(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 741 477 A2**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
10.01.2007 Bulletin 2007/02

(51) Int Cl.:
A63F 13/12 *(2006.01)*

(21) Application number: **06015875.5**

(22) Date of filing: **27.08.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
03818388.5 / 1 669 115

(71) Applicant: **SCYTL ONLINE WORLD SECURITY, S.A.**
08015 Barcelona (ES)

(72) Inventors:
- **Riera Jorba, Andreu**
  08251 Santpedor (Barcelona) (ES)
- **Borrell Viader, Joan**
  17464 Cervia de Ter (Girona) (ES)
- **Castella Roca, Jordi**
  25139 Menarguens (Lleida) (ES)
- **Bardera Bosch, Joan Miquel**
  08032 Barcelona (ES)
- **Primault, Christophe**
  08008 Barcelona (ES)

(74) Representative: **Gislon, Gabriele et al**
Torner, Juncosa i Associats, S.L.
c/ Bruc, 21
08010 Barcelona (ES)

Remarks:
This application was filed on 31 - 07 - 2006 as a divisional application to the application mentioned under INID code 62.

(54) **System for implementing a game of chance over a communications network**

(57) The recommended system comprises a set of programs through which one or more players participates in said game cooperating in the generation of chance events.

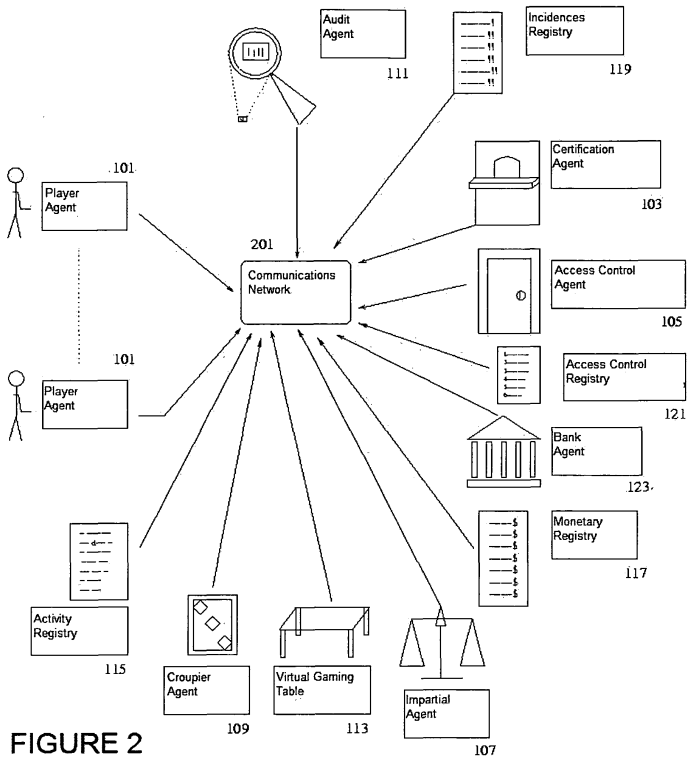

FIGURE 2

EP 1 741 477 A2

Description

Field of the invention

[0001] This invention describes a system for implementing games of chance over a communication network.

[0002] The summary of this invention contains material that may be protected by Copyright. The owners of said Copyright do not object at all to third parties reproducing the description of this patent application in its published or final version in Patent Offices, but they reserve all rights regarding the Copyright in other aspects that can be derived from said document.

Background to the invention

[0003] Gaming remotely or online gaming, offers players a series of advantages, since it gives them independence in terms of location (they do not need to be physically), and time-. Owing to these advantages, the deployment of remote gaming has increased rapidly.

[0004] The players see on site all the actions taking place during the game and Legislative Authorities periodically audits all the elements used for the gaming. This auditing guarantees that there are no mechanisms altering the random nature of the result. In the online gaming, the results are usually generated by the online casino using a pseudo random generator. However, the online casino can discard the result of said generator and choose a result that benefits it.

[0005] Some prior inventions relate to systems and/or methods for remote gaming over a communications network. A first group of inventions are described in US 4.926.327, US 4.958.835, US 5.038.022, US 6.196.920, GB 2307184, US 5.755.621 and US 5.823.879. Currently peer relationship models, also known as P2P (peer to peer), are becoming increasingly popular on the Internet. In this gaming model, the players can play without involving a casino. The most significant proposals in this field are the following patents, US 5.984.779 and US 6.152.824. The first invention relates to a game machine that allows playing on a casino without the need of an intermediary, also introducing the possibility that the machines can be connected remotely over a communication network such as the Internet. The players hire the machines and all the prizes are distributed among the game participants. It does not describe the methods for generating the random factor, nor the security or honesty of the gaming system. The second invention describes the architecture of an Online Casino which allows the game to be played with a central figure who distributes the messages without intervening in the game. Said system encrypts the communications among the game participants to ensure their privacy. Also it does not describe any method for protecting the information generated during the game, so there is no tamperproof evidence that the game was played honestly. Players are vulnerable to the collaboration between the system operator and one of the players on their benefit.

[0006] The present invention relates to a game of chance system, preferably remote, which according to the distributions of its elements allows a gaming with or without an intermediary. When the game is implemented with an intermediary, the latter takes an active part in the game. Typically, the intermediary would be an online casino. In the second organisation, the players play directly among themselves, according to a P2P model.

Brief summary of the invention

[0007] This invention describes a system for implementing a game of chance. The system includes a set of programs and/or implementing platforms forming a Player Agent 101 through which at least one of said players participates in said game.

[0008] According to an embodiment example, the preferred system also includes a set of programs and/or implementing platforms forming a Croupier Agent 109, intended to perform the actions corresponding to a Croupier in a casino game.

[0009] The invention proposes the game events be generated with the cooperation of the Croupier Agent and/or one or more Player Agent(s).

[0010] Other aspects and details of the invention are referenced in the detailed summary thereof, with reference to the figures.

Brief description of the Figures

[0011]

Figure 1 represents the elements making up the system for implementing an impartial game of chance over a communications network.

Figure 2 represents an example of how the elements of said system of this invention interact together by means of a Communications Network 201.

Figure 3 represents the game stages for a player..

Figure 4 represents the stages involved in the development of the game.

Detailed description of the invention

[0012] The essence of games of chance is to obtain at least one event (a roulette position, a card in a pack, the face of a die, etc.) in a random way, determining the game result using at least this event. In the on site games the events are obtained by means of a roulette wheel, a pack of cards, or dice for example.

[0013] In order to participate in the game over a communications network, the players need a set of programs and/or implementing platforms. Hereinafter this set of programs will be called Player Agent 101, which can be an application able to establish remote secure connections, or a Plug-In for the player's Internet browser. The

implementing platform, as its name implies, allows the Player Agent 101 to be deployed, and is able to connect to a communication network. The implementing platform can be a PC, a digital personal assistant, or a mobile telephone terminal, for example.

[0014] This invention considers the possibility of an Impartial Entity having a set of programs and/or implementing platforms so that it can take a more active part in the remote game, for example by generating the game events or by making the Player Agent 101 available to the players. Hereinafter, the term Impartial Agent 107 will be applied to this set of programs that preferably form an application that can provide a secure remote connection. The associated implementing platform, as its name implies, allows the Impartial Agent 107 to be implemented. This implementing platform can be a computer, or a secure tamperproof module that can internally execute applications, such as Hardware Secure Module (HSM) nShield by the manufacturer of nCipher [http://www.ncipher.com/nshield, 16/06/2003].

[0015] In a remote gaming system, the functions of the croupier can be automated by means of associated communication means and/or programs. Hereinafter this set will be called Croupier Agent 109.

[0016] In a first option, the Impartial Agent 107 implements a cryptographic protocol to generate impartial game events, in combination with the Croupier Agent 109. In a second option, the Impartial Agent 107 generates impartial game events. In a third option, the Croupier Agent 109 implements a cryptographic protocol to generate impartial game events, in combination with the Player Agent 101.

[0017] In any of the three options mentioned, pseudo random values are obtained. When any random value is obtained during the gaming process, it is obtained via pseudo random number generation routines (PRNG).

[0018] As mentioned in a first option, the Croupier Agent 109 applies a cryptographic protocol for the Impartial Generation of Game Events 405, together with the Impartial Agent 107. Five non-limiting embodiments of said first option, are provided below. The embodiments use a commitment cryptographic protocol as a basic tool. A first commitment protocol was introduced by Blum in 1982 [Blum M., Coin flipping by telephone: a protocol for solving impossible problems, Proc. IEEE Computer Conference, pages 133-137, IEEE, 1982]. In a commitment protocol one part, or commitment element, is compromised of certain information X to other parties or commitment verifiers. A commitment protocol C_p is made up of two phases; a commitment phase followed by a commitment release phase. In the commitment phase, the commitment element calculates a transformation T of the information X, $T = C_P\{X\}$, and makes T available to the commitment verifiers. In the second phase, the commitment element reveals X and/or the information for verifying the commitment, $T == C_P\{X\}$. The procedure can be described with the following physical example: In the first phase each participant places certain information in a box, which he locks and hands to the rest of the participants. In the second phase, he delivers the key for opening the box and recovering the information inside the initial box. The commitment verifiers cannot know anything about X from T, and the committed information X cannot be altered by its owner between the first and second stages. A general overview of the state of the art related to commitment protocols can be found in [Schneier B., Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C, Second Edition, John Wiley & Sons, 1996].

[0019] In a first embodiment of said first option, the player places a bet A by means of his/her Player Agent 101. The Player Agent 101 is committed to the bet A by means of a cryptographic commitment protocol C_P, and obtains a transformation T, $T = C_P\{A\}$. The Player Agent 101 makes this accessible to the Croupier Agent 109. Said Croupier Agent 109 obtains a value V_1 in a random manner from which the result of the game is derived, and makes V_1 accessible to the Player Agent 101. Next the Player Agent 101 makes the player's bet A accessible to the Croupier Agent 109 who checks that the commitment protocol $T == C_P\{A\}$ is correct.

[0020] Said first embodiment of the first option is securer if, in addition, the following steps are taken:

- The Croupier Agent 109 digitally signs V_1 with the private component S_C of its pair of keys, $X = S_C(V_1)$ and makes X accessible to the Player Agent 101.
- The Player Agent 101 digitally signs A with the private component of a pair of asymmetric keys belonging to said player, such as (P_J, S_J), (P^A_J, S^A_J), (P^P_J, S^P_J), (P^G_J, S^G_J).

In a second embodiment of said first option, the player places a bet A by means of the Player Agent 101. The Player Agent 101 implements a commitment protocol C_P with the bet, and obtains a transformation of the bet T_1, $T_1 = C_P\{A\}$. The Player Agent 101 makes T_1 accessible to the Croupier Agent 109. The Croupier Agent 109 obtains a first value V_1 in a random manner and implements a commitment protocol with V_1 obtaining a transformation T_2, $T_2 = C_P\{V_1\}$. The Croupier Agent 109 makes T_1 and T_2 accessible to the Impartial Agent 107. The Impartial Agent 107 obtains a second value V_2 and by means of the private component S_I of the pair of keys corresponding to the Impartial Authority (S_I, P_I) it calculates a digital signature X_1 on $\{V_2, T_1, T_2\}$, $X_1 = S_1<V_2/T_1/T_2>$. The Impartial Agent 107 makes V_2 and X_1 accessible to the Croupier Agent 109. The Croupier Agent 109 makes V_1, V_2 and X_1 accessible to the Player Agent 101. The Player Agent 101 makes A accessible to the Croupier Agent 109. In this instant, the Croupier Agent 109 and the Player Agent 101 obtains said game event from V_1 and V_2.

[0021] In a third embodiment of said first option, the Player Agent 101 makes available a player's request to obtain a game event. The Croupier Agent 109 obtains a first value V_1 in a random manner and implements a com-

mitment protocol C_P with V_1 obtaining a transformation T_1, $T_1 = C_P\{V_1\}$. The Croupier Agent 109 makes T_1 accessible to the Player Agent 101 and to the Impartial Agent. The Player Agent 101 makes a player's bet A accessible to the Croupier Agent 109. The Impartial Agent 107 obtains a second value V_2 and by means of the private component S_I of the pair of keys corresponding to the Impartial Authority (P_I, S_I), calculates a digital signature X_1 on $\{V_2, T_1\}$, $X_1 = S_I<V_2|T_1>$. The Impartial Agent 107 makes V_2 and X_1 accessible to the Croupier Agent 109. The Croupier Agent 109 makes V_1, T_1, V_2 and X_1 accessible to the Player Agent 101. The Croupier Agent 109 and the Player Agent 101 obtain said game event from V_1 and V_2.

[0022] In a fourth embodiment of said first option, the Player Agent 101 makes a player's bet A accessible to the Croupier Agent 109. The Croupier Agent 109 obtains a first value V_1 in a random manner and implements a commitment protocol C_P with V_1 obtaining a transformation T_1, $T_1 = C_P\{V_1\}$. The Croupier Agent 109 makes $T1$ and A accessible to the Impartial Agent 107. The Impartial Agent 107 obtains a second value V_2 and by means of the private component S_1 of the pair of keys corresponding to the Impartial Authority (P_I, S_I) calculates a digital signature X_1 on $\{T_1, V_2, A\}$, $X_1 = S_I<V_2/T_1/A>$. The Impartial Agent 107 makes V_2 and X_1 accessible to the Croupier Agent 109. The Croupier Agent 109 makes V_1, V_2, T_1 and X_1 available to the Player Agent 101. The Croupier Agent 109 and the Player Agent 101 obtain said game event from V_1 and V_2.

[0023] In a fifth embodiment of said first option, the player places a bet A by means of the Player Agent 101. The Player Agent 101 implements a commitment protocol C_P with A, and obtains a transformation T_1, $T_1 = C_P\{A\}$. The Player Agent 101 makes T_1 accessible to the Croupier Agent 109. The Croupier Agent 109 obtains a first value V_1 in a random manner and implements a commitment protocol C_P with V_1, obtaining a transformation T_2, $T_2 = C_P\{V_1\}$. The Croupier Agent 109 makes T_2 accessible to the Player Agent 101. The Player Agent 101 makes A accessible to the Croupier Agent 109, which makes A and T_2 accessible to the Impartial Agent 107. The Impartial Agent 107 obtains a second value V_2 and by means of the private component S_I of the pair of keys corresponding to the Impartial Authority (P_I, S_I) calculates a digital signature X_1 on $\{T_2, A, V_2\}$, $X_1 = S_I<V_2/T_2/A>$. The Impartial Agent 107 makes V_2 and X_1 accessible to the Croupier Agent 109. The Croupier Agent 109 makes V_1, V_2, and X_1 available to the Player Agent 101. The Croupier Agent 109 and the Player Agent 101 obtain said game event from V_1 and V_2.

[0024] Said second, third, fourth and fifth embodiments of said first option are more secure if, in addition, the following steps are taken:

- The Player Agent 101 digitally signs A with the private component of a pair of asymmetric keys belonging to said player, such as (P_j, S_j), (P^A_J, S^A_J), (P^P_J, S^P_J), (P^G_j, S^G_J).
- The Croupier Agent 109 digitally signs T_1 with the private component S_C of its pair of keys (P_c, S_c), $X_0 = S_C< V_1>$ and makes X_0 accessible to the Impartial Agent 107. The Impartial Agent 107 includes X_0 *in* X_1, $X_1 = S_I<V_2/T_1/T_2/X_0>$.
- The Croupier Agent 109 makes the identifier Id_M of the Virtual Gaming Table 113 accessible to the Impartial Agent 107. The Impartial Agent 107 includes Id_M in the digital signature X_1, $X_1 = S_I<V_2/T_1/T_2/Id_M>$.
- The Impartial Agent 107 includes a serial number N_i in each digital signature it creates.

As mentioned in a second option, the Impartial Agent 107 generates impartial game events. These events are impartially generated by means of a PRGN such as the ones described above. In a first embodiment of the second option, the Impartial Agent attaches the digital signature of the game event. The digital signature is generated with the private component SI of the pair of keys of the Impartial Authority (PI, SI). In a second embodiment of the second option, the Impartial Agent attaches the result of applying a keyed digest function to the game event. The key used is kept in secret and only the Player Agent 101 and the Impartial Agent possess it. The keyed digest functions are typically called MAC, the document [Menezes, A.J., Oorschot, P.C., Vanstone, S.A., Handbook of Applied Cryptography, CRC Press, 1997] contains a detailed description of their different variants and properties.

[0025] As mentioned in a third option, the Player Agent 101 implements a cryptographic protocol for the Impartial Generation of Game Events 405, together with the Croupier Agent 109. In a first embodiment of the third option, the Player Agent 101 and the Croupier Agent 109 carry out one of the protocols described in the International application [PCT/ES02/00485]. In a second embodiment of the third option, the Player Agent 101 and the Croupier Agent 109 carry out one of the protocols described in the Patent of Invention US 6.264.557. In a third embodiment of the third option, the Player Agent 101 and the Croupier Agent 109 carry out one of the protocols described in the Patent of Invention US 6.165.072.

[0026] The end of a time period set by the Croupier Agent 109, or the Player Agent 101 performing the croupier's functions, indicates the throw or game hand to be completed,

Claims

1. System for implementing a game of chance over a communications network, comprising the following elements:

a) a set of programs and/or implementing platforms forming one or more Player Agents (101)

through which at least one player participates in said game; and
b) a set of programs and/or implementing platforms forming a Croupier Agent (109), intended to carry out the actions corresponding to a Croupier in a casino type game; and
c) a cryptographic protocol for generating impartial game events such as a position on a roulette wheel, a card in a pack, or a face of a die, with the co-operation of said Croupier Agent (109) and a set of programs and/or implementing platforms forming an Impartial Agent (107).

2. System according to claim 1, **characterised in that** said cryptographic protocol for generating impartial game events, such as a position on a roulette wheel, a card in a pack, or a face of a die, generates said impartial game events with the co-operation of at least two of said Player Agents (101), pertaining to two different players.

3. System according to claim 1, **characterised in that** said cryptographic protocol for generating impartial game events such as a position on a roulette wheel, a card in a pack, or a face of a die, generates said impartial game events with the co-operation of at least one of said Player Agents (101) and said Croupier Agent (109).

4. Method for implementing a game of chance comprising an Impartial Agent in charge to generate the chance events and one or more Player Agents through which players participate in chance games; where the chance events are generated with the co-operation of two or more Player Agents or with the cooperation of the Impartial Agent and one or more Player Agents.

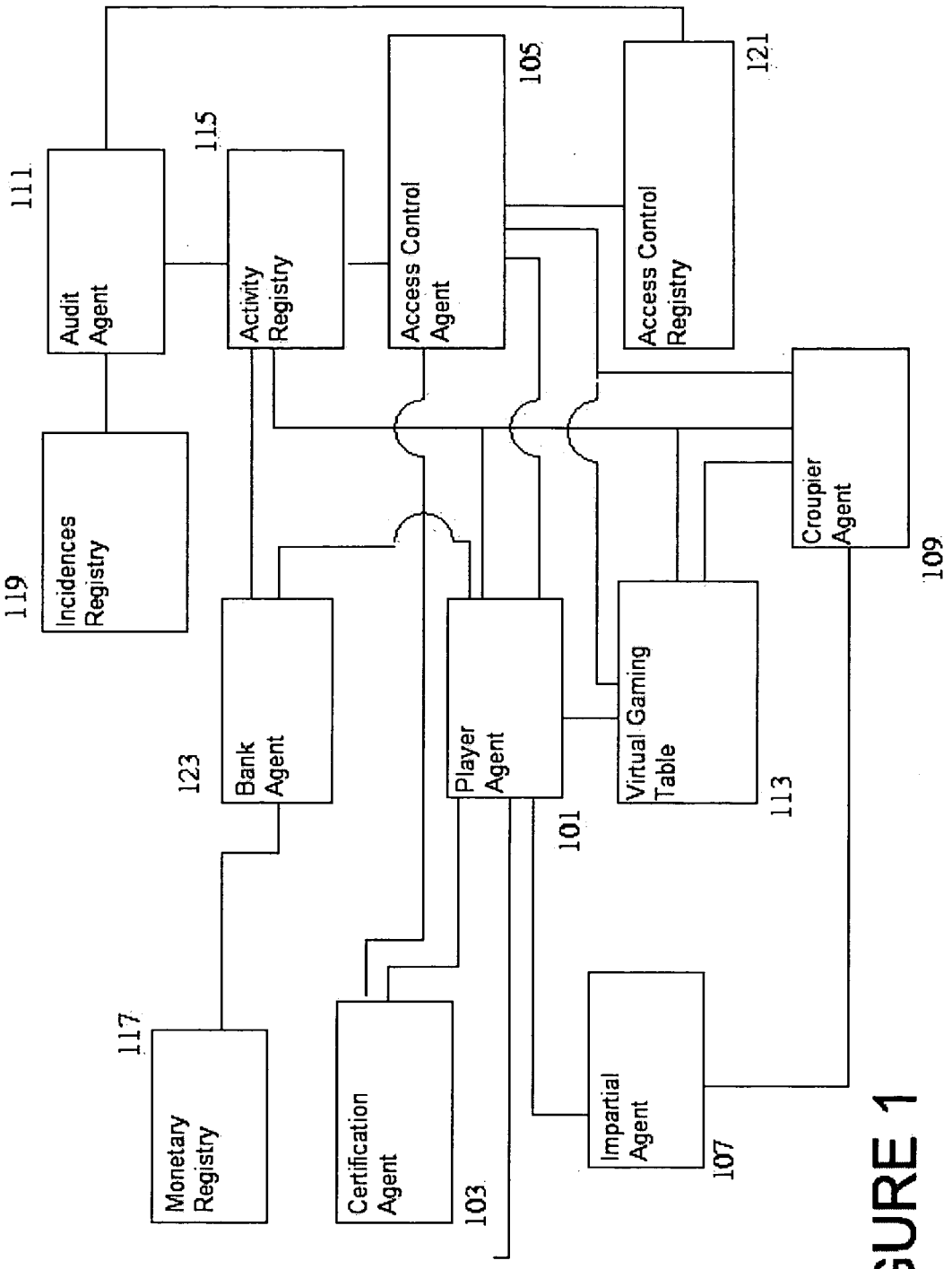
Audit Agent
111
Activity Registry
115
Access Control Agent
105
Access Control Registry
121
Incidences Registry
119
Croupier Agent
109
Bank Agent
123
Player Agent
101
Virtual Gaming Table
113
Monetary Registry
117
Certification Agent
103
Impartial Agent
107

FIGURE 1

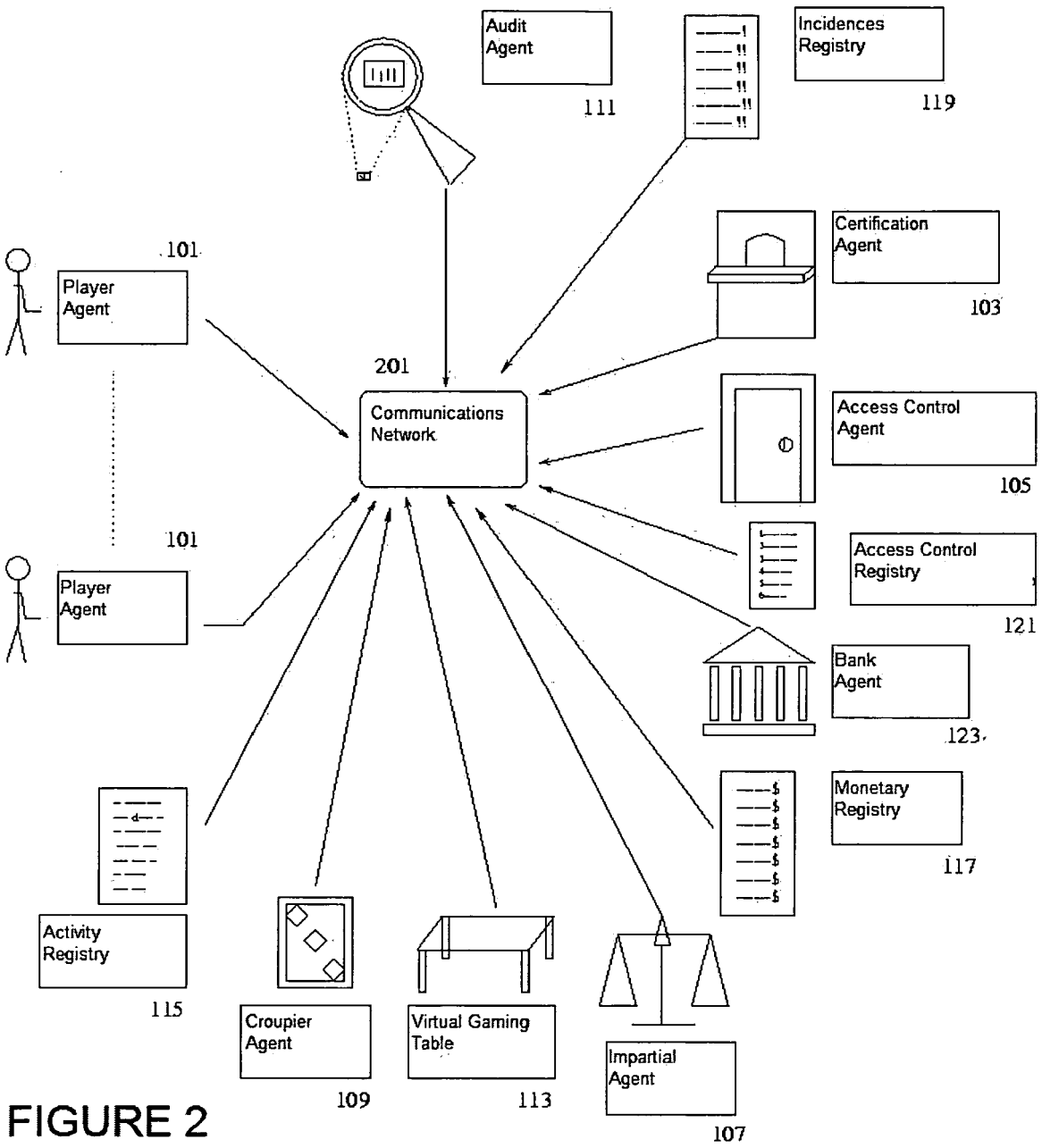
Audit Agent
111
Incidences Registry
119
Certification Agent
103
Player Agent
101
201
Communications Network
Access Control Agent
105
Player Agent
101
Access Control Registry
121
Bank Agent
123
Monetary Registry
117
Activity Registry
115
Croupier Agent
109
Virtual Gaming Table
113
Impartial Agent
107

FIGURE 2

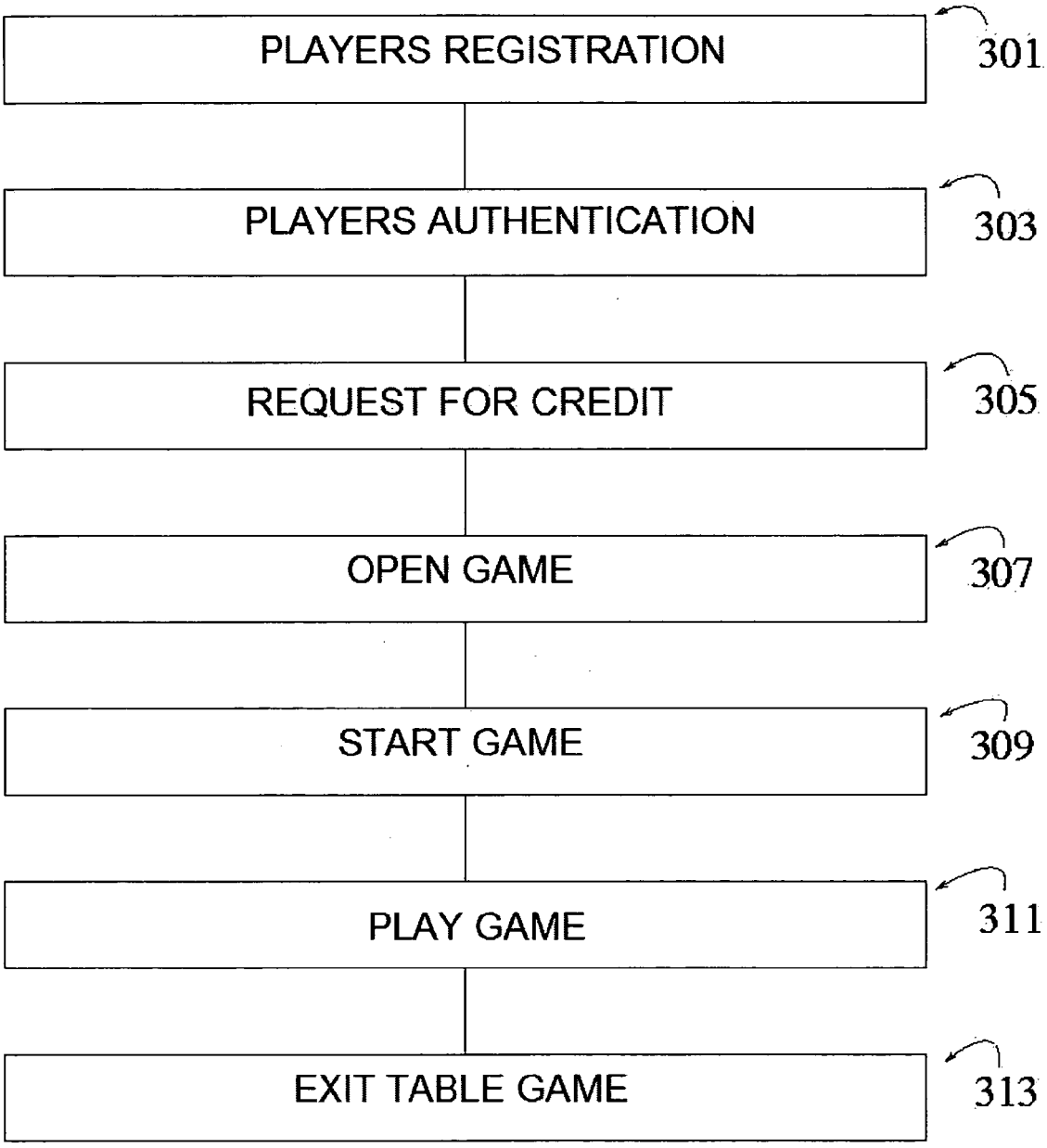
PLAYERS REGISTRATION
301
PLAYERS AUTHENTICATION
303
REQUEST FOR CREDIT
305
OPEN GAME
307
START GAME
309
PLAY GAME
311
EXIT TABLE GAME
313

FIGURE 3

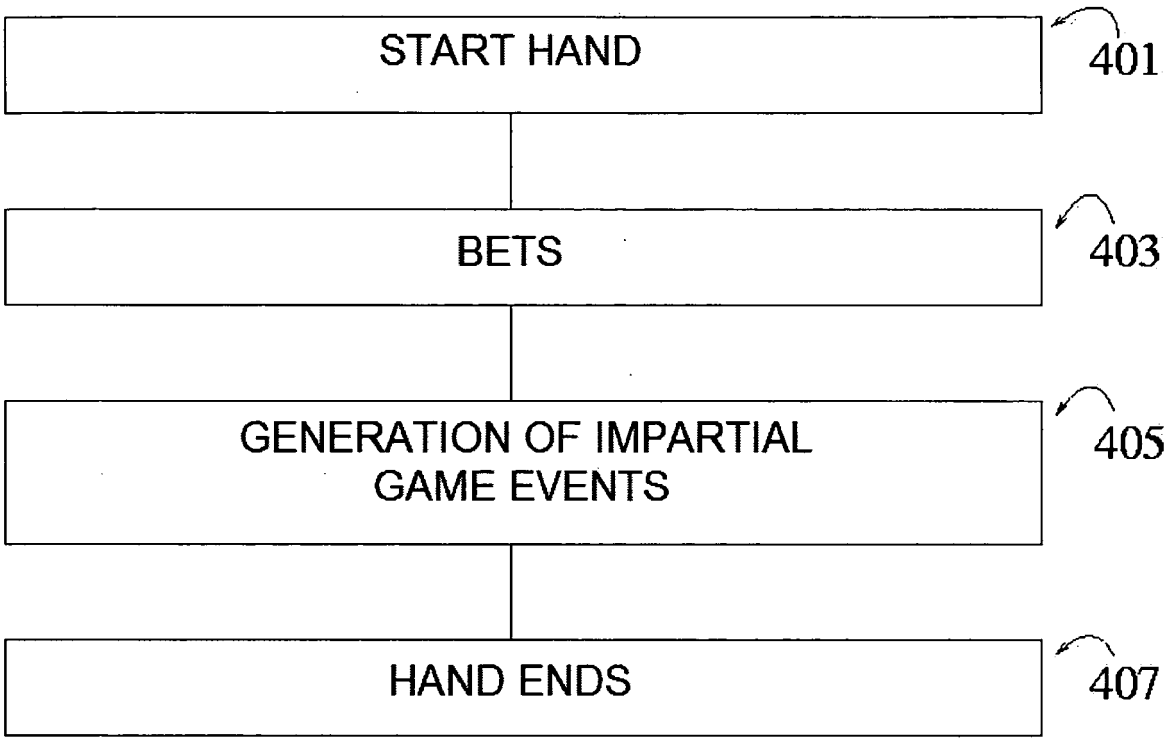
START HAND
401
BETS
403
GENERATION OF IMPARTIAL GAME EVENTS
405
HAND ENDS
407

FIGURE 4

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 4926327 A **[0005]**
- US 4958835 A **[0005]**
- US 5038022 A **[0005]**
- US 6196920 B **[0005]**
- GB 2307184 A **[0005]**
- US 5755621 A **[0005]**
- US 5823879 A **[0005]**
- US 5984779 A **[0005]**
- US 6152824 A **[0005]**
- ES 0200485 W **[0025]**
- US 6264557 B **[0025]**
- US 6165072 A **[0025]**

Non-patent literature cited in the description

- **BLUM M.** Coin flipping by telephone: a protocol for solving impossible problems. *Proc. IEEE Computer Conference,* 1982, 133-137 **[0018]**
- **SCHNEIER B.** Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1996 **[0018]**
- **MENEZES, A.J. ; OORSCHOT, P.C. ; VANSTONE, S.A.** Handbook of Applied Cryptography. CRC Press, 1997 **[0024]**