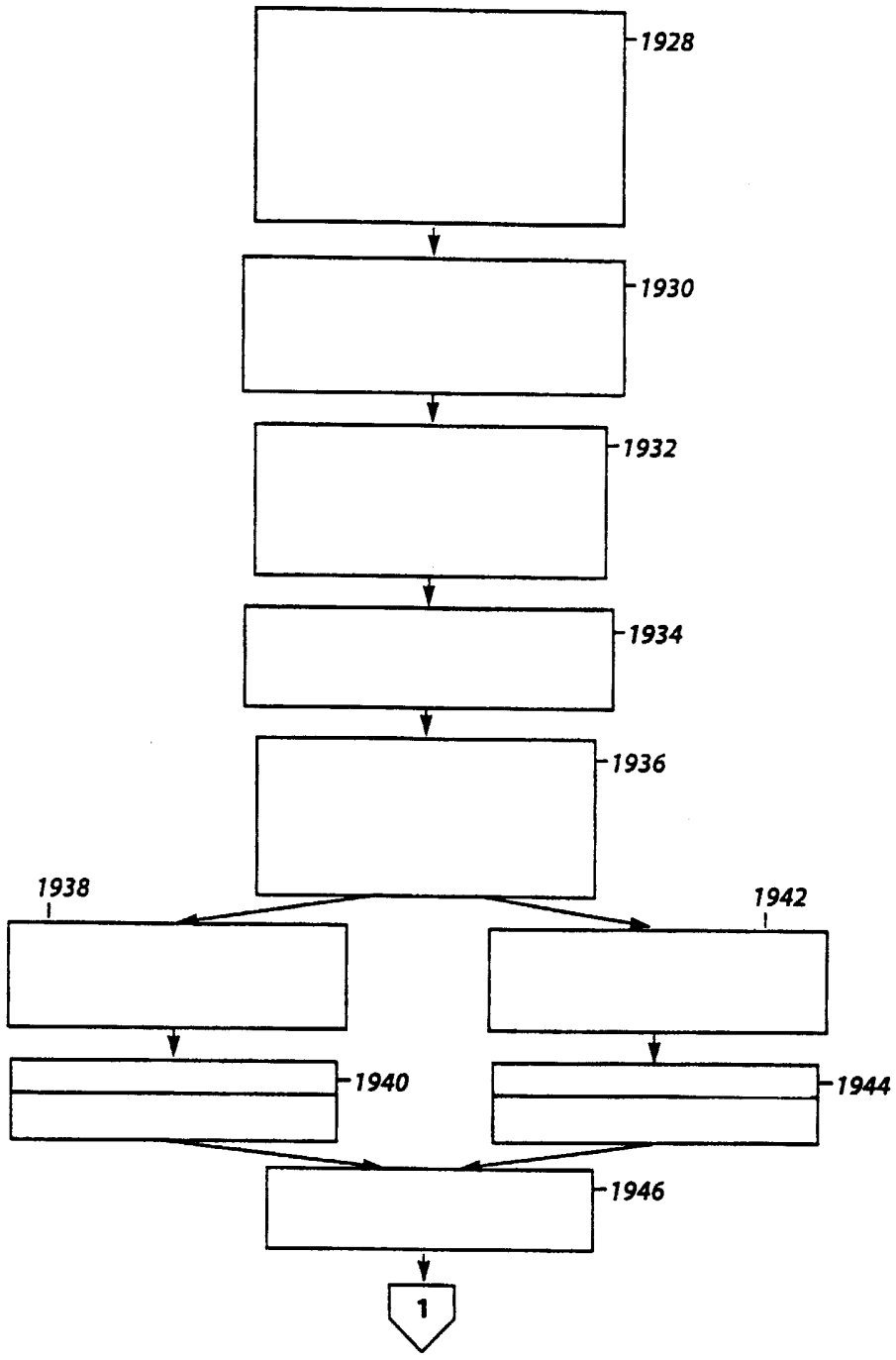
15B. ábra


DATE/TIME
MG
TELLER
TRANSACTION
1
2
3
4
5
6
1:00:00
CREATE
$50
1:00:01
WITHDRAW
$50
1:00:05
PAY
$10
1:01:00
PAY
$10
2:00:01
PAY
$5
2:00:06
PAY
$10
2:01:07
PAY
$5
3:07:05
PAY
$5
3:08:01
PAY
$25
3:09:12
PAY
$20
4:10:00
PAY
$10
4:11:08
PAY
$5
4:12:05
DEPOSIT
$5
5:00:06
PAY
$10
5:00:10
DEPOSIT
$10

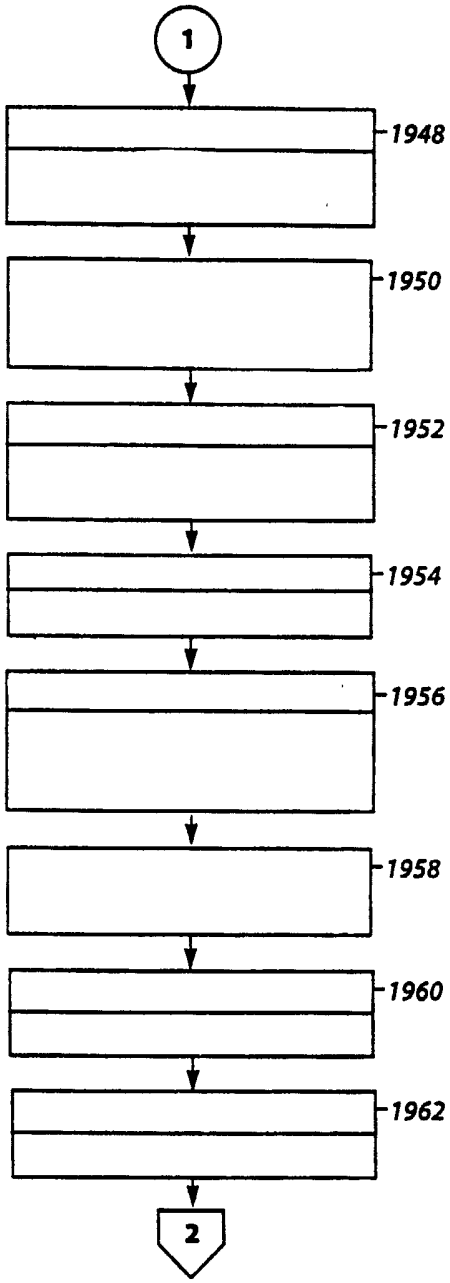
16. ábra


N12 1:00:00 ISSUED
MG1 12:00:00 EXPIRES
$50 BANK NAME
2300
SEQ1 1:00:00
TR2
$50
2302
SEQ1 1:00:01
TR3
$50
2304
2306
SEQ1 1:00:05
TR4
$10
2308
SEQ2 1:01:00
TR5
$10
2310
SEQ3 3:08:01
TR5
$25
2312
SEQ4 4:11:08
TR6
$5
2315
2316
2318
2320
SEQ1 2:00:01
TR6
$5
2314
SEQ2 2:01:07
TR6
$5
SEQ1 2:00:06
TR3
$10
SEQ1 3:09:12
TR6
$20
SEQ2 4:12:05
TR2
$5
2322
2321
SEQ1 3:07:05
TR3
$5
SEQ1 4:10:00
TR5
$10
SEQ2 5:00:06
TR3
$10
2324
2326
SEQ1 4:12:05
TR2
$10
SEQ1 5:00:10
TR2
$10
2328

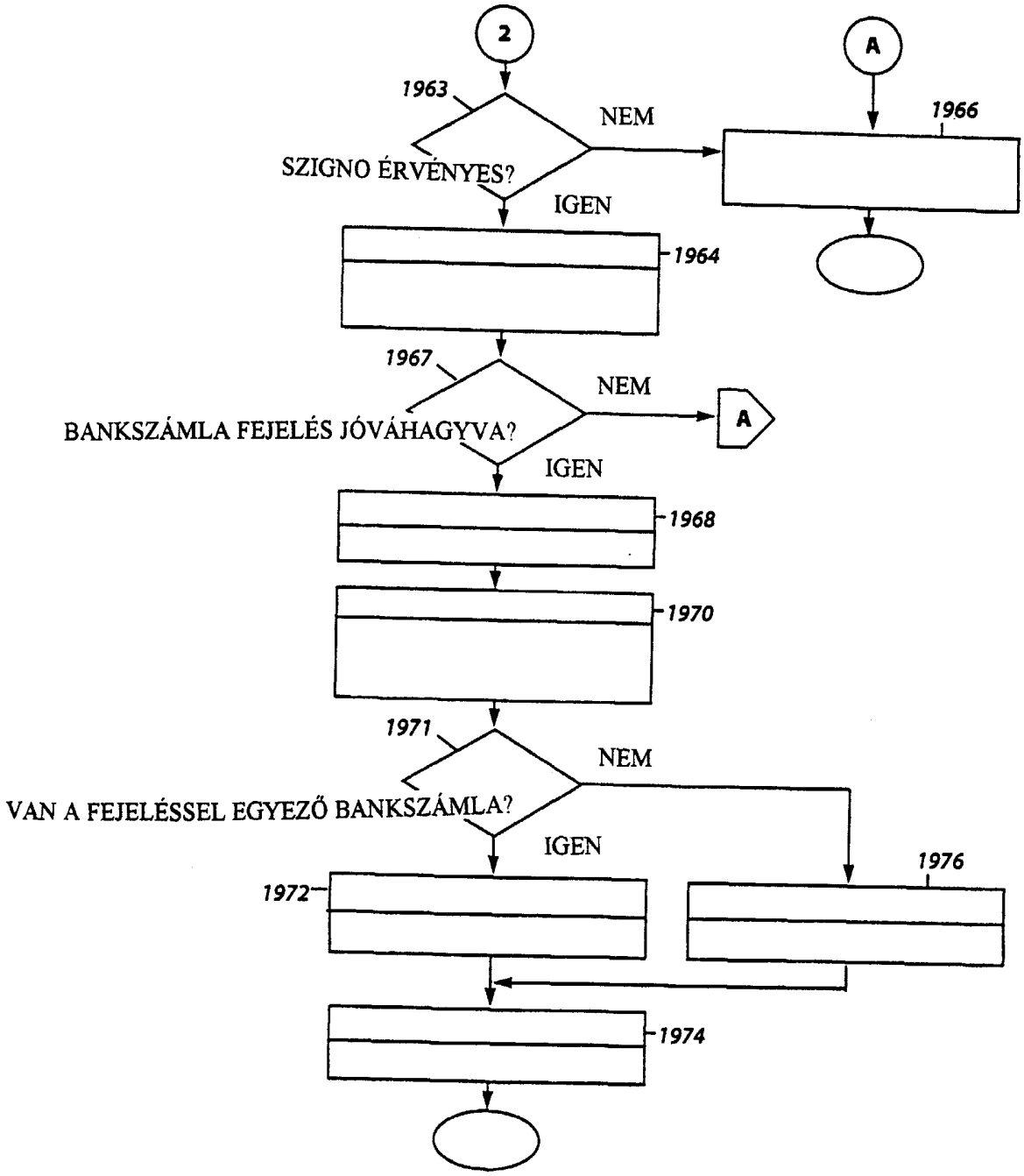
17. ábra



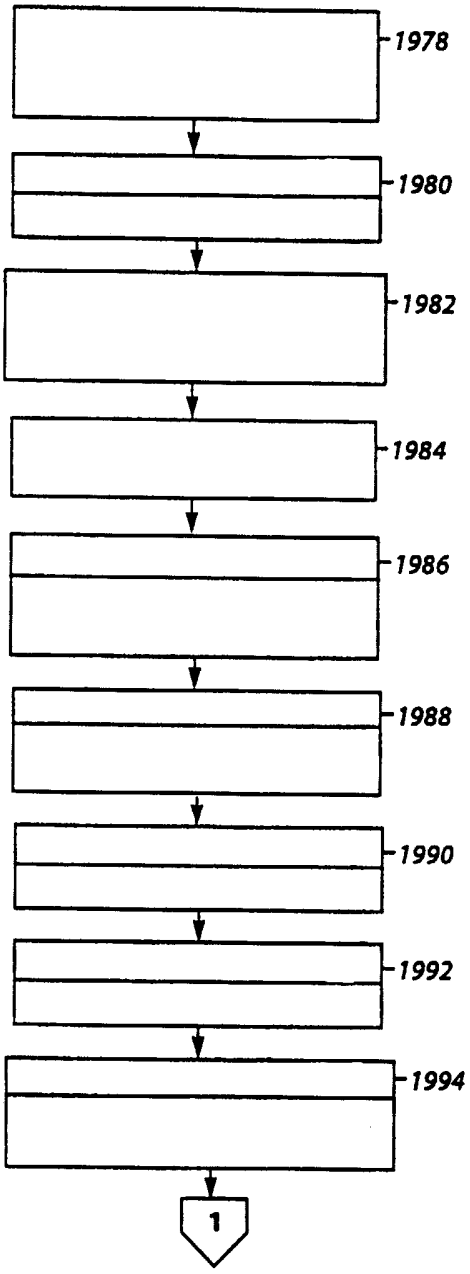
18A. ábra



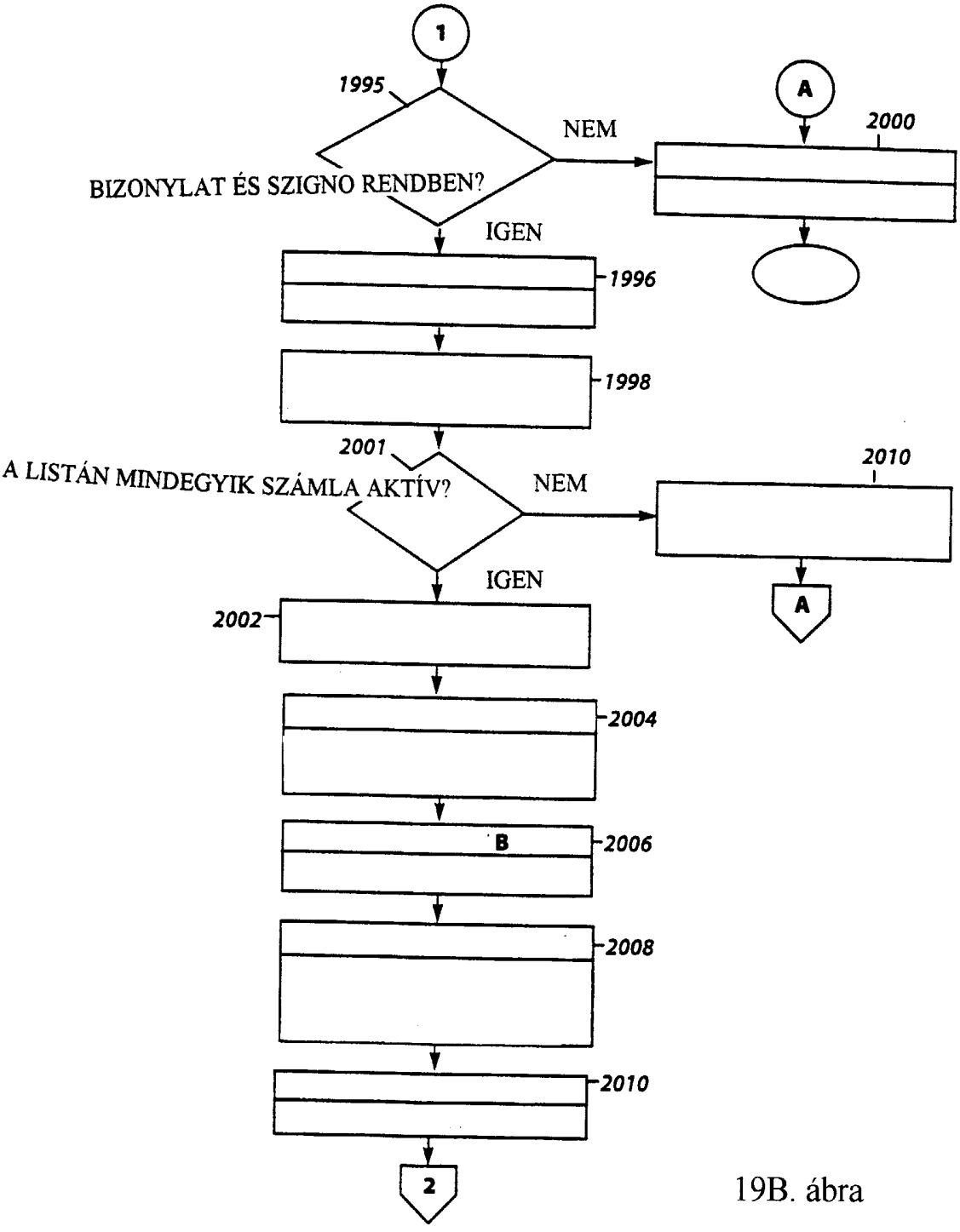
18B. ábra


2
A
1963
NEM
1966
SZIGNO ÉRVÉNYES?
IGEN
1964
1967
NEM
BANKSZÁMLA FEJELÉS JÓVÁHAGYVA?
A
IGEN
1968
1970
1971
NEM
VAN A FEJELÉSSEL EGYEZŐ BANKSZÁMLA?
IGEN
1976
1972
1974

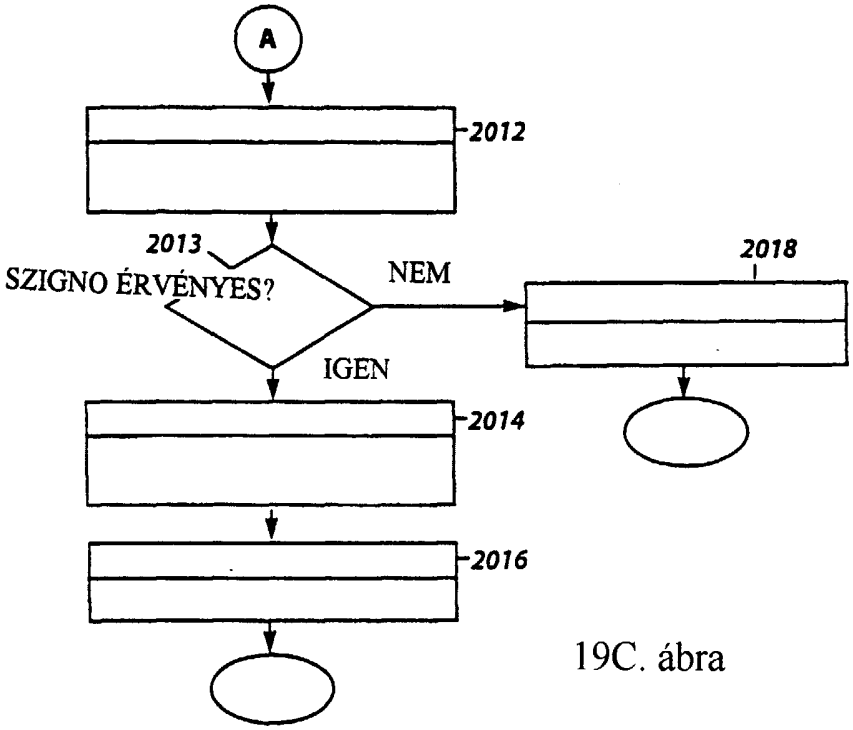
18C. ábra



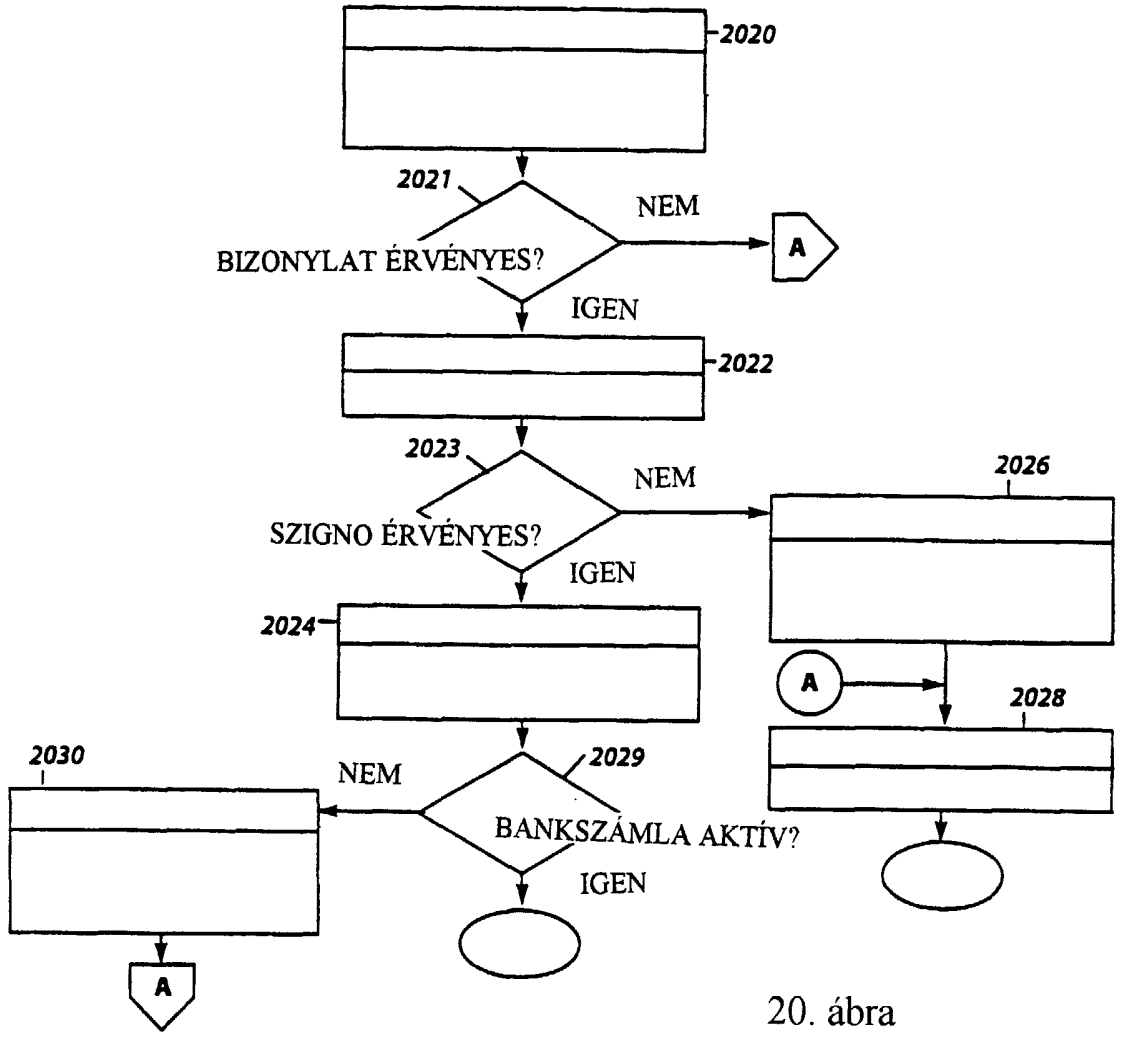
19A. ábra


1
1995
BIZONYLAT ÉS SZIGNO RENDBEN?
NEM
A
2000
IGEN
1996
1998
2001
A LISTÁN MINDEGYIK SZÁMLA AKTÍV?
NEM
2010
A
IGEN
2002
2004
B
2006
2008
2010
2

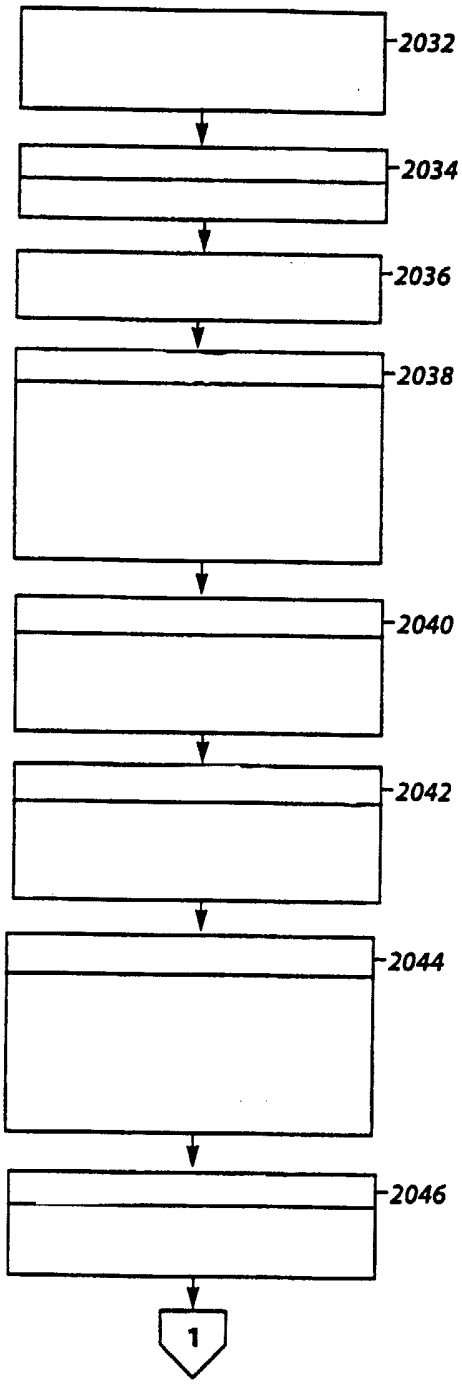
19B. ábra



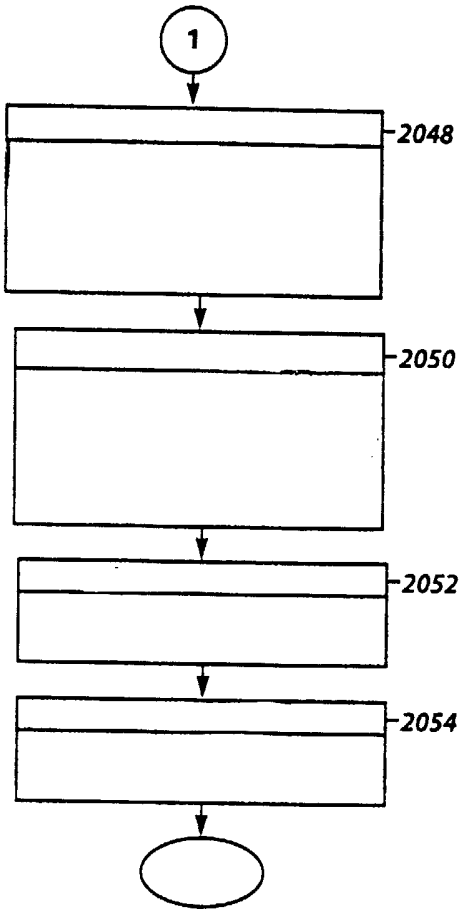
19C. ábra


2020
2021
BIZONYLAT ÉRVÉNYES?
NEM
A
IGEN
2022
2023
SZIGNO ÉRVÉNYES?
NEM
2026
IGEN
2024
A
2028
2030
NEM
2029
BANKSZÁMLA AKTÍV?
IGEN
A

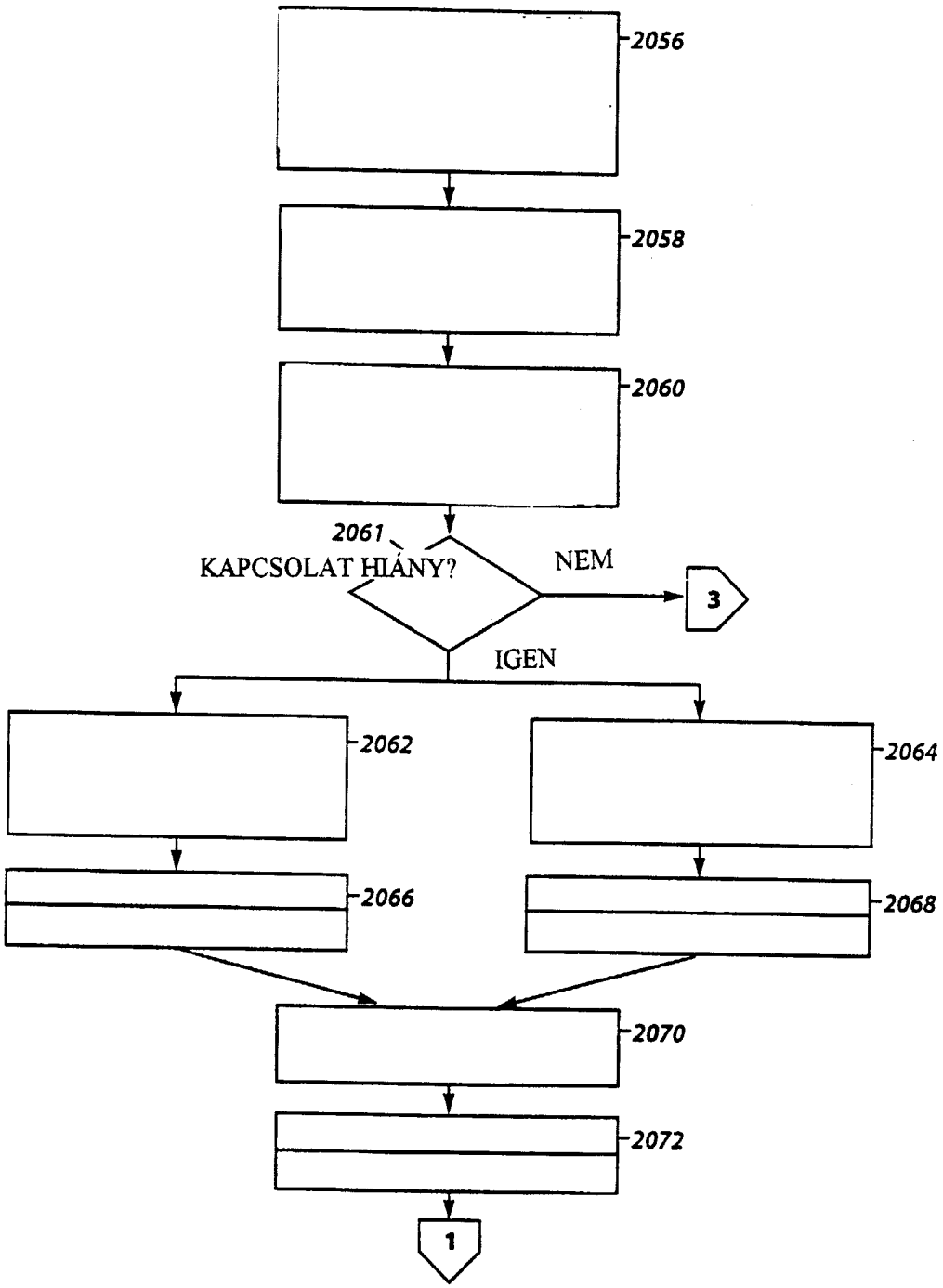
20. ábra



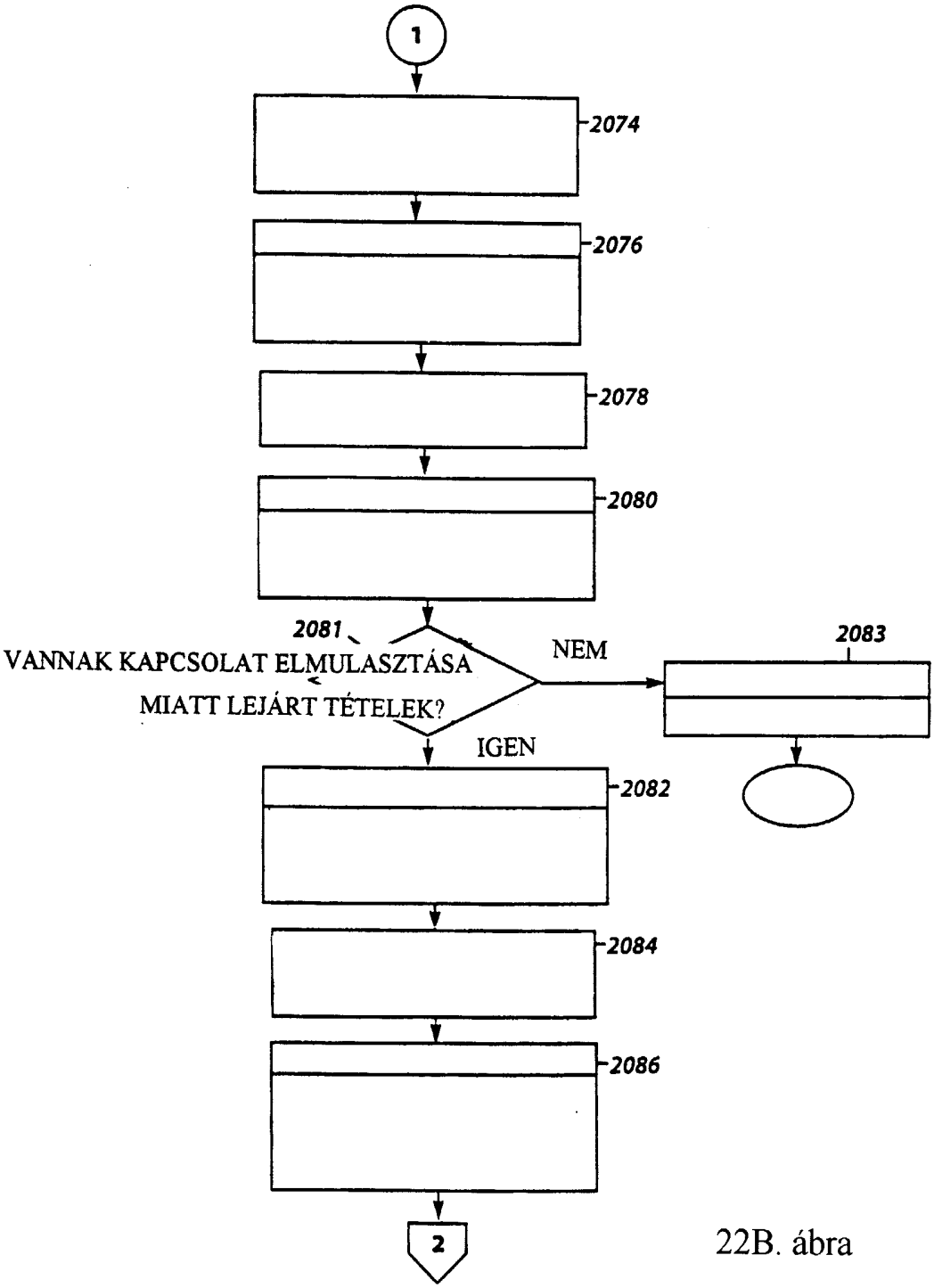
21A. ábra



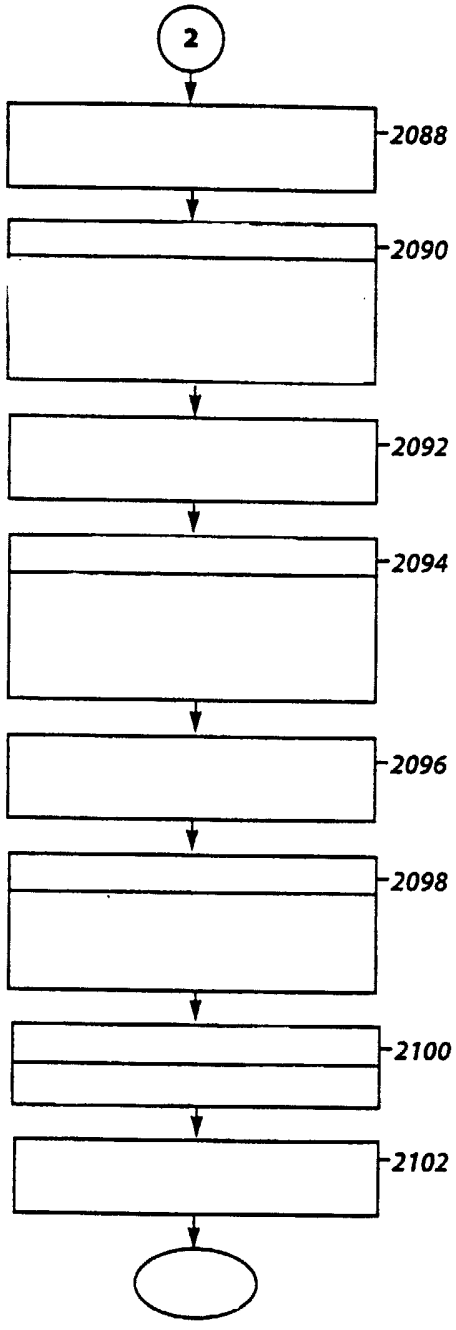
21B. ábra


2056
2058
2060
2061
KAPCSOLAT HIÁNY?
NEM
3
IGEN
2062
2064
2066
2068
2070
2072
1

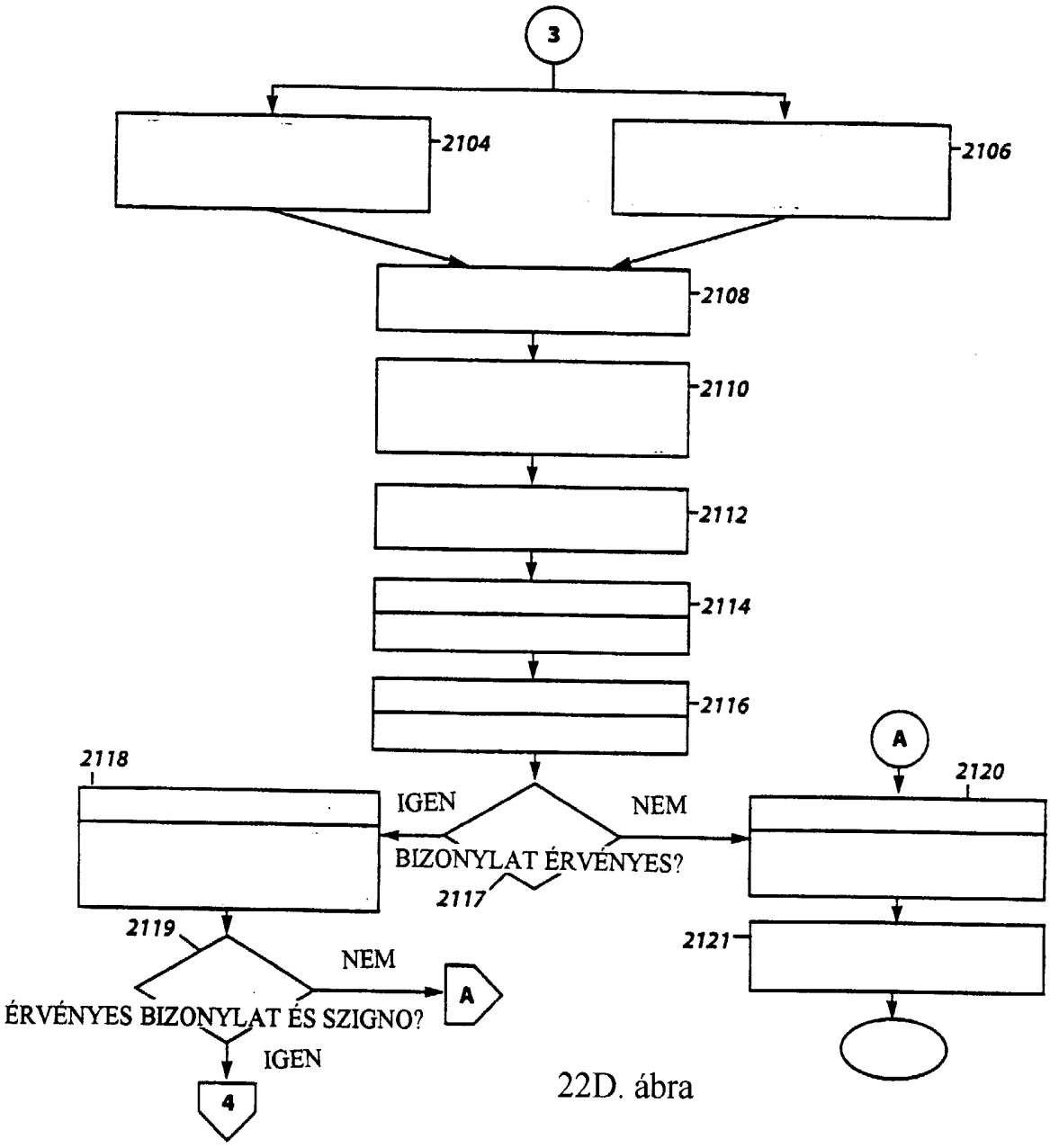
22A. ábra


1
2074
2076
2078
2080
2081
VANNAK KAPCSOLAT ELMULASZTÁSA MIATT LEJÁRT TÉTELEK?
NEM
2083
IGEN
2082
2084
2086
2

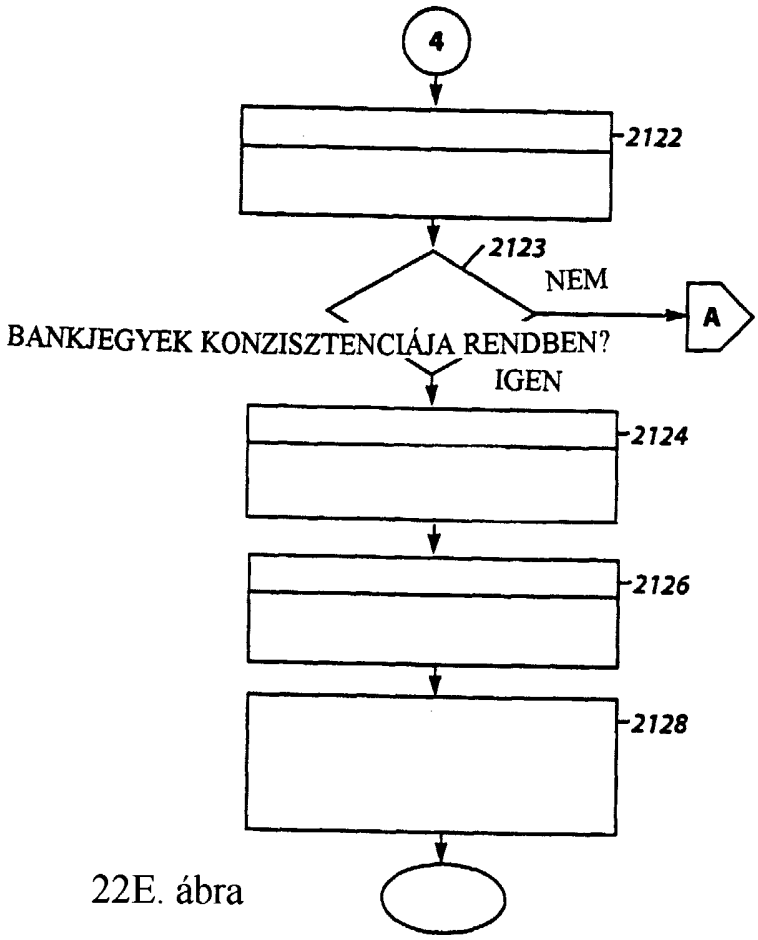
22B. ábra



22C. ábra


3
2104
2106
2108
2110
2112
2114
2116
2118
IGEN
NEM
BIZONYLAT ÉRVÉNYES?
2117
A
2120
2119
NEM
A
ÉRVÉNYES BIZONYLAT ÉS SZIGNO?
IGEN
2121
4

22D. ábra



22E. ábra

Kiadja a Magyar Szabadalmi Hivatal, Budapest
A kiadásért felel: Törőcsik Zsuzsanna főosztályvezető-helyettes
Windor Bt., Budapest