Invenţia se referă la un sistem de transmitere a valorii. Sistemele de transfer electronic al valorii au fost propuse pentru transferarea valorii între "pungile" electronice. Aceste pungi pot avea multe forme, dar o formă convenabilă este o cartelă cu circuit integrat (IC) care include un microprocesor şi memorie pentru valoarea acumulată cel puţin. Asemenea cartele pot folosite în aşa-numitele plăţi prin virament unde valoarea (mărimea) e transferată în "punga" comerciantului cu amănuntul în schimbul mărfurilor şi serviciilor.

Deci o aplicaţie majoră a unor asemenea sisteme este transferul valorii în locul lichidităţilor. Lichidităţile au atât avantaje cât şi neajunsuri. Un avantaj al lichidităţilor este faptul că micile tranzacţii de valoare pot fi efectuate fără acordurile specifice dintre conturile plătitorului şi a destinatarului plăţii. Pe lângă faptul că sistemul nu e suprasolicitat, aceasta le conferă tranzacţiilor anonimitate, ceea ce constituie un avantaj social.

Multe din sistemele electronice de transfer a valorii prin virament propuse mai înainte au ratat şansa de a recunoaşte aceste avantaje şi de a le implementa. Sistemul pe care se bazează prezenta invenţie este descris şi publicat în brevetul [1] şi asigură transferul de valoare între pungile electronice în aşa fel încât permită menţinerea tuturor plusurilor enumerate mai sus ale tranzacţiilor cu lichidităţi. Sistemul poate fi implementat în altul care că conţine un computator, o mulţime de pungi electronice, aparate de schimb, iar pungile pot comunica una cu alta pentru a transfera valoarea în tranzacţiile ce se fac fără intermediul computatorului; mijloace de iniţializare pentru pungile valoarea cărora se află sub controlul computatorului; mijloace de corecţie pentru corectarea valorii care se află sub controlul computatorului; contor de valoare, una sau mai multe din pungile de mai sus fiind pungi de volum care au posibilitatea de a încărca valoare şi a o corecta prin intermediul controlului de valoare are una sau mai multe înregistrări a valorii unde poate fi înscrică valoare netă ce corespunde pungii de volum sau pungilor, valoarea netă fiind diferenţa dintre valorile comune transferate în punga de volum sau ale pungilor cu valoare comună primită din punga sau pungile de volum, înregistrarea valorii flotante nu e caracteristică unor iniţializări şi corectării individuale.

Controlul de valoare poate avea o interfaţă prin intermediul căreia înregistrarea valorii flotante poate fi ajustată la comandă în aşa fel ca valoarea să poată fi creată sau distrusă într-o pungă sau pungi de volum.

E preferabil ca în orice pungă să fie prevăzut un mijloc de depozitare care să păstrează înregistrarea valorii cumulative a pungii şi în fiecare pungă sau în dispozitivul de schimb respectiv un microprocesor, tranzacţiile având loc între perechile de pungi una dintre care e punga transmiţătoare a valorii, iar alta e punga receptoare a valorii, microprocesoarele sunt programate în aşa fel încât la fiecare tranzacţie înregistrarea valorii pungii transmiţătoare se micşorează cu suma tranzacţiei, iar înregistrarea valorii pungii se măreşte cu aceeaşi sumă a tranzacţiei.

Prin introducerea unei înregistrări flotante a valorii, înregistrare nespecifică de altfel, e păstrat anonimatul tranzacţiei şi nu mai este necesară concordarea conturilor utilizatorilor la tranzacţiile de la pungă la pungă. În unele situaţii e necesar să fie că plata din fonduri sau alte valori este efectuată doar după un anumit eveniment. De exemplu, s-ar putea întâmpla ca valoarea să fie transmisă numai pe baza faptului că ea e folosită pentru scopuri specifice. Ca exemplu ar putea servi controlul schimbului valutar. Sau, să zicem, că guvernul ar dori să aprovizionează cu fonduri un importator cu condiţia ca aceste fonduri să fie folosite pentru anumite mărfuri.

Sistemul transferului de valoare, prezentat în soluţia analoagă cea mai apropiată [1], nu asigură posibilitatea întreruperii tranzacţiilor, îndeplinirea tranzacţiilor cu reţinerea achitării şi îndeplinirea serei de tranzacţii.

S-ar putea, de asemenea, întâmpla ca sistemul transferului de valoare să fie folosit la prelucrarea pachetelor de viramente.

Problema pe care o rezolvă este lărgirea posibilităţilor funcţionale ale sistemului de transfer al valorii.

Problema invenţiei se rezolvă prin aceea ca sistemul de transfer al valorii este asigurat u un computator, pungi electronice, dispozitive de schimb prin intermediul cărora pungile pot fi conectate una cu alta la efectuarea tranzacţiilor în afara computatorului şi un microprocesor în fiecare pungă sau în aparatele de schimb asociate, plata pentru tranzacţii se efectuează între perechi de pungi, una din care se transmite, iar alta recepţionează valoarea, microprocesoarele sunt programate în aşa fel încât tranzacţiile includ cel puţin următoarele etape:
A. Punga receptoare transmite mesajul: "Cerere de primire a valorii".

B. Punga transmiţătoare creează un mesaj ce conţine valoarea.

C. Punga transmiţătoare creează şi înmagazinează un mesaj de transmitere care confirmă transmiterea valorii cerute de către ce primeşte.

D. Punga transmiţătoare trimite între stadiile C şi B; şi

E. Punga transmiţătoare trimite mesajul ce conţine valoarea.

E preferabil ca fiecare pungă să aibă un volum de memorie pentru protocolarea tranzacţiilor, la formarea mesajului de transmitere protocolul se păstrează în volumul de memorie al pungii transmiţătoare, după transmitere - în cel al pungii receptoare.

Înaintea formării mesajului de transmitere, punga transmiţătoare va crea mesajul ce conţine valoarea şi va scădea mărimea cerută din acumulatorul său, această secvenţa de acţiuni înseamnă că dacă tranzacţia este întreruptă după formarea mesajului de transmitere, există garanţia că fondurile cerute sunt disponibile pentru punga receptoare şi doar pentru ea. Aceste fonduri nu mai sunt disponibile pungii transmiţătoare. Pentru a completa tranzacţia, suma dată trebuie transferată pungii receptoare. Dacă e necesar aceasta poate fi făcut printr-o serie de tranzacţii prin intermediul unuia sau a mai mulţi intermediari care pot fi consideraţi deţinători de fonduri i subiectului în cazul unor situaţii deosebite.

E preferabil ca pungile să aibă mijloacele prin intermediul cărora tranzacţia dintre o pereche de pungi să fie dată de un identificator unic şi microprocesoarele să fie programate ca să răspundă identificatoarelor pentru a preveni

repetarea tranzacţiilor. În cazul acesta nu se cere nici o referinţă la computator pentru a determina dacă unii şi aceeaşi "bani electronici" nu s-au folosit de două ori. În cazul apăriţiei cererii de primire a sumei, se adresează la computator şi cu ajutorul identificatorului poate fi clarificat dacă această cerere nu a fost înaintată de două ori, se referă la tranzacţia dată sau se referă la altă tranzacţie. E preferabil ca identificatorul tranzacţiei să fie transmis de la punga transmiţătoare la punga receptoare, fiind descris reieşind din datele ce determină punga receptoare şi numărul de ordine al tranzacţiei pungii receptoare sau marcajul electronic, dat/timpul obţinut de la punga receptoare la operaţiunea preliminară de "strângere a mâinii". În felul acesta punga receptoare va indica definitivarea tranzacţiei şi orice încercare de a primi una şi aceeaşi valoare de două ori va fi respinsă.

Securitatea sistemului cere folosirea tehnicii criptografice pentru a preveni fraudele. Cea mai efectivă tehnică criptografică este cea asimetrică, care cere diferite chei pentru cifrarea şi descifrarea informaţiei. Una din tehnicile criptografice convenabile şi bine cunoscute este cea atribuită lui Rivest, Shamir şi Adleman, cunoscută drept sistemul RSA. E prevăzut ca ambele pungi a unei perechi comunicând să poată folosi sistemul RSA egal, într-un mod echilibrat pentru prelucrarea algoritmică. Deşi la cifrare conform sistemului RSA se cer computatoare mai perfoante pentru a efectua descifrarea RSA într-un timp scurt. Pentru a depăşi această complicaţie, în interesul economiei şi vitezei, în corespundere cu invenţia, se propune folosire unui sistem dezechilibrat în care puterea de operare necesară pungilor cumpărătorilor e puţin mai mică decât necesară pungilor vânzătorilor.

Fiecare utilizator al unui sistem criptografic asimetric are o pereche de chei - una publică şi alta secretă. Mesajul către un altul e cifrat folosindu-se de cheia publică a aculuia care devine accesibilă, posibil, cu ajutorul procedurii de schimb a cheii. Mesajele primite sunt descifrate cu ajutorul cheii secrete locale. Folosirea cheii publice necesită cu mult mai puţină putere de operare a computatorului decât folosirea cheii secrete, din această cauză cifrare necesită mai puţine calcule decât descifrarea. În consecinţă, folosind un sistem dezechilibrat de tip deschis e raţional de a anula cerinţa ca punga cumpărătorului să efectueze obişnuinţa descifrare RSA.

O primă cale de a reduce încărcătura criptografică în punga cumpărătorului e de a o asigura cu un criptografic mai simplu, simetric. Un asemenea sistem foloseşte una şi aceeaşi cheie atât la cifrare cât şi la descifrare. Drept exemplu serveşte sistemul criptografic DES (standardul de cifrare a datelor - US FIPS 46, 1976). Punga vânzătorului reţine toate posibilităţile sistemului RSA.

O a doua metodă e de a folosi un sistem propriu: cheie publică/cheie secretă pentru schimbul de informaţii. La schimbul de chei punga cumpărătorului îi trimite pungii vânzătorului cheia sa secretă. La transmiterea informaţiei către punga vânzătorului, punga cumpărătorului va efectua cifrarea folosindu-şi cheia secretă.

Securitatea poate fi majorată folosind informaţie certificată electronic, de exemplu date semnate în cod numeric, în procesul tranzacţie. Fiecărei pungi în timpul introducerii îi va fi alocat un număr caracteristic şi va numărul acesta semnat de cheia secretă a unui sistem criptografic asimetric global. Ca rezultat vom avea marcajul global al numărului şi acesta va fi stocat în punga. Toate pungile vor poseda cheia publică a perechii globale, aşa că la primirea unui număr global marcat al altei pungi va exista posibilitatea verificării autenticităţii. Numerele pot fi prevăzute ca fiind global certificate. Deoarece încheierea tranzacţiilor va cere schimbul cheilor de cifrare e convenabil, deşi nu e necesar, de a se înţelege în prealabil că va avea loc schimbul de numere globale certificate şi de chei de cifrare.

Rezultatul tehnic al invenţiei prezente este asigurarea posibilităţii întreruperii tranzacţiilor precum şi asigurarea caracterului confidenţial al tranzacţiilor.

Rezultatul tehnic prezent este realizat cu ajutorul folosirii microprocesorului programat în aşa mod ca tranzacţia constă din următoarele faze:

A. Punga receptoare trimite un mesaj "cerere de primire a mărimii valorii".

B. Punga transmiţătoare creează un mesaj valoric.

C. Punga transmiţătoare creează şi păstrează un mesaj de transfer care marchează transferul mărimii valorii cerute către punga receptoare.

D. Punga transmiţătoare trimite mesajul de transfer.

E. Punga transmiţătoare trimite mesajul valorii

precum şi cu ajutorul protocolării mesajelor, care se transmit (tranzacţiilor) .

Asigurarea caracterului confidenţial al tranzacţiilor se realizează cu ajutorul folosirii sistemului criptografic simetric şi sistemului criptograficasimetric, care este mai econom.

În continuare invenţia va fi descrisă cu referiri la desenele din figurile respective:

Fig. 1, schema sistemului bancar de computatoare, conform invenţiei;

fig. 2, diagrama ce ilustrează controlul de valoare;

fig. 3, diagrama ce ilustrează exemplul producerii tranzacţiei de valoare, folosind sistemul criptografic RSA complet;

fig. 4, diagrama ce ilustrează exemplul producerii tranzacţiei de valoare, folosind tehnica transmiterii cheii secrete;

fig. 5, diagrama ce ilustrează exemplul producerii tranzacţiei de valoare, folosind un sistem criptografic mixt RSA/DES.

În fig. 1 sunt arătate trei bănci de clearing 1, 2 şi 3 cu computatoarele respective 1.1, 2.1 şi 3.1. Computatoarele au fişiere ce conţin detalii de calcul cu clienţii băncii - cumpărători şi vânzători. Fiecare computator are u contor de

valoare 1.2, 2.2 şi 3.2 care indică mărimea flotantă a valorii contului. Fondurile actuale reprezentate cu ajutorul înregistrărilor respective ale valorii flotante pot fi depuse în una sau în mai multe bănci 1, 2 şi 3 sau în altă parte.

Fiecare bancă are o pungă de volum 1.3, 2.3 şi 3.3 care este conectată la contorul de valoare respectiv şi care are un volum de memorie cu înregistrarea valorii pungii. Terminalele 4 sunt conectate selectiv prin telefon la computatoarele 1.1, 2.1 şi 3.1. De regulă, terminalele 4 sunt terminalele computatoarelor de la domiciliu sau ale celor din locurile publice. Consumatorii au pungi electronice în formă de cartele 5 cu circuite integrate (IC). Aceste cartele au microprocesoare şi memorie. În memoria fiecărei cartele înmagazinate înregistrarea valorii pungii 6 . Cartelele au contactele 7 prin intermediul cărora ele pot interacţiona cu terminalele 4 via cititoarele de cartele 8. Făcând o cerere corespunzătoare de la tastatura terminalului, un consumator poate fi conectat la computatorul băncii sale 1,2 sau 3 şi poate cere ca mărimea valorii sumei să fie înscrisă în punga sa. Dacă banca autorizează cererea, punga de volum e instruită să instituie decontarea valorii pentru încărcarea înregistrării valorii pungi 6 cu valoarea cerută. Cartela e gata acum pentru folosinţă.

În continuare pungile electronice sunt încărcate în terminalele 9, 10 echipate cu dispozitive de citire a cartelelor cu IC, situate în diferite puncte de negoţ. Pentru a folosi cartela sa cumpărătorul o transmite vânzătorului, care o introduce în dispozitivul de citire. E introdusă valoarea tranzacţiei şi, conform conţinutului pungii, e micşorată mărimea valorii înscrise cu mărimea sumei tranzacţiei. Înregistrarea valorii pungii ce se află în terminalul 9 sau 10 e mărită cu aceeaşi mărime a tranzacţiei. Cumpărătorul îşi ia marfa şi e liber să folosească cartela sa până la cheltuirea completă a valorii înscrise în punga sa la echipamentul altui vânzător.

Periodic vânzătorul poate să-şi întoarcă valoarea reprezentată în înregistrarea valorii pungii ce se conţine în terminalul 9 sau 10, indiferent de identitatea cumpărătorului şi fără prezentarea unor tranzacţii individuale suma cărora formează mărimea totală. Lucrul acesta e posibil conectând terminalele 9 şi 10 la banca respectivă a vânzătorului 1, 2 sau 3 şi cerând întoarcerea valorii sumei tranzacţiilor. Computatorul băncii efectuează operaţia de întoarcere care elimină valoarea din punga terminalului. Computatorul băncii creditează contul fondului vânzătorului. Contoarele de valoare formează baza pentru permiterea controlului totale de valoare în circulaţie în toate pungile şi pentru repartizarea, pe bază de acord, a fondurilor reprezentând valoarea totală.

Pungile de volum 1.3, 2.3, 3.3 diferă de altele pungi, fiindcă pot încărca şi deconta valoarea prin intermediul controlului de valoare, precum şi a tranzacţiilor pungă către punga. În toate celelalte privinţe pungile sunt similare din punct de vedere tehnic, subînţelegându-se în particular ca şi pentru tranzacţiile în serie. Desenul 2 arată un contor de valoare 1.2 conţinând un indicator 11 care indică o înregistrare de valoare flotantă. Aceasta este în cazul dat mărimea netă a sumei eliberate către punga de volum 1.3, fiind diferenţa dintre mărimea valorii toate aruncate prin contor şi mărimea valorii totale întoarse prin contor. Se va aprecia faptul că iniţializările individuale aproximative şi valorii întoarse pot fi indicate la fel de bine sau în locul valorii nete, fiind uşor de căpătat valoarea netă din valorile aproximative, chiar dacă aceasta nu e indicat direct. Legătura 12 dintre contorul de valoare şi fiecare din pungile lui de volum e secretă. Punga poate fi ajustată fizic la contorul la valoare, iar securitatea asigurată prin lăcăţi fizice etc. Ca alternativă punga de volum poate fi îndepărtată de contorul de valoare, iar securitatea e realizată cu ajutorul tehnicilor criptografice. E importantă garanţia ca contorul de valoare să, indice întotdeauna mărimea exactă din punga de volum, făcând imposibile manipulaţiile frauduloase. Fiecare contor de valoare are o interfaţă 13 care poate fi un lanţ spre facilităţi de computare bancară sau o unitate de tastatură. Personalul autorizat poate introduce valori care vor fi adăugate sau scăzute din înregistrarea valorii flotante, ceea ce reprezintă crearea sau distrugerea valorii de circulaţie. În felul acesta valoarea circulaţie poate fi introdusă în volum, posibil zilnic, în loc să fie introdusă la cereri şi comenzi individuale.

Folosirea valorii flotante a înregistrării va permite în felul acesta terminalelor să facă schimb de valoare între cumpărători fără computator şi fără necesitatea de a menţine un număr mare de conturi sau de a analiza detaliile contului pentru reconcilierea conturilor.

Înşişi cumpărătorii pot folosi înregistrările valorii din pungă în timpul schimbului dintre ei sau a împrumutului la vânzători. E prevăzut ca înregistrările valorii pungii să poată fi transmise pe contul individuale din înregistrarea valorii flotante prin intermediul unei proceduri de revendicare din înregistrarea valorii flotante într-o manieră similare celei a vânzătorilor.

Pungile pot fi folosite la scară internaţională încercând diferite valute în ele. E prevăzut că fiecare ţară sau grup de ţări va avea o înregistrare a valorii flotante în valuta respectivă. Cererea cumpărătorului de umplere a pungii sale cu valută străină poate fi efectuată pe contul său de la domiciliu, decontând suma respectivă valută proprie şi majorând mărimea valorii înregistrării flotante respective în valută străină.

O înregistrare de valoare din pungă ţinută în pungă poate fi convertită la cerere în diferite valute, convertire fiind efectuată la rata respectivă, şi mărimea înregistrării flotante a sumei poate fi transformată dintr-o valută în alt exact la fel se efectuează transferul de fonduri dintre valute.

Fig. 3 arată procedura efectuării unei tranzacţii în afara liniei computatorului în prima variantă a invenţiei. Ambele pungi au capacitatea de a aplica sistemul criptografic asimetric RSA. Punga transmiţătoare are o memorie SS care conţine înregistrarea valorii SVR şi următoarele chei RSA: cheile publice şi secrete PKS şi SKS ale pungii transmiţătoare şi cheia globală publică PKg. În afară de aceasta aici se mai conţine mesajul datelor certificate [PKS]*SKg. Acest mesaj este o cheie publică unică a pungii transmiţătoare marcată de computatorul principal cu cheia lui globală secretă SKg. Cheia publică PKS este în felul acesta certificată electronici ca validă pentru sistem. Punga

receptoare are memorie RS care conţine o înregistrare acumulativă a valorii Rvr şi propriile chei RSA ale pungii receptoare: cheile publice şi secrete PKr, SKr, cheia globală publică PKg şi datele transmisibile despre chiea publică certificată [PKr]*SKg.

Prima etapă procedurii tranzacţiei pentru punga receptoare este afişarea numărului R ce determină tranzacţia. El e căpătat din combinaţia ce constă din identitatea pungii receptoare şi numărul de ordine al tranzacţiei acestei pungi. Între pungi e instalată o legătură reciprocă; e posibilă una locală - cu ajutorul conectării directe sau cu ajutorul reţelei infraroşii sau la distanţă - cu ajutorul modemului şi a reţelei telefonice.

Următoarele etape sunt:

1. Punga receptoare transmite un mesaj-cerere care este [PKr]*SKg+[R]*SKr

2. Punga transmiţătoare poate controla [PKr]*SKg, folosind cheia publică globală PKg. Aceasta-i dă pungii transmiţătoare cheia autentică PKr pentru a verifica [R]*SK şi a-l primi pe R.

3. Punga transmiţătoare formează un mesaj despre mărimea tranzacţiei Vr din valoarea V pe care vrea să o transmită şi din mesajul de cerere a lui R. Acest mesaj e marcat de cheia secretă a pungii transmiţătoare pentru a da următorul mesaj de tranzacţie a valorii care e stocat în punga transmiţătoare:

[PKs]*SKg+[VR]*SKS

4. Punga transmiţătoare creează un mesaj al formei [PKs]*SKg+[Pr]SKS unde P este o combinaţie a valorii ***v*** ce trebuie transferată şi identificatorului că mesajul este unul de transmitere.

5. Mărimea valorii cerute V e scăzută din înregistrarea valorii pungii SVr.

6. Detaliile mesajului de transmitere sunt introduse în protocolul STL al pungii transmiţătoare.

7. Mesajul de transmitere e transmis către punga transmiţătoare.

8. Punga receptoare determină cheia publică PKs, folosind cheia publică PKg în timpul verificării mesajului

[PKs]*SKg

9. Folosirea cheii publice PKs permite determinarea [PR]*SKS şi deci primirea PRIVIND.

10. Mesajul R e controlat pentru a se asigura că e identic pungii receptoare şi numărului corespunzător al tranzacţiei. Dacă nu e aşa, tranzacţia e anulată.

11. Punga receptoare protocolează mesajul de transmitere în protocolul său RTL.

12. Punga transmiţătoare transmite mesajul ce conţine valoarea tranzacţiei. Lucrul acesta poate fi efectuat după întreruperea tranzacţiei pentru orice durată de timp cerută.

13. Punga receptoare obţine cheia publică PKs, folosind cheia publică PKg şi verificând mesajul [PKs]*SKg.

14. Folosirea cheia publice PKs permite în felul acesta controlul [VR]*SKs şi deci primirea VR.

15. Mesajul R e controlat pentru a asigura că e identic pungii receptoare şi numărului corespunzător al tranzacţiei. Dacă nu e aşa, tranzacţia e anulată.

16. Dacă totul e bine, valoarea V e adăugată şa înregistrarea valorii din punga receptoare.

17. Către punga transmiţătoare e trimisă o înştiinţare certificată.

Cifrarea şi descifrarea RSA necesită calculul expresiei X^y mod ***n***, unde ***y*** e diferit pentru cifrare şi descifrare. În particular indicele ***y*** pentru cifrare (în varianta ci cheia secretă) e cu mult mai mare. În consecinţă, în timp ce un computator de o generaţie veche permite cifrarea informaţiei într-un timp acceptabil, aceasta nu mai corespunde adevărului pentru descifrare. Crearea unui mesaj cifrat (adică în formă numerică) reprezintă o operaţie echivalentă depăşind descifrarea, controlul unui asemenea mesaj prezintă o operaţie echivalentă depăşind cifrarea. Variantele ilustrate în desenele 4 şi 5 îi permit uneia din perechi de pungi conectate să posede perfomanţă computerială mai mică şi deci să fie mai ieftină. La o asemenea organizare unele pungi ale sistemului (pungi ale vânzătorilor) au posibilitatea completă de a folosi RSA (capacitatea de a cifra şi a descifra) în timp ce pungile rămase (ale cumpărătorilor) conţin pentru transmiterea mesajului de înscriere a valorii tranzacţiei numai sistem criptografic cu cheie simetrică. Un sistem acceptabil criptografic cu cheia simetrică este sistemul DES. Acesta cere pentru cifrare şi descifrare o perfomanţă computerială similară celei adecvate pentru cifrarea RSA.

În ceea ce priveşte fig. 4, aici e ilustrată o procedură de tranzacţie între două pungi unde punga transmiţătoare e punga consumatorului, iar punga receptoare e punga vânzătorului. Punga vânzătorului are o capacitate RSA deplină, pe timp ce punga consumatorului are facilităţii computeriale mai mici. Punga transmiţătoare are o memorie CS care conţine mărimea valorii CVR şi cheia publică globală a sistemului RSA. Plus la aceasta mai există o cheie DES_c şi mesajul cifrat certificat al informaţiei $[DES_c]$*Skg, care este cheia unică a pungii transmiţătoare, certificată de computatorul principal cu cheia lui globală secretă Skg. Punga receptoare are un volum de memorie SR care e identic memorie SR a variantei din fig. 3, ce conţine Pkr, Skr, Pkg[Pkr]*Skg.

Ca şi în varianta din fig. 3 primul pas al procedurii de definitivare a tranzacţiei pentru punga receptoare este transmiterea identificatorului tranzacţiei R. Următoarele etape sunt:

1. Punga receptoare transmite mesajul său certificat de cheia publică [Pkr]*Skg.

2. Punga transmiţătoare controlează mesajul certificat şi extrage Pkr.

3. Punga transmiţătoare cifrează mesajul său certificat, folosind Pkr. Deoarece indicele cgeii publice Pkg e mai mic, cifrarea cu ajutorul lui e mai simplă. Către punga transmiţătoare e transmis mesajul:

Epkr[[DESc]*Skg]

4. Punga receptoare descifrează la început cu cheia sa secretă ca să extragă [DESc]*Skg care este controlat cu Pkg pentru a da verificarea şi a extrage DESc.

5. Punga receptoare transmite mesajul [R]*DESc care e identofocatorul tranzacţiei E prelucrat cu un algoritm integral DES.

6. Punga receptoare descifrează mesajul în DES, extrage identificatorul tranzacţiei R şi formează mesajul valori VR şi mesajul de emitere PRIVIND îăn acelaşi fel ca şi în varianta din fig. 3.

7. Punga transmiţătoare scade mărimea V din înregistrarea mărimii valorii pungii şi transmite mesajul [PR]*DESc către punga receptoare. Mesajul de transmitere e protocolat în STL.

8. Punga receptoare descifrează [PR]*DESc şi controlează corectitudinea lui R. Dacă nu e aşa, tranzacţia e anulată.

9. Dacă totul e bine, mesajul de transmitere e memorizat în protocolul RTL.

10. Punga transmiţătoare formează mesajul despre mărime şi transmite mesajul valori [VR]*DESc către punga receptoare.

11. Punga receptore prelucrează [VR]*DESc cu ajutorul algoritmului integral DES şi controlează dacă R e corect. În caz contrar tranzacţia e anulată.

12. Mărimea valorii V e adăugată în înregistrarea mărimii valorii pungii receptoare şi către punga transmiţătoare e trimis un mesaj de înştiinţare.

Referitor la fig. 5, aici e ilustrată o procedură de tranzacţie care permite pungilor să aibă perfomanţe computeriale neegale în timpul folosirii cheilor unui sistem criptografic asimetric. În fig. 5 memoria RS a pungii receptoare are aceleaşi chei în varianta din fig, 3. Perfomanţa computerială a pungii trsm e mai mică decât cea a pungii receptoare şi în locul unei chei publice marcate punga trsm are o chei publică nemarcată (care e ţinută în secret în cazul acesta) şi o cheie marcată secretă [Skr]*Skg (care conţine de asemenea Pks).

O procedură de tranzacţie conţine următoarele etape:

1. Punga receptoare transmite mesajul marcat [Pkg]*Skg.

2. Punga transmiţătoare controlează mesajul marcat cu Pkg, controlând [Pkg]*Skg şi deci obţinând Pkr.

3. Punga transmiţătoare cifrează mesajul său marcat cu Pkr şi transmite Epkr [[Pkg]*Skg].

4. Punga receptoare descifrează mesajul la început cu folosirea cheii sale secrete Skr pentru a da [Sks]*Skg, iar apoi foloseşte cheia publică globală Pkg pentru a controla [Sks]*Skf şi a obşine Sks.

5. Punga receptoare marchează identificatorul tranzacţiei R cu Sks şi transmite [R]*Sks.

6. Punga transmiţătoare extrage R cu ajutorul Pks.

7. Punga transmiţătoare formează mesajul valoric Epks[VR] şi un mesaj de transmitere Epks[PR]. Mesajul de transmitere e protocolat în STL şi e transmis pungii receptoare.

8. Punga receptoare descifrează mesajul cu Sks pentru a extrage P şi R. R e controlat şi dacă nu e corect, tranzacţia e anulată.

9. Mesajul de transmitere e protocolat în RTL.

10. Punga transmiţătoare transmite ,mesajul valoric Epks[VR].

11. Punga receptoare descifrează mesajul cu Sks pentru a extrage V şi R. R e controlat şi, dacă nu e corect, tranzacţia e anulată.

12. Dacă totul e bine, înregistrarea mărimii valorii pungii receptoare creşte cu V, cheia Sks în punga receptoare e aruncată şi către punga transmiţătoare e transmis un mesaj de înştiinţare.

Mesajul de înştiinţare poate fi prevăzut ca o “dovadă de transmitere” în sensul că ea demonstrează că valoarea a fost transmisă, limbaj, contabil de la contul pungii transmiţătoare. De aceea “dovada de transmitere” e dovada că acumulatorul de valoare din punga transmiţătoare a fost micşorat cu valoarea cerută. Efectiv, mesajul de înştiinţare îi spune pungii receptoare că valoarea cerută i-a fost transmisă irevocabil. Înştiinţarea sau “dovada de transmitere” ia forma mesajului valoric cu excepţia faptului că un număr de dovadă P ia locul valorii V. În felul acesta mesajul de înştiinţare are forma [Pks]*Skg+[PR]*Sks. În acelaşi timp detaliile sunt introduse în protocolul pungii transmiţătoare STL. La primirea mesajului de înştiinţare punga receptoare introduce detaliile în protocolul RTL.

În virtutea protocoalelor e posibilă păstrarea intactă a finanţelor de orice tranzacţii care au fost întrerupte fie în mod accidental, fie în mod deliberat. În cazul unei dispute despre alocarea fondurilor dintre pungi pentru careva scopuri, pungile pot fi examinate şi disputa rezolvată pe baza informaţiei protocolului. Tranzacţia poate fi anulată în orice timp după ce valoarea şi mesajul de înştiinţare au fost create şi protocolate.

Când valoarea şi mesajul de înştiinţarea au fost create, e posibilă întreruperea tranzacţiei. Aceasta e ilustrat, de exemplu, cu ajutorul liniei întrerupte marcate “întrerupere”. Întreruperea la etapa aceasta e folositoare în cazul unor plăţi neprevăzute, deoarece punga receptoare va primi mesajul că fondurile cerute sunt transmise, dar nu va primi fondurile în timpul acesta. La satisfacerea cerinţelor neprevăzute tranzacţia poate fi definitivată de către punga transmiţătoare prin transmiterea unui mesaj valoric în maniera descrisă anterior. Transmiterea curentă şi receptoarea mesajului valoric sunt protocolate de către pungile respective şi tranzacţia e terminată. NU e necesar ca mesajul valoric să fie transmis direct de la punga transmiţătoare către punga receptoare, pot fi prevăzute diferite tranzacţii intermediare în care mărimea valorii considerată ca fiind în contact să fie transmisă către pungi intermediare. Aceste pungi nu vor avea acces la fondurile reprezentate de către mesajul contractual, ele vor fi accesibile numai pentru punga receptoare.

Un avantaj l procesului de întrerupere este posibilitatea să se lucreze cu pachete de tranzacţii care se află în stare de suspensie. Iar aceasta, la rândul sau, transformă sistemul într-un tot întreg cu proceduri disponibile pentru lucrul cu serii de tranzacţii.

Invenţia nu se limitează la detaliile din variantele descrise mai sus cu referinţe la figuri. De exemplu, metoda descrisă de transmitere şi receptare a cheilor criptografice poate fi înlocuită cu nu stadiu protocolar preliminar de “schimb de chei”.