(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 October 2012 (11.10.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/138483 A1

(51) International Patent Classification:
G06Q 30/00 (2012.01)

(21) International Application Number:
PCT/US2012/030179

(22) International Filing Date:
22 March 2012 (22.03.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/081,367 6 April 2011 (06.04.2011) US

(71) Applicant *(for all designated States except US)*: **EBAY INC.** [US/US]; 2145 Hamilton Avenue, San Jose, California 95125 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **NUZZI, Frank Anthony** [US/US]; 2616 Windview Lane, Pflugerville, Texas 78660 (US).

(74) Agents: **SCHEER, Bradley W.** et al.; P.O. Box 2938, Minneapolis, Minnesota 55402 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: METHOD AND SYSTEM TO CONFIRM OWNERSHIP OF DIGITAL GOODS

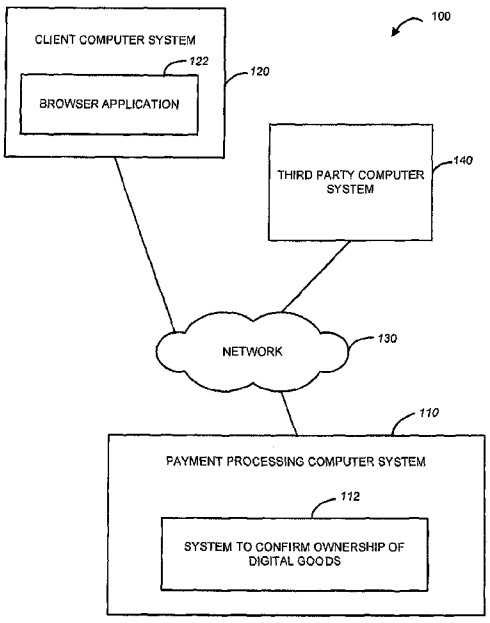

FIG. 1

(57) **Abstract**: A method and system to confirm ownership of digital goods is provided. In one embodiment, the method comprises receiving, from a client device via a data network interface, a request for a digital good, completing one or more micro transactions with respect to a financial account, generating a code utilizing information derived from the one or more micro transactions and embedding the code into a first copy of the digital good, the code to be used to confirm ownership of the digital good.

WO 2012/138483 A1

METHOD AND SYSTEM TO CONFIRM OWNERSHIP OF DIGITAL GOODS

CLAIM OF PRIORITY

[0001] This PCT application claims the benefit of the filing date of U.S. Patent Application Serial No. 13/081,367, filed April 6, 2011 entitled, "METHOD AND SYSTEM TO CONFIRM OWNERSHIP OF DIGITAL GOODS," the entire content of which is incorporated herein by reference.

TECHNICAL FIELD

[0002] This application relates to the technical fields of software and/or hardware technology and, in one example embodiment, to system and method to confirm ownership of digital goods.

BACKGROUND

[0003] Digital Rights Management ("DRM") is a term used to describe a range of techniques that use information about rights and rightsholders to manage proprietary content and the terms and conditions on which the content (e.g., digital goods, such as music or video clips) is made available to users. DRM-protected content is distributed, possibly together with a set of consumption rights, in encrypted form. Thus, only authorized parties, usually those that have paid for the content, are able to consume the content.

BRIEF DESCRIPTION OF DRAWINGS

[0004] Embodiments of the present invention are illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like reference numbers indicate similar elements and in which:

[0005] Fig. 1 is a diagrammatic representation of a network environment within which an example method and system to confirm ownership of digital goods may be implemented;

[0006] Fig. 2 is block diagram of a system to generate code suitable to confirm ownership of digital goods, in accordance with one example

embodiment;

[0007] Fig. 3 is a flow chart of a method to generate a code that can be used to confirm ownership of digital goods, in accordance with an example embodiment;

[0008] Fig. 4 is a flow chart of a method to recover a code that can be used to confirm ownership of digital goods, in accordance with an example embodiment;

[0009] Fig. 5 is a diagrammatic representation of an example machine in the form of a computer system within which a set of instructions, for causing the machine to perform any one or more of the methodologies discussed herein, may be executed.

DETAILED DESCRIPTION

[0010] A method and system to confirm ownership of digital goods is described. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of an embodiment of the present invention. It will be evident, however, to one skilled in the art that the present invention may be practiced without these specific details.

[0011] As used herein, the term "or" may be construed in either an inclusive or exclusive sense. Similarly, the term "exemplary" is construed merely to mean an example of something or an exemplar and not necessarily a preferred or ideal means of accomplishing a goal. Additionally, although various exemplary embodiments discussed below focus on administration of Java-based servers and related environments, the embodiments are given merely for clarity in disclosure. Thus, any type of server environment, including various system architectures, may employ various embodiments of the application-centric resources system and method described herein and is considered as being within a scope of the present invention.

[0012] In some existing systems, the owner (purchaser or consumer) of a

digital good may be unable to send the purchased digital good to another person, as a purchased digital good may be tied to one or more specific devices. If the user who has purchased the digital good wishes to move the DRM-protected digital good to another device, the user may need to explicitly authorize that device. The number of devices that may be used to play back a DRM-protected digital good is often limited.

[0013] Method and system are provided to permit the owner of a digital good to confirm or recover ownership of previously purchased digital good utilizing information derived from series financial micro transactions. A financial micro transaction is a financial transaction that involves a deposit or a withdrawal of certain, typically small, amount to/from a financial account of a user.

[0014] The micro transactions that may be used to generate a DRM key could be a series of small debits and credits to/from a financial account that are identifiable only to the holder of the financial account. The financial institution that is being used by the payment processing system may be, e.g., an online payment provider, a credit card provider, a bank, etc. The consumer of the digital good may be instructed by the payment processing system, using a computer-implemented user interface (UI), to use information derived from the micro transaction as a software key in order to indicate that they are the owner of the digital goods. For example, the user may be instructed to type into a designated field the string consisting of the type of purchased digital good and the amount involved in the micro transaction. One of the advantages of using information derived from a micro transaction to authenticate an owner of a digital good is that a consumer's financial information, such as the amounts involved in transactions, is typically kept private to the consumer.

[0015] In operation, a user may indicate, using a computer-implemented user interface (UI), that she wishes to purchase a digital good, such as a song or a video. The user may also indicate whether the song is being purchased for themselves or for another consumer. In response to such request, a payment processing system (which may be an on-line financial transaction service) may

process payment transaction for the user and also complete one or more micro transactions. The payment processing system may then embed into the digital good, as a DRM key or as part of a DRM key, information derived from the one or more micro transactions. In one example embodiment, a DRM key may be generated to include encrypted information about the user and the one or more micro transactions (e.g., the user's account number, the micro transaction amount, etc., e.g., using Secure Hash Algorithm (SHA). Thus generated DRM key, in one embodiment, is not designed to be decrypted and therefore cannot be manipulated to reveal the underlying information. The DRM key that the payment processing system embeds into the digital good may be utilized to authenticate a user as the owner of the digital good.

[0016] For example, when the user requests play back of media content that has DRM key embedded as described above, the embedded DRM key is extracted and communicated from the playback system (e.g., a playback system executing on the user's client computer or a portable playback device) to the computer system of the service provider, e.g., via a computer network communication. At the computer system of the service provider, the received DRM key is compared to the stored reference key. The authorization to play the media content is provided to the playback system only of the DRM key extracted from the media content matches the stored reference key.

[0017] In the instance were a user needs to reacquire a previously purchased digital good, e.g., where the owner has lost or no longer has access to the copy of the purchased digital good, the user may be instructed to make another series of small micro transactions directed to the user's financial account, using the same amount(s) as during the original micro transaction(s). The payment processing system would then recreate the DRM key for the purchased digital good, embed it in a new copy of the digital good and make it available to the user. A micro transaction may thus be used by the payment processing system to permit recovery by the consumer of a previously purchased digital good.

[0018] In one example embodiment, when a digital good is purchased,

the producer or retailer of the digital good may contact the payment provider indicating that a purchase has been made. Upon electronic checkout, the purchaser of the digital good may identify the consumer of the digital good (either self or another person) and a preferred financial institution. In the case where the purchaser of the digital good is not the consumer, the purchaser may provide information identifying an online financial institution where the consumer could view the micro transaction amounts. In the case that the consumer is a customer of an online payment service, the purchaser may provide the consumer's email address (or other identification information) in lieu of the identification of the financial institution. In that case, the consumer would use their account with the online payment service to view the micro transactions and thus obtain information needed to access the digital good. In some embodiment, a producer of digital goods may be permitted to specify a default financial institution that is to be used for payment.

[0019] The payment processing system may be configured to perform a micro transaction, derive a key from data associated with the micro transaction, embed the derived key into the digital good that is being purchased, and make the digital good having the embedded key available to the consumer. In some embodiments, the payment processing system may transmit the purchased digital good to the consumer. In other embodiments, the payment processing system may transmit the digital good having the embedded key to the producer, so that the consumer can obtain the digital good from the producer of the digital good.

[0020] A series of micro transactions used for generating a DRM key could vary in the number of transactions, in amount, and in transaction type. For example, if the digital good is quite expensive, a payment processing system may use a greater number of micro transactions. For example, a payment processing system may use two micro transactions comprising two small deposits to generate a DRM key for a digital good that costs one dollar, but four micro transactions comprising both deposit and withdrawal amounts to generate a DRM key for a digital good that costs one hundred dollars. An example method and system to confirm ownership of digital goods may be implemented in the context of a network environment illustrated in Fig. 1.

[0021] As shown in Fig. 1, a network environment 100 may include a payment processing computer system 110 and a client computer system 120. The client system 120 may host a browser application 122 and may have access to the payment processing computer system 110 via a communications network 130. The communications network 130 may be a public network (e.g., the Internet, a wireless network, etc.) or a private network (e.g., a local area network (LAN), a wide area network (WAN), Intranet, etc.).

[0022] The client computer system 120 may utilize the browser application 122 to access payment processing services provided by the payment processing computer system 110. In one embodiment, the payment processing computer system 110 may host a system 112 that may be configured to confirm ownership of digital goods. As described above, a user may send a request to purchase a digital good (e.g., a song) from the client computer system 120. The request may be sent to a third party computer system 140 operated by a producer of digital goods and the requested song in particular and then forwarded to the payment processing computer system 110 together with the requested song. The payment processing computer system 110 may then authenticate the requesting user, if necessary, as being authorized to use a certain financial account and then engage the system to confirm ownership of digital goods 112 to complete a series of micro transactions with respect to the financial account.

[0023] As stated above, the series of micro transactions may be one or more small debits and credits to/from a financial account that are identifiable only to the holder of the financial account. The system to confirm ownership of digital goods 112 may then generate a code derived from information associated from the completed micro transactions and embed it into the song received from the third party computer system 140. The information derived from the completed micro transactions may include, but not limited to, the username associated with the financial account (e.g., where the user's financial account is associated with an online payment service), bank account type, bank account number, the amount involved in the micro transaction, the type and/or format of the requested digital good, the name of the requested song, etc.

[0024] In some embodiments, a copy of the requested digital good is provided to the payment processing computer system 110 from the third party computer system 140. The payment processing computer system 110 may then transmit to the third party computer system 140 the copy of the requested digital good modified to include the embedded code. The third party computer system 140 may then transmit the copy of the requested digital good modified to include the embedded code to the originator of the request to purchase the digital good. In some other embodiments, the payment processing computer system 110 may also be configured to serve as a producer of digital goods. A request from a user to purchase a song may then be received at the payment processing computer system 110. The payment processing computer system 110 may then transmit the copy of the requested song modified to include the embedded code directly to the computer system of the requesting user, e.g., to the client computer system 120. In yet another embodiment, a user may obtain a digital good from the third party computer system 140 and then send it to the payment processing computer system 110 for processing by the system 112 to confirm ownership of digital goods.

[0025] Fig. 2 is a block diagram of a system 200 to generate code suitable to confirm ownership of digital goods that, in some embodiments, corresponds to the system to confirm ownership of digital goods 112 of Fig. 1. As shown in Fig. 2, the system 200 includes a communications module 202, a transaction module 204, a code generator 206, and an embedding module 208. The communications module 202 may be configured to receive a request for a digital good from a client system (e.g., from the client system 120 of Fig. 1), as well as copies of digital goods and other information, such as information related to the requesting user's financial account. The transaction module 204 may be configured to complete one or more micro transactions with respect to a financial account being controlled by the requesting user. The code generator 206 may be configured to generate a code utilizing information derived from the completed one or more micro transactions. As mentioned above, the micro transactions may be one or more small debits and credits to/from a financial account that are identifiable only to the holder of the financial account. The

information derived from the completed micro transactions may include, but not limited to, the username associated with the financial account (e.g., where the user's financial account is associated with an online payment service), bank account type, bank account number, the amount involved in the micro transaction, the type and/or format of the requested digital good, the name of the requested song, etc.

[0026] The embedding module 208 may be configured to embed the code generated utilizing information derived from the completed one or more micro transactions into a copy of the digital good. Thus generated code is suitable for confirming the user's ownership of the digital good. In one embodiment, the system 200 comprises an authentication module (not shown) that may be configured to obtain a user-supplied code associated with a request permit playback of a copy of a digital good on a client device (a DRM code embedded into the digital good), compare the user-supplied code to the code derived from the one or more micro transactions at the time when a request to purchase the digital good was made, and selectively permit playback of the copy of the digital good on the client device based on a result of the comparing.

[0027] The system 200 may also include a recovery module 210, which may be configured to process a request from a user who wishes to reacquire a previously-purchased digital good. In one embodiment, the recovery module 210 may provide an instruction to the requestor to effectuate one or more micro transactions that match the one or more completed micro transactions that occurred when the user first purchased the digital good. If the recovery module 210 determines that the user was able to perform one or more micro transactions that match the one or more completed micro transactions that occurred when the user first purchased the digital good, the code generator 206 may be instructed to recreate the code utilizing information derived from the one or more micro transactions, and the embedding module 208 may be instructed to embed the recreated code into a copy of the digital good. As a result, the user may be provided with a copy of the previously-purchased digital good that contains the recreated code that can be used to confirm ownership of the digital good. An

example method to generate a code that can be used to confirm ownership of digital goods can be described with reference to Fig. 3.

[0028] Fig. 3 is a flow chart of a method 300 to generate a code that can be used to confirm ownership of digital goods, according to one example embodiment. The method 300 may be performed by processing logic that may comprise hardware (e.g., dedicated logic, programmable logic, microcode, etc.), software (such as run on a general purpose computer system or a dedicated machine), or a combination of both. In one example embodiment, the processing logic resides at the payment processing computer system 110 of Fig. 1 and, specifically, at the system to generate code suitable to confirm ownership of digital goods shown in Fig. 2.

[0029] As shown in Fig. 3, the method 300 commences at operation 310, when the communications module 202 of Fig. 2 receives, from a client device via a data network interface, a request for a digital good. The transaction module 204, at operation 320, completes one or more micro transactions with respect to a financial account of the requesting user. Information identifying the user's financial account may be provided by the user together with the request to purchase a digital good. The identifying information may be, e.g., the account number, or the user's email address where the account is associated with an on-line payment service.

[0030] At operation 330, the code generator 306 generates a code utilizing information derived from the one or more micro transactions. As mentioned above, the micro transactions may be one or more small debits and credits to/from a financial account that are identifiable only to the holder of the financial account. The information derived from the completed micro transactions may include, but not limited to, the username associated with the financial account (e.g., where the user's financial account is associated with an online payment service), bank account type, bank account number, the amount involved in the micro transaction, the type and/or format of the requested digital good, the name of the requested song, etc. At operation 340, the embedding module 308 embeds the code generates, using information derived from the one

or more micro transactions, into a copy of the digital good. The purchased digital good can be then transmitted directly to the user or to the computer system controlled by the producer of the digital good so that the producer of the digital good makes the copy of the digital good with embedded code available to the user (e.g., to the purchaser or to another user designated by the purchaser). An example method to recover a code that can be used to confirm ownership of digital goods can be described with reference to Fig. 4.

[0031] Fig. 4 is a flow chart of a method 400 to recover ownership of a digital good, according to one example embodiment. The method 400 may be performed by processing logic that may comprise hardware (e.g., dedicated logic, programmable logic, microcode, etc.), software (such as run on a general purpose computer system or a dedicated machine), or a combination of both. In one example embodiment, the processing logic resides at the payment processing computer system 110 of Fig. 1 and, specifically, at the system to generate code suitable to confirm ownership of digital goods shown in Fig. 2.

[0032] As shown in Fig. 4, the method 400 commences at operation 410, when the communications module 202 of Fig. 2 receives a request from a user indication that the user wishes to reacquire previously-purchased digital good, which causes the recovery module 210 to provide an instruction to the requestor to effectuate one or more micro transactions that match the one or more completed micro transactions that occurred when the user first purchased the digital good. At operation 420 the recovery module 210 determines whether the user was able to perform one or more micro transactions that match the one or more completed micro transactions that occurred when the user first purchased the digital good. At operation 430, the code generator 206 recreates the code utilizing information derived from the one or more micro transactions. The embedding module 208 embeds the recreated code into a new copy of the digital good at operation 440. As a result, the user may be provided with this new copy of the previously-purchased digital good that contains the recreated code and that can be used to confirm ownership of the digital good.

[0033] Fig. 5 shows a diagrammatic representation of a machine in the

example form of a computer system 500 within which a set of instructions, for causing the machine to perform any one or more of the methodologies discussed herein, may be executed. In alternative embodiments, the machine operates as a stand-alone device or may be connected (e.g., networked) to other machines. In a networked deployment, the machine may operate in the capacity of a server or a client machine in a server-client network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The machine may be a personal computer (PC), a tablet PC, a set-top box (STB), a Personal Digital Assistant (PDA), a cellular telephone, a web appliance, a network router, switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

[0034] The example computer system 500 includes a processor 502 (e.g., a central processing unit (CPU), a graphics processing unit (GPU) or both), a main memory 504 and a static memory 506, which communicate with each other via a bus 505. The computer system 500 may further include a video display unit 510 (e.g., a liquid crystal display (LCD) or a cathode ray tube (CRT)). The computer system 500 also includes an alpha-numeric input device 512 (e.g., a keyboard), a user interface (UI) navigation device 514 (e.g., a cursor control device), a disk drive unit 516, a signal generation device 518 (e.g., a speaker) and a network interface device 520.

[0035] The disk drive unit 516 includes a machine-readable medium 522 on which is stored one or more sets of instructions and data structures (e.g., software 524) embodying or utilized by any one or more of the methodologies or functions described herein. The software 524 may also reside, completely or at least partially, within the main memory 504 and/or within the processor 502 during execution thereof by the computer system 500, with the main memory 504 and the processor 502 also constituting machine-readable media.

[0036] The software 524 may further be transmitted or received over a network 526 via the network interface device 520 utilizing any one of a number of well-known transfer protocols (e.g., Hyper Text Transfer Protocol (HTTP)).

[0037] While the machine-readable medium 522 is shown in an example embodiment to be a single medium, the term "machine-readable medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The term "machine-readable medium" shall also be taken to include any medium that is capable of storing and encoding a set of instructions for execution by the machine and that cause the machine to perform any one or more of the methodologies of embodiments of the present invention, or that is capable of storing and encoding data structures utilized by or associated with such a set of instructions. The term "machine-readable medium" shall accordingly be taken to include, but not be limited to, solid-state memories, optical and magnetic media. Such media may also include, without limitation, hard disks, floppy disks, flash memory cards, digital video disks, random access memory (RAMs), read only memory (ROMs), and the like.

[0038] The embodiments described herein may be implemented in an operating environment comprising software installed on a computer, in hardware, or in a combination of software and hardware. Such embodiments of the inventive subject matter may be referred to herein, individually or collectively, by the term "invention" merely for convenience and without intending to voluntarily limit the scope of this application to any single invention or inventive concept if more than one is, in fact, disclosed.

[0039] Thus, a method and system to confirm ownership of digital goods has been described. Although embodiments have been described with reference to specific example embodiments, it will be evident that various modifications and changes may be made to these embodiments without departing from the broader spirit and scope of the inventive subject matter. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a

restrictive sense.

CLAIMS

1. A computer-implemented system comprising:

receiving, from a client device via a data network interface, a request for a digital good;

completing one or more micro transactions with respect to a financial account;

generating a code utilizing information derived from the one or more micro transactions;

embedding the code into a first copy of the digital good, the code to be used to confirm ownership of the digital good.

2. The method of claim 1, comprising transmitting the first copy of the digital good with the embedded code to a third party computer system.

3. The method of claim 1, comprising providing the first copy of the digital good with the embedded code to the client device.

4. The method of claim 3, comprising:

obtaining a user-supplied code;

comparing the user-supplied code to the code generated utilizing information derived from the one or more micro transactions; and

selectively permitting playback of the first copy of the digital good on the client device based on a result of the comparing.

5. The method of claim 1, wherein the receiving of the request for the digital good comprises receiving a request to purchase the digital good.

6. The method of claim 1, wherein the receiving of the request for the digital good comprises receiving a request to reacquire the digital good.

7. The method of claim 6, comprising:

in response to the request from a requestor to reacquire the digital good, providing an instruction to the requestor to effectuate subsequent one or more micro transactions that match the one or more completed micro transactions with respect to the financial account;

determining that the subsequent one or more micro transactions match the one or more completed micro transactions with respect to the financial account;

responsive to the determining, recreating the code utilizing information derived from the one or more micro transactions; and

embedding the recreated code into a further copy of the digital good, the recreated code to be used to confirm ownership of the digital good.

8. The method of claim 1, wherein the one or more micro transactions comprise a deposit transaction.

9. The method of claim 1, wherein the one or more micro transactions comprise a withdrawal transaction.

10. The method of claim 1, wherein the generating of the code utilizing information derived from the one or more micro transactions comprises utilizing one or more information items from a list consisting of a transaction amount, a user name associated with the financial account, a type of the financial account, and a type of the digital good.

11. A computer-implemented system comprising:

a communications module to receive, from a client device via a data network interface, a request for a digital good;

a transaction module to complete one or more micro transactions with respect to a financial account;

a code generator to generate a code utilizing information derived from the one or more micro transactions;

embedding module to embed the code into a first copy of the digital good, the code to be used to confirm ownership of the digital good.

12. The system of claim 11, wherein the communications module is to transmit the first copy of the digital good with the embedded code to a third party computer system.

13. The system of claim 11, wherein the communications module is to transmit the first copy of the digital good with the embedded code to the client device.

14. The system of claim 13, comprising an authentication module to:

obtain a user-supplied code;

compare the user-supplied code to the code generated utilizing information derived from the one or more micro transactions; and

selectively permit playback of the first copy of the digital good on the client device based on a result of the comparing.

15. The system of claim 11, wherein the request for the digital good is a request to purchase the digital good.

16. The system of claim 11, wherein the request for the digital good is a request to reacquire the digital good.

17. The system of claim 16, comprising a recovery module to:

in response to the request from a requestor to reacquire the digital good, provide an instruction to the requestor to effectuate subsequent one or more micro transactions that match the one or more completed micro transactions with respect to the financial account;

determine that the subsequent one or more micro transactions match the one or more completed micro transactions with respect to the financial account, wherein:

the code generator is to recreate the code utilizing information derived from the one or more micro transactions, and

the embedding module is to embed the recreated code into a further copy of the digital good, the recreated code to be used to confirm ownership of the digital good.

18. The system of claim 11, wherein the one or more micro transactions comprise one or more of a deposit transaction and a withdrawal transaction.

19. The system of claim 11, wherein the code generator is to utilize one or more information items from a list consisting of a transaction amount, a user name associated with the financial account, a type of the financial account, and a type of the digital good.

20. A machine-readable non-transitory medium having instruction data to cause a machine to:

receive, from a client device via a data network interface, a request for a digital good;

complete one or more micro transactions with respect to a financial account;

generate a code utilizing information derived from the one or more micro transactions;

embed the code into a first copy of the digital good, the code to be used to confirm ownership of the digital good.

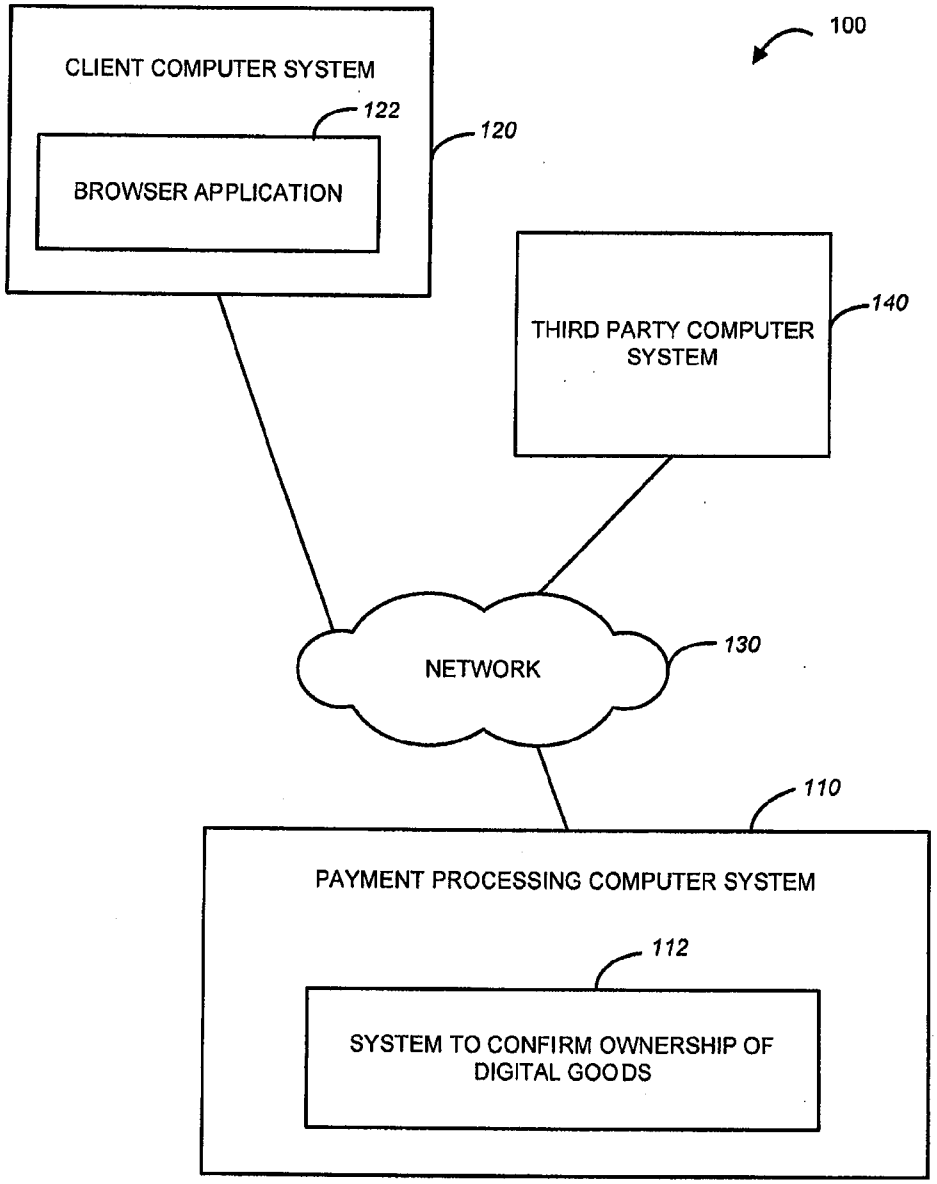
100
CLIENT COMPUTER SYSTEM
122
120
BROWSER APPLICATION
THIRD PARTY COMPUTER SYSTEM
140
NETWORK
130
110
PAYMENT PROCESSING COMPUTER SYSTEM
112
SYSTEM TO CONFIRM OWNERSHIP OF DIGITAL GOODS

FIG. 1

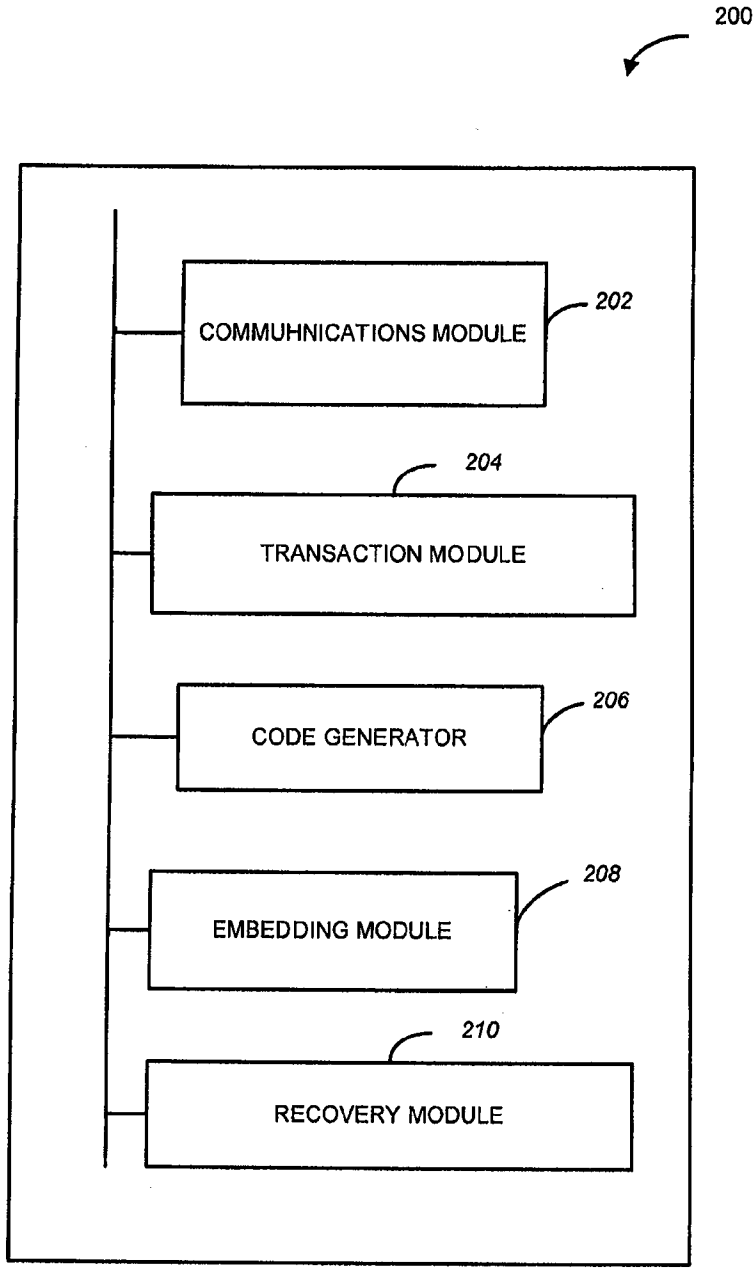
200
COMMUHNICATIONS MODULE
202
204
TRANSACTION MODULE
CODE GENERATOR
206
EMBEDDING MODULE
208
210
RECOVERY MODULE

FIG. 2

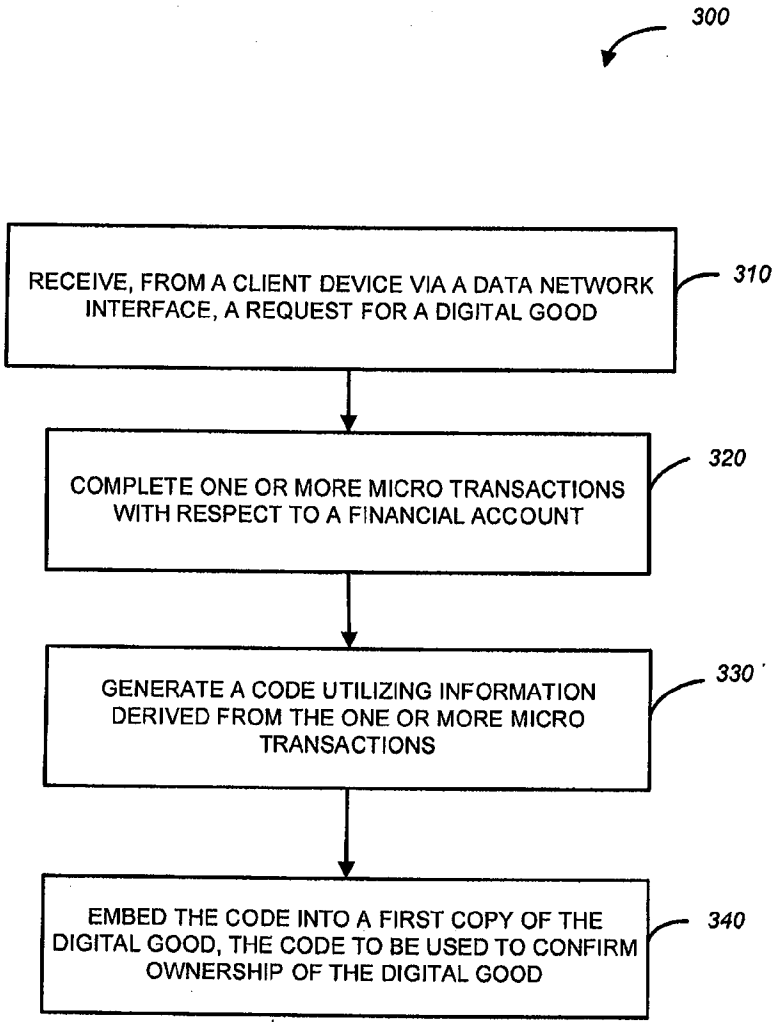
300
RECEIVE, FROM A CLIENT DEVICE VIA A DATA NETWORK INTERFACE, A REQUEST FOR A DIGITAL GOOD
310
COMPLETE ONE OR MORE MICRO TRANSACTIONS WITH RESPECT TO A FINANCIAL ACCOUNT
320
GENERATE A CODE UTILIZING INFORMATION DERIVED FROM THE ONE OR MORE MICRO TRANSACTIONS
330
EMBED THE CODE INTO A FIRST COPY OF THE DIGITAL GOOD, THE CODE TO BE USED TO CONFIRM OWNERSHIP OF THE DIGITAL GOOD
340

FIG. 3

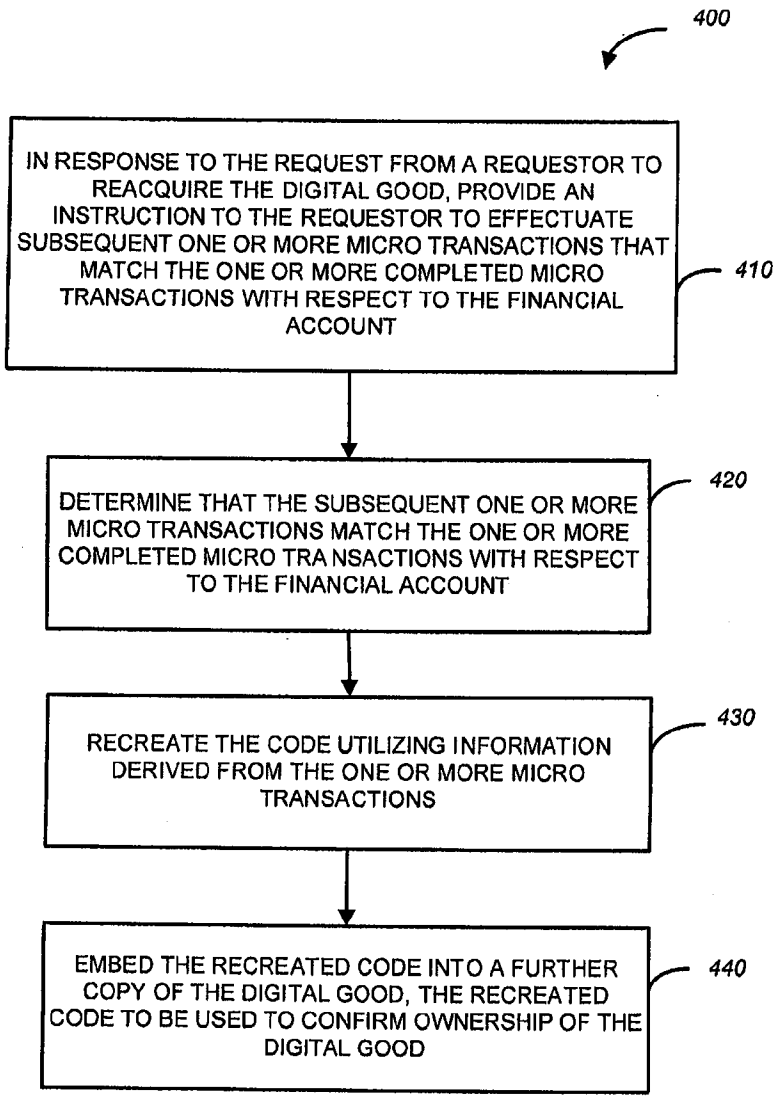
400
IN RESPONSE TO THE REQUEST FROM A REQUESTOR TO REACQUIRE THE DIGITAL GOOD, PROVIDE AN INSTRUCTION TO THE REQUESTOR TO EFFECTUATE SUBSEQUENT ONE OR MORE MICRO TRANSACTIONS THAT MATCH THE ONE OR MORE COMPLETED MICRO TRANSACTIONS WITH RESPECT TO THE FINANCIAL ACCOUNT
410
DETERMINE THAT THE SUBSEQUENT ONE OR MORE MICRO TRANSACTIONS MATCH THE ONE OR MORE COMPLETED MICRO TRA NSACTIONS WITH RESPECT TO THE FINANCIAL ACCOUNT
420
RECREATE THE CODE UTILIZING INFORMATION DERIVED FROM THE ONE OR MORE MICRO TRANSACTIONS
430
EMBED THE RECREATED CODE INTO A FURTHER COPY OF THE DIGITAL GOOD, THE RECREATED CODE TO BE USED TO CONFIRM OWNERSHIP OF THE DIGITAL GOOD
440

FIG. 4

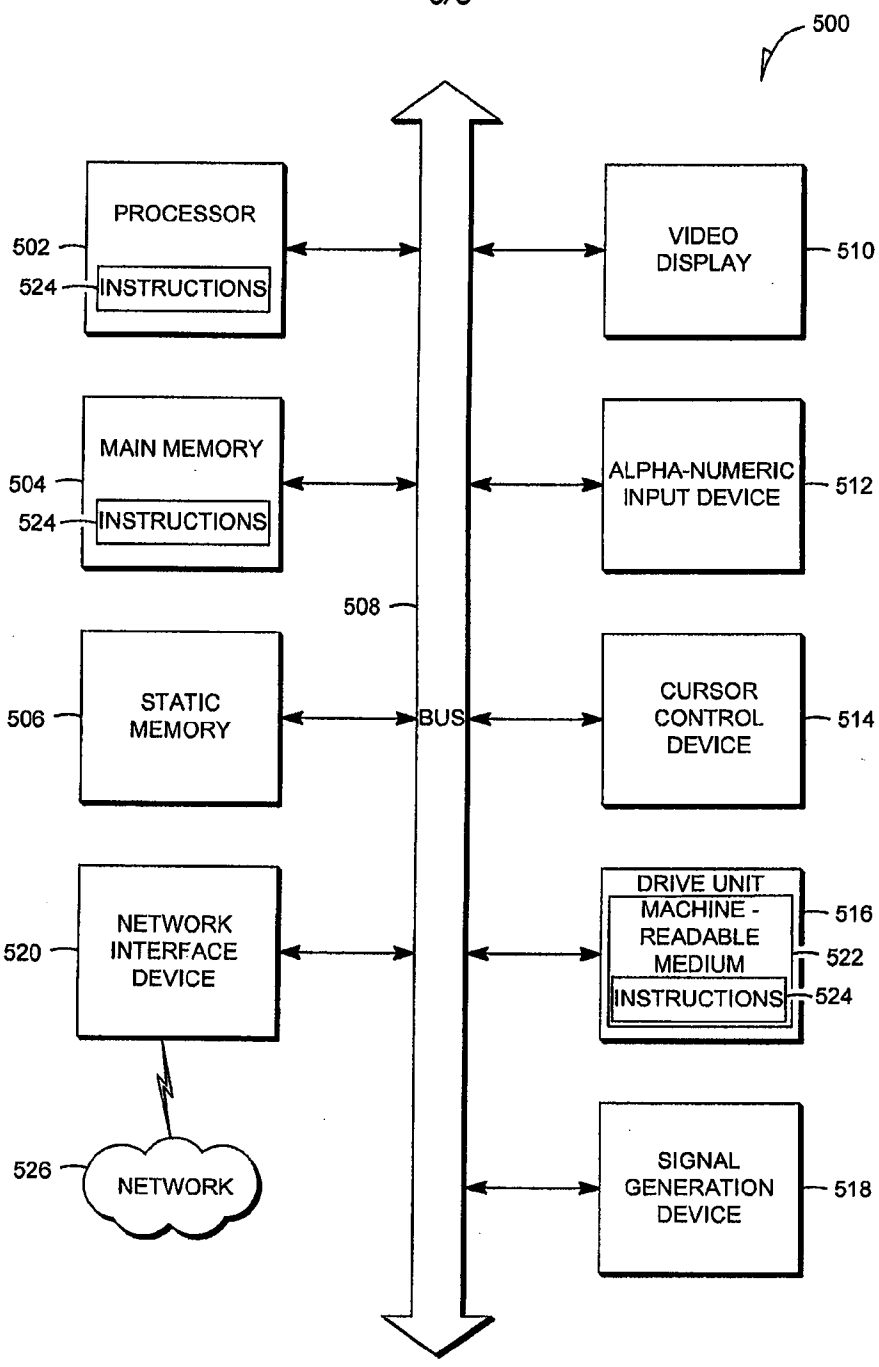
500
PROCESSOR
502
INSTRUCTIONS
524
MAIN MEMORY
504
INSTRUCTIONS
524
508
STATIC MEMORY
506
BUS
NETWORK INTERFACE DEVICE
520
526
NETWORK
VIDEO DISPLAY
510
ALPHA-NUMERIC INPUT DEVICE
512
CURSOR CONTROL DEVICE
514
DRIVE UNIT
MACHINE - READABLE MEDIUM
516
522
INSTRUCTIONS
524
SIGNAL GENERATION DEVICE
518

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US12/30179

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **G06Q 30/00**(2012.01)

USPC: 705/026.100
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/026.100

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2005/0289081 A1 (SPORNY) 29 December 2005 (29.12.2005)	1,3,8-11,13,15 and 18-20 --- 2,4,6-7,12,14 and 16-17
Y	US 2004/0127277 A1 (WALKER et al) 01 July 2004 (01.07.2004)	4, 14
Y	US 2008/0022086 A1 (HO et al) 24 January 2008 (24.01.2008)	6-7 and 16-17
A	US 2007/0223704 A1 (BRICKELL et al) 27 September 2007 (27.09.2007)	1-20
A	US 2007/0232272 A1 (GONSALVES et al) 04 October 2007 (04.10.2007)	1-20
A	US 2009/0293116 A1 (DeMELLO et al) 26 November 2009 (26.11.2009)	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 April 2012 (10.04.2012)	13 APR 2012
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Teri Luu Telephone No. 571-272-7045

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT	International application No. PCT/US12/30179

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of any additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.