

TRANSACTION PROCESSING USING UNIQUE MESSAGING

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] None.

BACKGROUND

5 **[0002]** Receivers of value such as resource providers prefer to immediately receive funds for transactions that they conduct. However, traditional methods for processing transactions can be slow, sometimes taking days for receivers to receive funds for their transactions. A traditional pull transaction involves a receiver transmitting an authorization request message for a transaction to an acquirer institution. The acquirer institution transmits the authorization request message to an issuer institution, which approves of the authorization request message. A clearing and settlement process can occur between the acquirer institution and the issuer institution one or more days later. The receiver receives the funds during the settlement process.

15 **[0003]** Some methods can allow receivers to receive funds quickly using a pull message such as an AFT (account funding transaction) message, a push message such as an OCT (original credit transaction) message, and an intermediate account held by an entity such as a service provider institution (e.g., a service provider bank). The use of the intermediate account and the service provider institution adds a layer of complexity to fast funds transfer processing, and also requires additional computational resources.

[0004] Embodiments of the disclosure address these and other problems, individually and collectively.

SUMMARY

25 **[0005]** One embodiment of the invention is related to a method comprising: receiving, by an acceptance server computer from a user device, a sender account identifier; generating, by the acceptance server computer, an authorization request

message comprising a primary account identifier data field comprising the sender account identifier, an amount data field comprising a value, and an additional data field comprising a receiver account identifier, wherein the additional data field is associated with an acquiring institution; transmitting, by the acceptance server computer to a first
5 authorizing entity computer associated with the sender account identifier via a processing network computer, the authorization request message; in response to transmitting the authorization request message, receiving, by the acceptance server computer from the first authorizing entity computer, an authorization response message; and in response to receiving the authorization response message,
10 transmitting, by the acceptance server computer to a second authorizing entity computer associated with the receiver account identifier, an advice message comprising the receiver account identifier and the value.

[0006] Another embodiment of the invention includes an acceptance server computer comprising: a processor; and a computer readable medium comprising
15 code, executable by the processor for implementing a method comprising: receiving, from a user device, a sender account identifier; generating an authorization request message comprising a primary account identifier data field comprising the sender account identifier, an amount data field comprising a value, and an additional data field comprising a receiver account identifier, wherein the additional data field is associated
20 with an acquiring institution; transmitting, to a first authorizing entity computer associated with the sender account identifier via a processing network computer, the authorization request message; in response to transmitting the authorization request message, receiving, from the first authorizing entity computer, an authorization response message; and in response to receiving the authorization response message,
25 transmitting, to a second authorizing entity computer associated with the receiver account identifier, an advice message comprising the receiver account identifier and the value.

[0007] Another embodiment of the invention includes a method comprising: receiving, by a processing network computer from an acceptance server computer, an
30 authorization request message comprising a primary account identifier data field comprising a sender account identifier, an amount data field comprising a value, and an additional data field comprising a receiver account identifier, wherein the additional

data field is associated with an acquiring institution; transmitting, by the processing network computer to a first authorizing entity computer associated with the sender account identifier, the authorization request message; and facilitating, by the processing network computer, a transfer of funds associated with the value from the first authorizing entity computer associated with the sender account identifier to a second authorizing entity computer associated with the receiver account identifier.

[0008] Another embodiment of the invention includes a processing network computer comprising: a processor; and a computer readable medium couled to the processor, the computer readable medium comprising code, executable by the processor, for performing a method comprising: receiving, from an acceptance server computer, an authorization request message comprising a primary account identifier data field comprising a sender account identifier, an amount data field comprising a value, and an additional data field comprising a receiver account identifier, wherein the additional data field is associated with an acquiring institution; transmitting, to a first authorizing entity computer associated with the sender account identifier, the authorization request message; and facilitating a transfer of funds associated with the value from the first authorizing entity computer associated with the sender account identifier to a second authorizing entity computer associated with the receiver account identifier.

[0009] Further details regarding embodiments of the disclosure can be found in the Detailed Description and the Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

- [0010]** FIG. 1 shows a block diagram of a system for processing a transaction according to some embodiments, and an overlaid process flow.
- [0011]** FIG. 2 shows exemplary authorization request message data fields.
- [0012]** FIG. 3 shows a block diagram of an exemplary acceptance server computer.
- [0013]** FIG. 4 shows a block diagram of an exemplary processing network computer.

[0014] FIG. 5 shows a block diagram of an exemplary user device.

TERMS

[0015] Prior to discussing embodiments of the disclosure, some terms can be described in further detail.

5 **[0016]** A “user” may include an individual. In some embodiments, a user may be associated with one or more personal accounts and/or mobile devices. The user may also be referred to as a cardholder, account holder, or consumer in some embodiments.

[0017] A “user device” may be a device that is operated by a user. Examples
10 of user devices may include a mobile phone, a smart phone, a card, a personal digital assistant (PDA), a laptop computer, a desktop computer, a server computer, a vehicle such as an automobile, a thin client device, a tablet PC, etc. Additionally, user devices may be any type of wearable technology device, such as a watch, earpiece, glasses, etc. The user device may include one or more processors capable of processing user
15 input. The user device may also include one or more input sensors for receiving user input. As is known in the art, there are a variety of input sensors capable of detecting user input, such as accelerometers, cameras, microphones, etc. The user input obtained by the input sensors may be from a variety of data input types, including, but not limited to, audio data, visual data, or biometric data. The user device may
20 comprise any electronic device that may be operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or
25 a private network.

[0018] A “resource provider” may be an entity that can provide a resource such as goods, services, information, and/or access. Examples of resource providers includes merchants, data providers, transit agencies, governmental entities, venue and dwelling operators, etc. A “merchant” may typically be an entity that engages in
30 transactions and can sell goods or services, or provide access to goods or services.

[0019] An “acquirer” may typically be a business entity (e.g., a commercial bank) that has a business relationship with a particular merchant or other entity. Some entities can perform both issuer and acquirer functions. Some embodiments may encompass such single entity issuer-acquirers. An acquirer may operate an acquirer computer, which can also be generically referred to as a “transport computer.”

[0020] A “server computer” may include a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers.

[0021] A “processing network” may include data processing subsystems, networks, and operations. In embodiments of the invention, a processing network may be used to support and deliver authorization services, exception file services, and clearing and settlement services. A processing network may be a payment processing network able to transmit and receive financial system transaction messages (e.g., ISO 8583 messages), and process original credit and debit card transactions. An exemplary payment processing system may include VisaNet™. Payment processing systems such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions.

[0022] An “authorization request message” may be an electronic message that requests authorization for an interaction. In some embodiments, it is sent to a transaction processing computer and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with International Organization for Standardization (ISO) 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a user using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to

“identification information” including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), a PAN (primary account number or “account number”), a payment token, a user name, an expiration date, etc. An authorization request message may also comprise “transaction information,” such as any information associated with a current transaction, such as the transaction value, merchant identifier, merchant location, acquirer bank identification number (BIN), card acceptor ID, information identifying items being purchased, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

10 **[0023]** An “authorization response message” may be a message that responds to an authorization request. In some cases, it may be an electronic message reply to an authorization request message generated by an issuing financial institution or a transaction processing computer. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval --
15 transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either
20 directly or through the transaction processing computer) to the merchant's access device (e.g., POS equipment) that indicates approval of the transaction. The code may serve as proof of authorization.

[0024] An “authorizing entity” may be an entity that authorizes a request. Examples of an authorizing entity may be an issuer, a governmental agency, a
25 document repository, an access administrator, etc. An authorizing entity may operate an authorizing entity computer. An “issuer” may refer to a business entity (e.g., a bank) that issues and optionally maintains an account for a user. An issuer may also issue payment credentials stored on a user device, such as a cellular telephone, smart card, tablet, or laptop to the consumer, or in some embodiments, a portable device.

30 **[0025]** A “clearing and settlement process” may include a process of reconciling a transaction. A clearing process is a process of exchanging financial details between

an acquirer and an issuer to facilitate posting to a party's account and reconciliation of the party's settlement position. Settlement involves the delivery of funds from one party to another.

[0026] An "account identifier" may include an identifier for an account. An account identifier may include a primary account number (PAN) issued by an issuer for a card account (e.g., credit card, debit card, etc.). For instance, in some embodiments, a primary account number may include a sixteen digit numerical value such as "4147 0900 0000 1234." The first six digits of the real account identifier (e.g., "414709"), may represent a real issuer identifier (BIN) that may identify an issuer associated with the primary account number.

[0027] A "processor" may include a device that processes something. In some embodiments, a processor can include any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to accomplish a desired function. The processor may include a CPU comprising at least one high-speed data processor adequate to execute program components for executing user and/or system-generated requests. The CPU may be a microprocessor such as AMD's Athlon, Duron and/or Opteron; IBM and/or Motorola's PowerPC; IBM's and Sony's Cell processor; Intel's Celeron, Itanium, Pentium, Xeon, and/or XScale; and/or the like processor(s).

[0028] A "memory" may be any suitable device or devices that can store electronic data. A suitable memory may comprise a non-transitory computer readable medium that stores instructions that can be executed by a processor to implement a desired method. Examples of memories may comprise one or more memory chips, disk drives, etc. Such memories may operate using any suitable electrical, optical, and/or magnetic mode of operation.

DETAILED DESCRIPTION

[0029] An existing method for rapidly delivering funds from a sender to a receiver may use an account funding transaction (AFT) message and an original credit transaction (OCT) message. The AFT message is used to transfer funds from a sender account at a sender authorizing entity (e.g., a sender issuer) to an intermediate

account, often held by an intermediate service provider such as an intermediate financial institution (e.g., a service provider bank). The AFT message causes the sender authorizing entity to debit the sender's account for an amount. The intermediate service provider can then initiate the sending of an OCT message to a receiver authorizing entity computer associated with the receiver's account. The OCT message causes the receiver's authorizing entity to credit the account of the receiver, thereby resulting in a funds transfer from the sender to the receiver.

[0030] The amount of the debit is the amount of the credit to be delivered to the recipient plus any fees being charged by the service provider such as a transfer fee, or a currency conversion fee. In some instances, an AFT indicator is used in both the authorization and clearing and settlement transactions and is preceded by an authorization. Settlement takes place within two working days. Neither the authorization nor the clearing transaction carries any financial information about the recipient of a money transfer. The AFT carries only the account number associated with the account of the sender. An AFT is also accompanied by indicators, which allow the sender's card issuing bank to take appropriate authorization decisions. Indicators include channel information such as Mail Order/Telephone Order or Internet, and merchant type. A financial services association (such as Visa) performs currency conversion on AFT transactions when the currency of the sender is different from the currency accepted by the service provider. AFT indicators are used to show funds transfers instead of standard purchase transactions. The following fields can be used for an AFT: Processing Code; Merchant Type; CAVV Result Code; Mail Order/Telephone Order/Electronic Commerce Indicator; Mail/Phone/Electronic Commerce Indicator; Transaction ID (XID); and CAVV Data.

[0031] An OCT (Original Credit Transaction) is typically a clearing and settlement credit transaction designed for use in business applications such as a business money transfer or business-to-consumer repayments. When used in the context of money transfer, the OCT is the transaction used to deliver funds to the recipient account. It is typically separate from, and takes place after, the AFT transaction. This timing is to ensure that payment funds are secured before funds are sent to the recipient.

[0032] The amount of the OCT is the amount agreed by the sender and the service provider in the currency agreed. If the recipient's billing currency is different from the currency agreed at the transaction time, currency conversion is performed on the OCT and the exact amount credited to the recipient account will not be known at transaction time. The OCT carries only the account number of the recipient and no information about the sender. A special indicator identifies an OCT to the recipient's issuer bank.

[0033] A drawback to the traditional method above is that AFT messaging may require specialized computers or programming. As a result, it may only work with select authorizing entities or service providers as not all entities may have systems capable of processing AFT messages. Further, some authorizing entities may be required to complete an onboarding process with the intermediate service provider before AFT messaging can be used. This also restricts the ability of the traditional fast transfer methods. Still further, the additional messaging to and from the intermediate service provider and the account maintained by the intermediate service provider results in a larger number of messages and computations to process transactions. The larger number of messages and computations results in a need for increased computational resources and also results in increased amounts of computation time.

[0034] Embodiments of the invention introduce a transaction processing method that enables the fast or immediate transfer of funds from a sender to a receiver, without the requirement of an intermediate service provider or intermediate account. Further, existing transmission protocols associated with more ubiquitous financial transaction messages such as ISO 8583, 0200 financial messages, can be used instead of AFT messages. Embodiments of the invention can allow for the fast transfer of funds while using an existing infrastructure that is widely used for convention "pull" transactions. Receivers such as resource providers can quickly receive funds from senders, without the need to onboard with an acquirer. Moreover, embodiments are interoperable because they do not require authorizing entities to onboard with an intermediate service provider and do not require that they make significant modifications to their systems.

[0035] FIG. 1 shows a block diagram of a transaction processing system and an overlaid process flow according to some embodiments. The transaction may involve a sender sending funds (e.g, a payment) to a receiver (e.g., a resource provider such as a merchant) in exchange for access to a resource such as an item. FIG. 1 shows a sender portable device 103 interacting with a receiver user device 102 to initiate a transaction. The receiver user device 102 comprises an acceptance application 102A which enables the receiver to conduct transactions using a receiver account. The acceptance application 102A may also enable the receiver user device 102 to communicate with a second authorizing entity computer 110 that manages the receiver account, and an acceptance server computer 106. FIG. 1 also shows a processing network computer 108 in operable communication with the acceptance server computer 106, the second authorizing entity computer 110, and a first authorizing entity computer 112.

[0036] The first authorizing entity computer 112 (e.g., a first issuer bank computer) may issue the sender portable device 103 to the sender user, and manage a sender account associated with the sender portable device 103 on behalf of the sender user. Similarly, the second authorizing entity computer 110 may issue a receiver portable device (not shown) to the receiver user and manage a receiver account for the receiver. In some embodiments, the sender portable device 103 and the receiver portable device may be payment cards such as debit cards.

[0037] An advantage the transaction processing system shown in FIG. 1 over some existing transaction processing systems is that the system in FIG. 1 does not require an acquiring institution computer associated with an acquirer and does not require an intermediate service provider computer associated with an intermediate service provider that manages an intermediate account. The receiver operating the receiver user device 102 does not have to be onboarded with an acquirer before the receiver can receive payments from the sender.

[0038] For simplicity of illustration, a certain number of components are shown in FIG. 1. It is understood, however, that embodiments of the invention may include more than one of each component. In addition, some embodiments of the invention may include fewer than or greater than all of the components shown in FIG. 1.

[0039] Messages between at least the devices of the system in FIG. 1 can be transmitted using a secure communications protocols such as, but not limited to, File Transfer Protocol (FTP); HyperText Transfer Protocol (HTTP); Secure Hypertext Transfer Protocol (HTTPS), SSL, ISO (e.g., ISO 8583) and/or the like. The communications network may include any one and/or the combination of the following: a direct interconnection; the Internet; a Local Area Network (LAN); a Metropolitan Area Network (MAN); an Operating Missions as Nodes on the Internet (OMNI); a secured custom connection; a Wide Area Network (WAN); a wireless network (e.g., employing protocols such as, but not limited to a Wireless Application Protocol (WAP), I-mode, and/or the like); and/or the like. The communications network can use any suitable communications protocol to generate one or more secure communication channels. A communications channel may, in some instances, comprise a secure communication channel, which may be established in any known manner, such as through the use of mutual authentication and a session key, and establishment of a Secure Socket Layer (SSL) session.

[0040] The acceptance application 102A can be an application which can communicate with the acceptance server computer 106. For example, the acceptance application 102A may be a wallet application, an issuer application (e.g., a banking application) or resource provider application on the receiver user device 102 that uses an SDK (software development kit) to communicate with the acceptance server computer 106. The acceptance application 102A may use the SDK to obtain and transmit transaction details to the acceptance server computer 106.

[0041] The acceptance server computer 106 can be programmed to generate authorization request messages using the transaction details and transmit the authorization requests to the processing network computer 108. The processing network computer 108 can be programmed to receive authorization request messages from the acceptance server computer 106 and route them to the first authorizing entity computer 112 for approval. The processing network computer 108 may also be programmed to settle transactions (e.g., between the first authorizing entity computer 112 and second authorizing entity computer 110).

[0042] Prior to step S2, the receiver can provide a receiver account identifier such as a PAN (a primary account number) to the acceptance application 102A. The receiver account identifier (e.g., a receiver's PAN) can include a second authorizing entity computer identifier (e.g., a BIN or bank identification number associated with a second authorizing entity). The receiver can enter the receiver account identifier into the acceptance application 102A by manual data entry, by interacting a receiver portable device (a debit card of the receiver) storing the receiver account identifier (e.g., a receiver debit card number), or by downloading it from the second authorizing entity computer 110.

10 **[0043]** At step S2, the acceptance application 102A on the receiver user device 102 obtains a sender credential from the sender portable device 103 (e.g., via NFC). For example, the receiver may request payment from the sender in exchange for access to a resource or good. The receiver can input a value for the transaction (e.g., a transaction amount) to the acceptance application 102A and prompt the sender user
15 to provide payment via a contactless interaction such as an NFC (near field communication) interaction). The sender user can tap the sender portable device 103 (e.g., debit card) to the receiver user device 102 (e.g., mobile phone) to transmit the sender account identifier from the sender portable device 103 to the receiver user device 102. The SDK inside the acceptance application 102A can then obtain the
20 sender account identifier.

[0044] At step S4, the acceptance application 102A then transmits the captured sender account identifier, the receiver account identifier, and the amount of the transaction to the acceptance server computer 106. The acceptance application 102A may also transmit an identifier for the acceptance application 102A or the receiver user
25 device 102.

[0045] Account identifiers may comprise authorizing entity computer identifiers. In some embodiments, an account identifier may be a primary account identifier (PAN). It can include a sixteen digit numerical value such as "4147 0900 0000 1234." The first six digits of the account identifier (e.g., "414709"), may represent the
30 authorizing entity computer identifier (e.g., BIN) that may identify the authorizing entity associated with the account identifier. For example, the sender account identifier may

comprise a first authorizing entity computer identifier which represents the first authorizing entity, and the receiver account identifier may comprise a second authorizing entity computer identifier which represents the second authorizing entity.

[0046] At step S6, after receiving the sender account identifier from the acceptance application 102A, the acceptance server computer 106 may generate an authorization request message comprising a number of data fields with values in the data fields. The data fields and the values may include, but it not limited to the following: a primary account identifier data field comprising the sender account identifier, an amount data field comprising a value, and an additional data field comprising a receiver account identifier. The additional data field is associated with an acquiring institution. For example, the additional data field can be an acquiring institution identification code data field or a card acceptor identification data field. An “acceptor” is an entity that has been onboarded with an acquirer and can accept payments using payment cards, where the payments are processed by an acquirer. The authorization request messages may be in an 0200 financial request message format, as opposed to an AFT message format.

[0047] FIG. 2 shows exemplary authorization request message data fields in an 0200 financial request message. The illustrated data fields are examples and there may be many more data fields. The data fields include: a card acceptor identification data field 202, an acquiring institution identification code data field 203, an amount data field 204, a primary account number (PAN) data field 205, a resource provider type data field 206, a settlement date data field 207, a transmission date and time data field 208, a card acceptor terminal identification data field 209, and a transaction ID data field 210. In some embodiments, the settlement date data field 207 comprises a date that is the same as the date in the transmission date in the transmission date and time data field 208. The transmission date and time data field 208 may contain the date and time when the authorization request message was generated and transmitted to an authorizing entity computer for authorization. The card acceptor terminal identification data field 209 typically contains an identifier for a POS (point of sale) terminal at a merchant. However, in embodiments of the invention, an identifier associated with the receiver user device 102 or the acceptance application 102A may be in the card acceptor terminal identification data field 209. The transaction identifier

or ID in the transaction ID data field 210 can be generated by the acceptance server computer 126.

[0048] The acquiring institution identification code data field 203 may traditionally comprise an acquirer identifier associated with an acquirer. The card
5 acceptor identification data field 202 may ordinarily contain an identifier for a resource provider (e.g., a merchant) that has onboarded with an acquirer. However, embodiments of the invention do not use an acquiring institution (e.g., an acquiring bank). Instead, the acquiring institution identification code data field 203 may instead contain the receiver account identifier or the first authorizing entity identifier in the
10 receiver account identifier. The card acceptor identification data field 202 can contain the receiver account identifier. If the acquiring institution identification code data field 203 contains the receiver account identifier, then the card acceptor identification data field 202 can have a null value.

[0049] Referring back to the method of FIG. 1, at step S6, the acceptance server
15 computer 106 can generate the authorization request message by populating the data fields in the authorization request message with the appropriate transaction details. After generating and formatting the authorization request message, the acceptance server computer can transmit it, via the processing network computer 108 to the first authorizing entity computer 112 for approval (as shown in steps S8 and S10). The
20 authorizing entity computer 112 may then make an authorization decision using the transaction details, and transmit the authorization decision back to the acceptance server computer 106 in an authorization response message.

[0050] In some embodiments, during step S6 the acceptance server computer 106 may perform transaction control checks. For example, the acceptance server
25 computer 106 may check the transaction velocity associated with the sender account identifier or the receiver account identifier, and/or an accumulated transaction amount associated with the sender account identifier or the receiver account identifier within a predetermined time period (e.g., a week or a month). The transaction control checks may be used to monitor and reduce risk. In some embodiments, the acceptance
30 application 102A may have domain controls to reduce risk. For example, the

acceptance server computer 106 may only process domestic debit card transactions to reduce risk.

[0051] At step S8, the acceptance server computer 106 can transmit the authorization request message to the processing network computer 108. The processing network computer 108 can determine the network address associated with the first authorizing entity computer 112 using the first authorizing entity identifier in the sender account identifier. It can then route the authorization request message to the first authorizing entity computer 112 as in step S10.

[0052] Upon receiving the authorization request message, the first authorizing entity computer 112 can make an authorization decision. For example, the first authorizing entity computer 112 can approve the transaction and immediately debit the balance of the sender account for the transaction amount (as opposed to placing a hold on the account). Since the expected clearing date in the authorization request message is set to "today/same day," the sender account balance is immediately debited for the transaction amount, instead of being held as a "pending transaction." The transaction is posted in real-time upon approval. However, the funds from the sender account are not transmitted until the next settlement cycle which can occur within the day.

[0053] At step S12, the first authorizing entity computer 112 can then notify the acceptance server computer 106 (e.g., via the processing network computer) of the authorization decision. For example, the first authorizing entity computer 112 may transmit an authorization response message with the authorization decision to the acceptance server computer 106. In some embodiments, the first authorizing entity computer 112 may transmit the authorization response message to the acceptance server computer 106 via the processing network computer 108. For example, the first authorizing entity computer 112 may transmit the authorization response message to the processing network computer 108, and the processing network computer 108 may notify the acceptance server computer 106 of the authorization decision.

[0054] At step S14, after receiving the authorization decision, if the transaction is approved, the acceptance server computer 106 can transmit an advice message to the second authorizing entity computer 110. As an example, the advice message may

be a clearing only OCT message. The advice message may notify the second authorizing entity computer 110 that the transaction was posted to the sender account and the funds are expected in a next settlement cycle. The advice message can thus enable the second authorizing entity computer 110 to post the transaction to the receiver account and immediately credit the receiver account. The receiver user may notice the credit in their receiver account statement balance even before the funds actually arrive to the second authorizing entity computer 110 in the next closest settlement cycle.

[0055] In contrast to a push transaction, (e.g., OCT message), the advice message does not push the funds to the receiver account. Instead, the advice message notifies the second authorizing entity computer 110 that funds will arrive with the next settlement cycle. The advice message can include data including a time and time of transmission, the receiver account identifier, the transaction identifier, and the value for the transaction.

[0056] At step S16, after receiving the advice message from the acceptance server computer 106, the second authorizing entity computer 110 can post the transaction and immediately credit the balance of the receiver account for the value of the transaction. At this point, the receiver can view the newly updated balance and may withdraw funds from their account if they wish to do so.

[0057] At step S18, within a short period of time (e.g., by the end of the day), the processing network computer 108 can facilitate settlement between the first authorizing entity computer 112 and the second authorizing entity computer 110. The funds are transferred from the first authorizing entity computer 112 to the second authorizing entity computer 110, as part of a settlement process between various authorizing entity computers and acquirer computers. The settlement processing can occur using an existing settlement infrastructure. Embodiments of the invention advantageously do not need to utilize an intermediate service provider bank or intermediate holding account to temporarily hold the funds during the transaction.

[0058] FIG. 3 shows a block diagram of acceptance server computer 300. The acceptance server computer 300 may comprise a processor 304 coupled to a memory 302, a network interface 306, and a computer readable medium 308. The computer

readable medium 308 can comprise a communication module 308A, an authorization module 308B, and an advice messaging module 308C.

5 **[0059]** The memory 302 can be used to store data and code. The memory 302 may be coupled to the processor 304 internally or externally (e.g., cloud based data storage), and may comprise any combination of volatile and/or non-volatile memory, such as RAM, DRAM, ROM, flash, or any other suitable memory device. For example, the memory 302 can store account identifiers, authorizing entity identifiers, transaction data, tokens, etc.

10 **[0060]** The computer readable medium 308 can comprise code or software, executable by the processor 304, for receiving, from a user device, a sender account identifier; generating an authorization request message comprising a primary account identifier data field comprising the sender account identifier, an amount data field comprising a value, and an additional data field comprising a receiver account identifier, wherein the additional data field is associated with an acquiring institution;
15 transmitting, to a first authorizing entity computer associated with the sender account identifier via a processing network computer, the authorization request message; in response to transmitting the authorization request message, receiving, from the first authorizing entity computer, an authorization response message; and in response to receiving the authorization response message, transmitting, to a second authorizing
20 entity computer associated with the receiver account identifier, an advice message comprising the receiver account identifier and the value.

25 **[0061]** The communication module 308A may comprise code or software, executable by the processor 304, for communicating with other devices. The communication module 308A may be configured or programmed to perform some or all of the functionality associated with receiving, sending, and generating electronic messages for transmission. The communication module 308A, in conjunction with the processor 304, may receive information from the computer readable medium 308 and generate an electronic message in an appropriate data format in conformance with a transmission protocol so that the message may be sent to one or more entities. The
30 electronic message may then be passed to the network interface 306 for transmission.

[0062] The authorization module 308B may comprise code or software, executable by the processor 304, for generating, formatting, and transmitting authorization request messages as described above.

[0063] The advice messaging module 308C may comprise code executable by the processor 304 for generating and transmitting advice messages as described above.

[0064] The network interface 306 may include an interface that can allow the acceptance server computer 300 to communicate with external computers. The network interface 306 may enable the acceptance server computer 300 to communicate data to and from another device (e.g., user devices, processing network computers, etc.). Some examples of the network interface 306 may include a modem, a physical network interface (such as an Ethernet card or other Network Interface Card (NIC)), a virtual network interface, a communications port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, or the like. The wireless protocols enabled by the network interface 306 may include Wi-Fi™. Data transferred via the network interface 306 may be in the form of signals which may be electrical, electromagnetic, optical, or any other signal capable of being received by the external communications interface (collectively referred to as “electronic signals” or “electronic messages”). These electronic messages that may comprise data or instructions may be provided between the network interface 306 and other devices via a communications path or channel. As noted above, any suitable communication path or channel may be used such as, for instance, a wire or cable, fiber optics, a telephone line, a cellular link, a radio frequency (RF) link, a WAN or LAN network, the Internet, or any other suitable medium.

[0065] FIG. 4 shows a block diagram of a processing network computer 400. The processing network computer 400 can include functionality for facilitating the processing of interactions. The processing network computer 400 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. For example, the processing network computer 400 may comprise a server coupled to a network interface 406 (e.g., by an external communication interface), and

databases of information. The processing network computer 400 may be representative of a transaction processing network. An exemplary transaction processing network may include VisaNet™. Transaction processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services. The processing network computer 400 may use any suitable wired or wireless network, including the Internet.

10 **[0066]** The processing network computer 400 can comprise a processor 404 coupled to a memory 402, a network interface 406, and a computer readable medium 408. The computer readable medium 408 can comprise a settlement module 408A, a communication module 408B, and an authorization module 408C.

[0067] The memory 402 can be used to store data and code. The memory 402
15 may be coupled to the processor 404 internally or externally (e.g., cloud based data storage), and may comprise any combination of volatile and/or non-volatile memory, such as RAM, DRAM, ROM, flash, or any other suitable memory device. For example, the memory 402 can store interaction data, tokens, credentials, etc.

[0068] The computer readable medium 408 can comprise code or software,
20 executable by the processor 404 for causing the processing network computer 400 to perform a method comprising: receiving, by a processing network computer from an acceptance server computer, an authorization request message comprising a primary account identifier data field comprising a sender account identifier, an amount data field comprising a value, and an additional data field comprising a receiver account
25 identifier, wherein the additional data field is associated with an acquiring institution; transmitting, by the processing network computer to a first authorizing entity computer associated with the sender account identifier, the authorization request message; and facilitating, by the processing network computer, a transfer of funds associated with the value from the first authorizing entity computer associated with the sender account
30 identifier to a second authorizing entity computer associated with the receiver account identifier.

[0069] The settlement module 408A may comprise code or software, executable by the processor 404, for facilitating the transfer of funds between authorizing entities. For example, following the purchase of an item or good, code or software in the settlement module 408A may enable the processing network computer
5 400 to handle settlement of transactions. An example of the clearing and settlement module is Base II, which provides clearing, settlement, and other interchange-related services.

[0070] The communication module 408B may comprise code or software, executable by the processor 404, for communicating with other devices. The
10 communication module 408B may be configured or programmed to perform some or all of the functionality associated with receiving, sending, and generating electronic messages for transmission through the processing network computer 108 to or from any of the devices shown in FIG. 1.

[0071] The authorization module 408C may comprise code or software,
15 executable by the processor 404, to enable processing authorization request messages and determining the appropriate destination for the authorization request messages.

[0072] The network interface 406 can be similar to the network interface 306 of FIG. 3 and its description will not be repeated here.

20 **[0073]** FIG. 5 shows a block diagram of a user device 500. User device 500 may include device hardware 504 coupled to a system memory 502.

[0074] Device hardware 504 may include a processor 506, a short range antenna 514, a long range antenna 516, input elements 510, a user interface 508, and output elements 512 (which may be part of the user interface 508). Examples of input
25 elements may include microphones, keypads, touchscreens, sensors, etc. Examples of output elements may include speakers, display screens, and tactile devices. The processor 506 can be implemented as one or more integrated circuits (e.g., one or more single core or multicore microprocessors and/or microcontrollers), and is used to control the operation of user device 500. The processor 506 can execute a variety
30 of programs in response to program code or computer-readable code stored in the

system memory 502, and can maintain multiple concurrently executing programs or processes.

[0075] The long range antenna 516 may include one or more RF transceivers and/or connectors that can be used by user device 500 to communicate with other devices and/or to connect with external networks. The long range antenna 516 may be configured to communicate with a remote base station and a remote cellular or data network, over the air. The short range antenna 509 may be configured to communicate with external entities through a short range communication medium. The short range antenna 509 may comprise a contactless interface that can interact with a contactless interface of another device (e.g., a portable device). Examples of a contactless interface may include one or more radio frequency (RF) transceivers that can send and receive communications using near-field communications (NFC), or other radio frequency or wireless communication protocols. The user interface 508 can include any combination of input and output elements to allow a user to interact with and invoke the functionalities of user device 500.

[0076] The system memory 502 can be implemented using any combination of any number of non-volatile memories (e.g., flash memory) and volatile memories (e.g., DRAM, SRAM), or any other non-transitory storage medium, or a combination thereof media. The system memory 502 may store an acceptance application 502A, a storage application 502B, and an operating system 502C.

[0077] Acceptance application 502A may be any application that can run on user device 500 that can communicate with an acceptance server. The acceptance application 502A may include instructions or code executable by the processor 506 for initiating and conducting a transaction with an external device such a portable device, and for transmitting credentials to an acceptance server. In an exemplary case, acceptance application 502A may be a wallet application with an SDK which enables communication with the acceptance server.

[0078] Although the steps in the flowcharts and process flows described above are illustrated or described in a specific order, it is understood that embodiments of the invention may include methods that have the steps in different orders. In addition, steps may be omitted or added and may still be within embodiments of the invention.

[0079] Any of the software components or functions described in this application may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C, C++, C#, Objective-C, Swift, or scripting language such as Perl or Python using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions or commands on a computer readable medium for storage and/or transmission, suitable media include random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a compact disk (CD) or DVD (digital versatile disk), flash memory, and the like. The computer readable medium may be any combination of such storage or transmission devices.

[0080] Such programs may also be encoded and transmitted using carrier signals adapted for transmission via wired, optical, and/or wireless networks conforming to a variety of protocols, including the Internet. As such, a computer readable medium according to an embodiment of the present invention may be created using a data signal encoded with such programs. Computer readable media encoded with the program code may be packaged with a compatible device or provided separately from other devices (e.g., via Internet download). Any such computer readable medium may reside on or within a single computer product (e.g., a hard drive, a CD, or an entire computer system), and may be present on or within different computer products within a system or network. A computer system may include a monitor, printer, or other suitable display for providing any of the results mentioned herein to a user.

[0081] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0082] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0083] As used herein, the use of "a," "an," or "the" is intended to mean "at least one," unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 receiving, by an acceptance server computer from a user device, a
3 sender account identifier;
4 generating, by the acceptance server computer, an authorization
5 request message comprising a primary account identifier data field comprising
6 the sender account identifier, an amount data field comprising a value, and an
7 additional data field comprising a receiver account identifier, wherein the
8 additional data field is associated with an acquiring institution;
9 transmitting, by the acceptance server computer to a first authorizing
10 entity computer associated with the sender account identifier via a processing
11 network computer, the authorization request message;
12 in response to transmitting the authorization request message,
13 receiving, by the acceptance server computer from the first authorizing entity
14 computer, an authorization response message; and
15 in response to receiving the authorization response message,
16 transmitting, by the acceptance server computer to a second authorizing
17 entity computer associated with the receiver account identifier, an advice
18 message comprising the receiver account identifier and the value.
- 1 2. The method of claim 1 wherein the advice message is an OCT
2 message.
- 1 3. The method of claim 1, wherein the additional data field is an
2 acquiring institution identification code data field or a card acceptor
3 identification data field.
- 1 4. The method of claim 1, wherein the authorization request
2 message further comprises a settlement date data field comprising a date is
3 the same date that the authorization request message is transmitted to the
4 first authorizing entity computer.

1 5. The method of claim 1, wherein the sender account identifier is
2 obtained by the user device from a sender portable device comprising the
3 sender portable device via a contactless interaction.

1 6. The method of claim 5, wherein the contactless interaction is an
2 NFC interaction.

1 7. The method of claim 1, wherein the sender account identifier
2 and the receiver account identifier are card identifiers.

1 8. The method of claim 1, wherein prior to the acceptance server
2 computer receiving the authorization response message, the first authorizing
3 entity computer deducts the value from a sender account managed by the first
4 authorizing entity computer.

1 9. The method of claim 8, wherein after the acceptance server
2 computer transmits the advice message to the second authorizing entity
3 computer, the second authorizing entity computer credits the value to a
4 receiver account associated with the receiver account identifier, the receiver
5 account managed by the second authorizing entity computer.

1 10. The method of claim 9, wherein the method transfers the value
2 from the sender account to the receiver account, without using an
3 intermediate account.

1 11. An acceptance server computer comprising:
2 a processor; and
3 a computer readable medium comprising code, executable by the
4 processor for implementing a method comprising:
5 receiving, from a user device, a sender account identifier;
6 generating an authorization request message comprising a primary
7 account identifier data field comprising the sender account identifier, an
8 amount data field comprising a value, and an additional data field comprising

9 a receiver account identifier, wherein the additional data field is associated
10 with an acquiring institution;
11 transmitting, to a first authorizing entity computer associated with the
12 sender account identifier via a processing network computer, the authorization
13 request message;
14 in response to transmitting the authorization request message,
15 receiving, from the first authorizing entity computer, an authorization response
16 message; and
17 in response to receiving the authorization response message,
18 transmitting, to a second authorizing entity computer associated with the
19 receiver account identifier, an advice message comprising the receiver
20 account identifier and the value.

1 12. The acceptance server computer of claim 11, wherein the
2 advice message is an OCT message.

1 13. The acceptance server computer of claim 11, wherein prior to
2 the acceptance server computer receiving the authorization response
3 message, the first authorizing entity computer deducts the value from a
4 sender account managed by the first authorizing entity computer without
5 placing a hold on the sender account for the value.

1 14. The acceptance server computer of claim 13, wherein after the
2 acceptance server computer transmits the advice message to the second
3 authorizing entity computer, the second authorizing entity computer credits
4 the value to a receiver account associated with the receiver account identifier,
5 the receiver account managed by the second authorizing entity computer.

1 15. The acceptance server computer of claim 14, wherein the
2 method transfers the value from the sender account to the receiver account,
3 without using an intermediate account.

1 16. The acceptance server computer of claim 11, wherein the
2 sender account identifier and the receiver account identifier are card
3 identifiers.

1 17. A method comprising:
2 receiving, by a processing network computer from an acceptance
3 server computer, an authorization request message comprising a primary
4 account identifier data field comprising a sender account identifier, an amount
5 data field comprising a value, and an additional data field comprising a
6 receiver account identifier, wherein the additional data field is associated with
7 an acquiring institution;
8 transmitting, by the processing network computer to a first authorizing
9 entity computer associated with the sender account identifier, the
10 authorization request message; and
11 facilitating, by the processing network computer, a transfer of funds
12 associated with the value from the first authorizing entity computer associated
13 with the sender account identifier to a second authorizing entity computer
14 associated with the receiver account identifier.

1 18. The method of claim 17, wherein the transfer of funds is
2 included in a settlement process between a first authorizing entity associated
3 with the first authorizing entity computer and a second authorizing entity
4 associated with the second authorizing entity computer.

1 19. The method of claim 17, wherein the transfer of funds occurs on
2 the same day as the day that the authorization request message is
3 transmitted to the first authorizing entity computer.

1 20. The method of claim 19, wherein the sender account identifier
2 and the receiver account identifier are card identifiers.