

Blockchain-based System and Method for Federated Automated Teller Machine Management

Technical Field

[0001] The present invention relates broadly, but not exclusively, to servers, methods and distributed ledger networks for processing a transaction at an automated teller machine. Specifically, it relates to a blockchain-based system and method for federated Automated Teller Machine (ATM) management

Background Art

[0002] An Automatic Teller Machine (ATM) is an electronic device which provides transaction services to customers of financial institutions. The transaction services typically include cash withdrawals, cash deposits and fund transfers. ATMs can be placed at any location, but are most commonly installed at locations with high human traffic such as train stations, airports, and shopping malls. As ATMs operate round-the-clock, ATMs provide convenience and ease of access to customers seeking transaction services beyond the financial institutions' operating hours. Moreover, when located off-premises, ATMs can extend the financial institutions' geographical reach while providing efficient and timely transaction services. ATMs can also augment the service capacity of financial institutions as their customer base increase, and can reduce the need for financial institutions to open additional branches and/or hire additional staff.

[0003] However, financial institutions such as banks, typically operate individual ATM networks, and install their own ATMs in various locations. The banks typically do not share ATM networks as the systems on ATMs are often proprietary. Therefore, it is common to see ATMs owned by different banks located in close proximity or even side-by-side. Financial institutions often incur considerable operational costs (such as electricity and land lease) as a result of owning and sustaining the ATM networks, especially in low-use locations.

[0004] Fig. 9A and the below-mentioned steps describe a conventional transaction process flow when a customer of a financial institution (e.g. Bank A) initiates a transaction using a payment card (e.g. ATM card) at an ATM of Bank A:

Step 1: An ATM transaction request is initiated. The customer (of Bank A) inserts his ATM card (of Bank A) and enters a personal identification number (PIN) at the ATM (of Bank A).

Step 2: The ATM card details and PIN are verified at ATM switch (of Bank A).

Step 3: Upon confirmation of transaction (e.g. withdrawal of a cash amount) at the ATM (of Bank A) by the customer, a transaction message flows from ATM switch (of Bank A) to a core banking system (CBS) server (of Bank A). At the same time, the ATM switch will log the transaction and create a settlement file that will be used in the settlement process.

Step 4: The transaction is recorded at CBS Server of Bank A upon approval of the transaction (e.g. an amount is debited if the customer has sufficient balance in his account with Bank A).

Step 5: Cash balance at ATM switch (of Bank A) is reduced by the amount debited in Step 4.

Step 6: The debited amount is dispensed to the customer, and ATM (of Bank A) counter is reduced by the debited amount.

[0005] Fig. 9B shows a conventional transaction process flow when a customer of a financial institution (e.g. Bank A) initiates a transaction using a payment card (e.g. ATM card of Bank A) at an ATM of another financial institution (e.g. Bank B). As shown in Fig. 9B, it is possible for a bank's customer to initiate transactions using the bank's payment card at ATMs owned by another bank. Conventionally, upon confirmation of transaction at the ATM (of Bank B), the transaction message initiated by the customer of Bank A would be routed to the CBS server of Bank A via the ATM switch of Bank B, an interbank network switch (shown as "National Finance Switch") and ATM switch of Bank A. The transaction message is logged at every stage. A surcharge is typically imposed on the customer for the use of Bank B's ATM.

[0006] Accordingly, what is needed is a server, a method and a network for processing a transaction request at an ATM that seek to address one or more of the above-mentioned problems. Furthermore, other desirable features and characteristics will become apparent from the subsequent detailed description and the appended claims, taken in conjunction with the accompanying drawings and this background of the disclosure.

Summary of Invention

[0007] An aspect provides a server for processing a transaction request at an automated teller machine (ATM), the ATM being a node in a distributed ledger network, the server being managed by an issuer who is a party in the distributed ledger network, the distributed ledger network being configured for maintaining a distributed ledger, the server comprising:

at least one processor; and

at least one memory including computer program code;

the at least one memory and the computer program code configured to, with the at least one processor, cause the server at least to:

receive, from the ATM, the transaction request comprising an encrypted identifier associated with an account and a transaction amount;

decrypt the encrypted identifier using a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account; and

process the transaction request in response to the decryption.

[0008] Another aspect provides a method for processing a transaction request at an automated teller machine (ATM), the ATM being a node in the distributed ledger network, the distributed ledger network being configured for maintaining a distributed ledger, the method comprising:

receiving, at a server managed by an issuer who is a party in a distributed ledger network, the transaction request comprising an encrypted identifier associated with an account and a transaction amount;

decrypting, at the server, the encrypted identifier using a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account; and

processing, at the server, the transaction request in response to the decryption.

[0009] A further aspect provides an automated teller machine (ATM) for processing a transaction request, the ATM being a node in the distributed ledger network, the distributed ledger network being configured for maintaining a distributed ledger, the ATM associated with an issuer who is a party in the distributed ledger network, the ATM comprising:

at least one processor; and

at least one memory including computer program code;

the at least one memory and the computer program code configured to, with the at least one processor, cause the ATM at least to:

receive a transaction request comprising an encrypted identifier associated with an account, and a transaction amount;

forward, to a server, the transaction request, the server being one that is managed by the issuer; and

receive, from the server, a transaction response based on a result of a decryption of the encrypted identifier, the encrypted identifier decryptable with a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account.

[0010] Yet another aspect provides a method for facilitating a transaction request on an automated teller machine (ATM), the ATM being a node in a distributed ledger network, and associated with an issuer who is a party in the distributed ledger network, the method comprising:

providing, at the ATM, an instruction to receive an ATM transaction request comprising an encrypted identifier associated with an account, and a transaction amount;

providing, at the ATM, an instruction to display a transaction response, the transaction response based on a result of a decryption of the encrypted identifier using a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account.

[0011] Another aspect provides a distributed ledger network for processing a transaction request, the network comprising a plurality of ATMs, each of the plurality of ATMs being a node in a distributed ledger network and associated with a respective issuer who is a party in the distributed ledger network, each of the plurality of ATMs comprising:

at least one processor; and

at least one memory including computer program code;

the at least one memory and the computer program code configured to, with the at least one processor, cause an ATM of the plurality of ATMs at least to:

receive, from one of the plurality of ATMs, the transaction request comprising an encrypted identifier associated with an account, and a transaction amount; the encrypted identifier decryptable with a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account;

forward, to at least one of the plurality of ATMs, the transaction request, the at least one of the plurality of ATMs being an endorsing ATM in the distributed ledger network;

receive, from the at least one of the plurality of ATMs, an approval message, the approval message indicating whether the issuer associated with the encrypted identifier permits the transaction request.

[0012] Another aspect provides a non-transitory computer readable medium having stored thereon an application which when executed by a computer causes the computer to perform steps comprising:

receiving, at a server managed by an issuer who is a party in a distributed ledger network, the transaction request comprising an encrypted identifier associated with an account and a transaction amount;

decrypting, at the server, the encrypted identifier using a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account; and

processing, with the server, the transaction request in response to the decryption.

Brief Description of Drawings

[0013] Embodiments of the disclosure will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only, and in conjunction with the drawings, in which:

Fig.1

[0014] Fig. 1 shows a schematic diagram of a distributed ledger network for processing a transaction request at an ATM, in accordance with embodiments of the disclosure.

Fig.2

[0015] Fig. 2 shows a schematic diagram of a distributed ledger network for processing a transaction request at an ATM, in accordance with embodiments of the disclosure.

Fig.3

[0016] Fig. 3A shows a schematic diagram of a server for processing a transaction request at an ATM, in accordance with embodiments of the disclosure. Fig. 3B shows a schematic diagram of an ATM for processing a transaction request, in accordance with embodiments of the disclosure.

Fig.4

[0017] Fig. 4 shows a flowchart illustrating a method for processing a transaction request at an ATM, in accordance with embodiments of the disclosure.

Fig.5

[0018] Fig. 5 shows a flowchart illustrating a method for facilitating a transaction request on an ATM, in accordance with embodiments of the disclosure.

Fig.6

[0019] Fig. 6 shows a permissioned distributed ledger architecture for processing a transaction request on an ATM, in accordance with embodiments of the disclosure.

Fig.7

[0020] Fig. 7 shows a sequence diagram for processing a transaction request on an ATM, in accordance with embodiments of the disclosure.

Fig.8

[0021] Fig. 8 shows a schematic diagram of a computing device used to realise the server, ATM and distributed ledger network of Figs. 1-3.

Fig.9

[0022] Figs. 9A and 9B show conventional systems for processing a transaction request, in accordance with embodiments of the disclosure.

[0023] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been depicted to scale. For example, the dimensions of some of the elements in the illustrations, block diagrams or flowcharts may be exaggerated in respect to other elements to help to improve understanding of the present embodiments.

Description of Embodiments

Overview

[0024] Various embodiments of the present disclosure provide a server, a method and a network for processing a transaction request at an Automated Teller Machine (ATM). More specifically, embodiments of the present disclosure provide a server, a method and network using distributed ledger technology (also known as blockchain technology) which can free financial institutions from ownership and operation of ATM networks. The financial institutions instead participate in a distributed ledger network configured to process transactions, the network comprising a plurality of ATMs, each of the plurality of ATMs being a node in a distributed ledger network and associated with a respective financial institution who is a party in the distributed ledger network. The plurality of ATMs can be geographically distributed and can allow a user (a customer of a financial institution who is a party in the distributed ledger network) to transact with multiple financial institutions from any one of the plurality of ATMs.

[0025] In various embodiments of the present disclosure, the distributed ledger network can be a permissioned distributed ledger network. That is, the distributed ledger held by each node in the network has an access control layer that only allows specific nodes to perform certain actions on the distributed ledger (e.g. permissions to read, access and write information onto the distributed ledger). The distributed ledger network, in various embodiments, includes servers associated with respective financial institution who is a party in the distributed ledger network and ATMs. The distributed ledger network can also include an overseeing regulator and a certificate authority. Each financial institution party to the distributed ledger network can provide a set of transaction services (e.g. cash withdrawals, cash deposits and fund transfers) which can be accessed directly by any ATM in the network. Integrity of the transaction can be advantageously guaranteed by the distributed ledger network itself, as the distributed ledger is immutable and the distributed ledger network includes multiple validating peers.

[0026] In embodiments of the present disclosure, a subset of the plurality of ATMs in the permissioned distributed ledger network can function as transaction validators which execute instructions based on a set of pre-defined rules called smart contracts. Records of executed transactions, also known as blocks, are stored on the distributed ledger (also known as a blockchain). As will be explained in more detail below, each block (i.e. record) contains at least a cryptographic hash of the preceding block, a timestamp associated with a time at which the transaction request is received and transaction details including an encrypted identifier and a transaction amount. As each block contains a hash of the preceding block, the linked blocks forms a chain, and the iterative process of generating a block with the preceding hash value confirms integrity of preceding blocks. In other words, as each entry in the distributed ledger is chain-hashed with the preceding entry, alteration of any entry in the distributed ledger would not be possible without alteration of all subsequent blocks, which requires consensus of a network majority. The distributed ledger is therefore considered immutable and tamperproof, and can advantageously provide a high level of privacy and security as information on the permissioned distributed ledger network are accessible only by participants (i.e. nodes) on the permissioned network. Moreover, the presence of encrypted identifiers in transaction requests and entries of the distributed ledger can provide a high level of obfuscation of customer's account information.

[0027] In embodiments of the present disclosure, the distributed ledger network can replace the need for a central authority of trust and reliance on an interbank network for logging transaction information, when transactions are performed across financial institutions.

[0028] A sample of a segment of the distributed ledger, showing the encrypted identifier is shown below:

Bank:	A
ID:	HkLRzkLFRSzcUYzDbGgb
Action:	Withdraw
Amount:	50
Hash	3g3m5lAhq9gJqWhwMaOh XX6bQWaQ50sGMLGTL5Sj
Bank:	B
ID:	Yz7XQp9v1IE7opH70lqS
Action:	Withdraw
Amount:	100
Hash	LPwatI2hlw3XN7DYkHQP O0QuNAILxxHAuvbuHAxl
Bank:	C
ID:	QghuQGHeQD2QgBQC0AjR
Action:	Transfer
Amount:	500
Hash:	yvZXH7iax7204zHn3eWx vqZH9pqbU2i5uP91LmZP

[0029] In various embodiments of the disclosure, a hash value of the first transaction can be computed as shown below:

Hash = Hash(Encrypted Identifier + Action + Time + Transaction Amount)

[0030] In various embodiments, hash values of a second transaction onwards can be computed using additionally, the hash value of the preceding block:

Hash = Hash(Hash value of the preceding block + Encrypted Identifier + Action + Time + Transaction Amount)

[0031] As will be described in greater detail below, embodiments of the present disclosure can advantageously provide a consolidated ATM network (based on a permissioned distributed ledger) which can alleviate the need for financial institutions to operate their own individual ATM networks, as ATMs in the network can be bank-agnostic. That is, the ATMs in the distributed ledger network can accept transaction requests from customers of any one of the institutions a party to the distributed ledger network. The consolidated ATM network can allow financial institutions to share ATMs and reduce operational costs by allocating fixed costs of operating the network over a much higher volume of transactions from customers of all participating financial institutions. Unit transactional costs can be lowered, resulting in greater cost savings for both financial institutions and their customers. Furthermore, as the consolidated ATM network leverages on distributed ledger technology, the network can allow financial institutions to improve security, convenience and quality of

ATM services, while enhancing sustainability, efficiency and continued availability of ATMs in various locations, particularly in low-use or remote locations.

[0032] Moreover, in embodiments of the disclosure, operation and upkeep of the distributed ledger network (including ATMs) may be outsourced to a third party vendor. The third party vendor can maintain a pool of ATMs for financial institutions to use upon joining the distributed ledger network. Advantageously, the pool of ATMs can have better utilisation. Embodiments of the disclosure can therefore alleviate the need for institutions to operate and maintain a separate ATM network and reduce costs related to ATM operations.

[0033] In various embodiments of the disclosure, the distributed ledger network can be a federated network (i.e. a federated ATM network). As will be discussed in greater detail below, in a federated ATM network, a consensus mechanism associated with validation of transactions can be controlled by a pre-selected set of nodes (also known as endorsing nodes or endorsing ATMs in the following disclosure), each storing a smart contract comprising rules of an agreement (business logic) for validating the transactions. For example, the consensus mechanism may require a predetermined majority in the federated ATM network (e.g. two-third of the endorsing nodes) to validate a transaction before transaction blocks can be committed to the distributed ledger.

Terms Description (in Addition to Plain and Dictionary Meaning of Terms)

[0034] An account refers to one that is suitable for an ATM transaction. The account can be used for the purpose of cash withdrawals, cash deposits and fund transfers. The account can be a deposit account, a credit card account, a current account, or any other type of account offered by a financial institution, and represents the funds that an account holder has entrusted to the financial institution and from which the account holder can make withdrawals. Alternatively, an account can be a loan account in which case the account holder owes money to the financial institution. In various embodiments of the present disclosure, the account can be associated with an encrypted identifier that is stored on a payment card. The payment card is a card that can be used by an account holder for a transaction at an ATM. In the following disclosure, the term “card” refer to any suitable transaction cards, such as credit cards, debit cards, prepaid cards, charge cards, membership cards, promotional cards, frequent flyer cards, identification cards, gift cards, and/or any other device that may hold account information, such as mobile phones, smartphones, smartwatches, tablets, personal digital assistants (PDAs), and/or computers. Each type of payment card can be used as a method of payment for performing a transaction.

[0035] A database, or databases refer to any databases located within a computing system or remote server such as a computer in a cloud server. The database or databases may each be a cloud database running on a cloud computing platform.

[0036] An issuer refers to financial institution, usually a bank or credit union who offers credit and debit means to consumers (or users). The issuer may manage a corresponding issuer server which can communicate with an ATM. The issuer server is generally associated with the account issuer, i.e. the issuer of the account associated with the account information and used to fund the transaction. The issuer server may include one or more computing devices that are used to process the transaction. The issuer may be an entity (e.g. a company or organisation) which issues (e.g. establishes, manages, administers) an account (e.g. a credit card account, a stored value card, or a debit card account linked to a bank account) and account information. The issuer server may include one or more computing devices that are used to establish communication with another server by exchanging messages with and/or passing information to the other server.

[0037] An Automated Teller Machine (ATM) refers to a device which interfaces with payment cards to facilitate a transaction, and can be also known as a transaction terminal. In the following disclosure, the ATM can be associated with an entity managing the distributed ledger network. The entity can be a respective issuer party to the distributed ledger network. The ATM, being a node in the distributed ledger network, can store a copy of the distributed ledger. In various embodiments, the ATM can be configured to receive a transaction request comprising an encrypted identifier and a transaction amount, and forward the transaction request to a server managed by an issuer. The ATM can also be configured to receive from the server, a transaction response based on a result of a decryption of the encrypted identifier, the encrypted identifier decryptable with a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account. In various embodiments, the ATM can be a node in a federated network (i.e. a federated ATM network). A consensus mechanism associated with validation of transactions can be run on a pre-selected set of nodes (also known as endorsing ATMs), each of the pre-selected set of nodes storing a smart contract for validating the transactions. For example, the consensus mechanism, which includes a Practical Byzantine Fault Tolerance (PBFT) algorithm, can require a predetermined majority in the federated ATM network to validate a transaction prior to committing the transactions to the distributed ledger.

[0038] A transaction generally includes a financial transaction which can effect a change in the balance of financial account(s) of one or more parties. A transaction can also include an

agreement, or communication between a buyer (e.g. a user or account holder) and a seller (e.g. a merchant) to exchange goods and/or services for payment. Examples of transactions include cash withdrawals, cash deposits and fund transfers (e.g. payment of bills, fees and taxes). Accordingly, a transaction request includes information that is exchanged or provided to facilitate the transaction. In embodiments of the disclosure, a transaction request include the encrypted identifier that is associated with the account. The transaction request can also include a transaction amount (e.g. the amount withdrawn, deposited or transferred). In transactions which involve two parties, the transaction request can also include information relating to the merchant, e.g. a merchant's account identifying an acquirer managing the merchant's account. The transaction can also include an electronic funds transfer (i.e. the electronic transfer of money from one financial account to another, either within a single financial institution or across multiple institutions via computer-based systems including the distributed ledger network).

Exemplary Embodiments

[0039] Embodiments of the present disclosure will be described, by way of example only, with reference to the drawings. Like reference numerals and characters in the drawings refer to like elements or equivalents.

[0040] Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

[0041] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as “associating”, “calculating”, “comparing”, “decrypting”, “determining”, “forwarding”, “generating”, “hashing”, “identifying”, “including”, “inserting”, “modifying”, “processing”, “receiving”, “replacing”, “scanning”, “transmitting”, “updating” or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other

data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[0042] The present specification also discloses apparatus for performing the operations of the methods. Such apparatus may be specially constructed for the required purposes, or may include a computer or other computing device selectively activated or reconfigured by a computer program stored therein. The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various machines may be used with programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate. The structure of a computer will appear from the description below.

[0043] In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the disclosure.

[0044] Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a computer. The computer readable medium may also include a hard-wired medium such as exemplified in the Internet system, or wireless medium such as exemplified in the GSM mobile telephone system. The computer program when loaded and executed on a computer effectively results in an apparatus that implements the steps of the preferred method.

[0045] In embodiments of the present disclosure, use of the term 'server' may mean a single computing device or at least a computer network of interconnected computing devices which operate together to perform a particular function. In other words, the server may be contained within a single hardware unit or be distributed among several or many different hardware units.

[0046] Fig. 1 shows a schematic diagram of a distributed ledger network 100 for processing a transaction request. The network 100 includes issuer nodes 102, endorsing ATMs 104 each storing a smart contract 112, non-endorsing ATMs 106, regulator node 108 and certificate authority server 110. The issuer nodes 102, the endorsing and non-endorsing ATMs 104, 106 (also known as endorsing and non-endorsing nodes) and regulator node 108 each stores a permissioned distributed ledger 111. That is, the distributed ledger held by each node 102, 104, 106, 108 in the network has an access control layer that only allows specific nodes to perform certain actions on the distributed ledger. For example, in various embodiments of the disclosure, only nodes specified as a committer node would be able to commit transaction blocks to the distributed ledger, once the transaction has been verified by the endorsing nodes according to a smart contract stored by the endorsing nodes. Smart contracts will be explained in detail further below. In embodiments of the disclosure, the non-endorsing nodes can be configured to commit transaction blocks to the distributed ledger 111, once the transactions have been verified by the endorsing nodes (e.g. endorsing ATMs 104).

[0047] Each issuer node 102 is associated with respective financial institution (shown as Issuer A, B and C) who is a party in the distributed ledger network. Each financial institution that is party to the distributed ledger network can provide a set of transaction services (e.g. cash withdrawals, cash deposits and fund transfers) which can be accessed directly by any ATMs 104, 106 in the network. Each of the ATMs 104, 106 and issuer nodes 102 is enrolled by a membership service (shown in Fig. 6) that forms a component of the distributed ledger architecture. That is, the membership service is responsible for enrolling nodes into the permissioned distributed ledger network. In embodiments of the present disclosure, the membership service can be run on the regulator server 108 associated with certificate authority 110. Enrolment process by the membership process can include each node receiving a set of cryptographic keys from the certificate authority 110, the set of cryptographic keys required for the node to communicate with other nodes in the distributed ledger network 100. Specifically, the certificate authority 110 can provide a number of certificate services relating to node enrolment, transactions invoked on the distributed ledger and Transport Layer Security (TLS) secured connections between nodes of the distributed ledger network.

[0048] With reference to Fig. 6, the membership service can be associated with an enrolment certificate authority (ECA), a transaction certificate authority (TCA) and a TLS certificate authority (TLSCA). That is, the certificate authority 110 can include a ECA, a TCA and a TLSCA. The certificate authority 110 generally manages all trust and security issues

within the distributed ledger network. That is, each node that seeks to join the distributed ledger network has to be equipped with a valid trust certificate issued by the certificate authority 110. The ECA of the certificate authority 110 is configured to issue the trust certificates for enrolment of new nodes in the distributed ledger network and can also be configured to provide nodes with an enrolment certificate pair once enrolled. One certificate is for data signing, while the other is for data encryption. The data encryption certificate can comprise a symmetric encryption key that can be used by all parties (nodes) in the network for the purpose of encrypting the distributed ledger.

[0049] The TCA is configured to issue trust certificates for deployment of smart contracts 112 and for committing transaction records (i.e. transaction blocks) onto the distributed ledger. In various embodiments of the disclosure, the smart contracts 112 are stored by endorsing ATMs 104 which participate in a consensus mechanism to provide validation of transactions. It can be appreciated that in embodiments, the consensus mechanism comprises a Practical Byzantine Fault Tolerance (PBFT) algorithm. An ordering service, run on nodes of the distributed ledger network, implements the PBFT algorithm. The ordering service comprises a consenter service that validates transaction, commits the validated transactions in blocks on the distributed ledger and distributes the blocks to other nodes within the distributed ledger network. The TLSCA is configured to issue trust certificates that secure communication channels between nodes in the distributed ledger network.

[0050] In embodiments of the disclosure, the smart contract 112 is a code that stores rules of an agreement (business logic). The smart contract 112 is stored by the endorsing ATMs 104, and can be run by the endorsing ATMs 104 to verify transaction requests received by the endorsing ATMs 104. In other words, the implementation of the smart contracts 112 in the distributed ledger network 100 advantageously allows nodes to validate a transaction by relying on the consensus mechanism mentioned above, and can replace the need for validation with a trusted third party. In various embodiments, the smart contract 112 can include the follow rules to validate transaction requests including:

- cash withdrawal, wherein the transaction request is validated if a balance of the account identified in the transaction request is more than the withdrawal amount;
- money transfer, wherein the transaction request is validated if a balance of the account from which the amount is withdrawn is more than the amount to be transferred, and wherein a bank account to which the amount is deposited exists.

[0051] Fig. 2 shows a schematic diagram of a distributed ledger network 200 for processing a transaction request at an ATM, in accordance with embodiments of the disclosure. The distributed ledger network 200 is similar to the distributed ledger network 100, but explicitly shows an exemplary endorsing ATM 104 that is in communication with server 202. It is appreciated that each endorsing ATM 104 in the distributed ledger network 100 can be in communication with server 202, and that the server 202 is not shown in Fig. 1 for clarity. In embodiments of the disclosure, the server 202 is configured to process a transaction request. In various embodiments, the server 202 does not store a copy of the distributed ledger 111 and is therefore not a node of the distributed ledger network 100, but is rather in communication with the ATM 104.

[0052] The server 202 is used to implement the method 400 shown in Fig. 4. Fig. 4 shows a flowchart illustrating the method 400 for processing a transaction request at an ATM, in accordance with embodiments of the disclosure. The method 400 broadly includes:

step 402: receiving, at a server managed by an issuer who is a party in a distributed ledger network, the transaction request comprising an encrypted identifier associated with an account and a transaction amount

step 404: decrypting, at the server, the encrypted identifier using a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account; and

step 406: processing, at the server, the transaction request in response to the decryption.

[0053] At step 502, a transaction request 204 is received from an ATM 104. The transaction request 204 can include an encrypted identifier and a transaction amount. In various embodiments, the ATM 104 is a node in the distributed ledger network 100 configured to maintain a distributed ledger 111.. The transaction request 204 can be generated by any one of the ATMs 104, 106 (either by any one of endorsing ATMs 104 or any one of non-endorsing ATMs 106) when an encrypted identifier and a transaction amount is received by the ATM 104, 106. That is, the transaction request 204 received by the server 202 can either be generated by the endorsing ATM 104 shown in Fig. 2, or originate from any one of ATMs 104, 106 in the distributed ledger network 100 (also shown as “client ATM” in Fig. 7). That is, the endorsing ATM 104 can be configured to generate the transaction request 204, or receive the transaction request 104 from the distributed ledger network 100. Where the endorsing ATM 104 generates the transaction request 204, the endorsing ATM 104 is also configured to transmit the transaction request 204 to the distributed ledger

network 100, and in particular to other endorsing ATMs 104 in the distributed ledger network 100. The server 202 which receives the transaction request 204 is managed by an issuer who is a party in the distributed ledger network. The issuer may also be associated with at least one of the issuer nodes 102 in the distributed ledger network 100.

[0054] Particularly, in various embodiments of the disclosure, the encrypted identifier is associated with an account party to the transaction, and can be decryptable only by the issuer which issues the account. That is, the encrypted identifier associated with the account is protected, and each participating issuer (or financial institution) would only be able to determine a customer's account information identifying the account by decrypting the encrypted identifier. As the distributed ledger 111 stores the encrypted identifier and transaction details (i.e. at least the transaction amount) in each block, but not information associated with information identifying the customer's exact account unless otherwise encrypted, the customer's identity can be protected. In other words, the encrypted identifier advantageously ensures that each participating issuer would not be able to derive customer identities of other issuers.

[0055] In various embodiments, the encrypted identifier can be an anonymised identifier. That is, in embodiments of the disclosure, encryption can include anonymization, and the mapping between the customer's account information identifying the account and the anonymised identifier may be stored on database 206 that is in communication with the server 202 as a mapping table. The mapping table can include account information identifying the account and the anonymised identifier. An example of the anonymised identifier is shown below:

Bank	Customer	Anonymised ID
A	John	HkLRzkLFRSzcUYzDbGgbWanHaEJgSfGqk6LPYTUc
B	Dave	Yz7XQp9v1IE7opH70lqS
C	Steve	QghuQGHeQD2QgBQC0AjR

[0056] In various embodiments, the database 206 can store a copy of the decryption key that is associated with the distributed ledger network to identify an issuer which issues the account. The server 202 can be configured to retrieve the decryption key from the linked database 206. At step 504, the server 202 can be configured to decrypt the encrypted identifier using the decryption key, and process the transaction request in response to the decryption at step 506. In response to a successful decryption of the encrypted identifier, the server 202 can be configured to generate and forward an approval request 208 to the

endorsing ATM 104. The approval request 208 can include an identifier based on whether the issuer associated with the encrypted identifier permits the transaction request.

[0057] In embodiments where the transaction request 204 includes a cash withdrawal request, processing of the transaction request 204 in response to a successful decryption, can include comparing the transaction amount with the balance of the account identified in the transaction request 204. Accordingly, the generating and forwarding of the approval request 208 can be made on condition that the transaction amount falls within a predetermined limit, or falls within the balance of the account. In embodiments where the transaction request 204 includes cash deposit request into the account associated with encrypted identifier, processing of the transaction request 204 in response to a successful decryption, can include an identifier confirming that the account associated with the encrypted identifier exists on record of the issuer. In embodiments where the transaction request includes a transfer request between different account issuers, or a cash deposit request into an account that is different from the account associated with the encrypted identifier, it can be appreciated that the ATM 104 can be configured to transmit the transaction request 204 to other servers (not shown) that are similar to the server 202, but being managed by other issuers who are party in the distributed ledger network. Thus, the transaction request 204 can be received by servers managed by the other issuers whose customers' account is to be debited. Accordingly, the generating and forwarding of the approval request 208 can be made on condition that the account to be debited exists. It can be appreciated that the endorsing ATM 104 would receive one or more approval request 208 – one of the one or more approval request 208 sent by the issuer associated with the encrypted identifier, and the other of the more than one approval request 208 sent by the issuer associated with the account to be debited.

[0058] In embodiments of the disclosure, the endorsing ATM 104 generates the transaction request 204, the endorsing ATM 104 can be configured to forward the approval request 208 to the distributed ledger network 100. The endorsing ATM 104 can be further configured to receive approval requests 208 generated by other endorsing ATMs 104 from the distributed ledger network 100. When a majority of approval requests 208 received are valid in accordance with the consensus mechanism (i.e. determined to be valid by an ordering service running on nodes of the distributed ledger network 100, the ordering service implementing the PBFT algorithm), an approval message 210 can be generated by the endorsing ATM 104 and transmitted to the server 202. The approval message 210 indicates whether the issuer associated with the encrypted identifier permits the transaction request

204, as determined by a majority of endorsing ATMs 104 within the distributed ledger network 100.

[0059] The server 202 is configured to receive the approval message 210. In embodiments of the disclosure, the approval message 210 can include a copy of the distributed ledger 111. The server 202 can generate a hash value using at least the encrypted identifier, the transaction amount and a timestamp associated with a time at which the transaction request 204 is received, on receipt of the approval message 210 which indicates that the issuer permits the transaction request. In various embodiments of the disclosure, additionally or alternatively, the server 202 can also include a hash value of a preceding transaction in the generation of a hash value for the present transaction, such that the hash value of the transaction includes at least the hash value of a preceding transaction, the encrypted identifier, the transaction amount and the timestamp.

[0060] In embodiments of the disclosure, the distributed ledger 111 can then be updated by the server 202 using at least the generated hash value. The updated distributed ledger 212 is then forwarded to the endorsing ATM 104. The updated distributed ledger 212 can be in turn forwarded by the endorsing ATM 104 to other nodes of the distributed network 100. In other embodiments of the disclosure, the server 202 can generate a message (not shown) comprising the generated hash value and the transaction request 204. The transaction message is then forwarded to the endorsing ATM 104. The endorsing ATM 104 can upon receipt of the message, update the distributed ledger 111 using at least the generated hash value.

[0061] In embodiments of the disclosure, the server 202 and the endorsing ATM 104 can comprise a single node in the distributed ledger network 100. In other words, the server 202 does not communicate with other nodes within the distributed ledger network 100. In alternate embodiments, the server 202 can additionally communicate with one or more ATMs 104, 106 of the distributed ledger network 100. The server 202 can be further configured to forward the updated ledger 212 to one or more non-endorsing ATMs 106, the non-endorsing ATMs being one that is not configured to forward the approval message 210.

[0062] In embodiments of the disclosure, there can be instances where the approval request 212 may not be received by the endorsing ATM 104, or where the server 202 may not transmit the approval request 212 (e.g. due to a delay in communication with the database 206, a delay in communication between the server 202 and the endorsing ATM 104, or unsuccessful decryption of the encrypted identifier). Nonetheless, the approval

request 208 may still be received by the endorsing ATM 104 from the distributed ledger network 100, as a result of the consensus mechanism validating the transaction request 204. That is, when a majority of approval requests 208 received are valid in accordance with the consensus mechanism (i.e. determined to be valid by a ordering service running on nodes of the distributed ledger network 100, the ordering service implementing the PBFT algorithm), an approval message 210 can be generated by the endorsing ATM 104 and transmitted to the server 202, independent of whether an approval request 208 is received by the endorsing ATM 104 from the server 202, the approval message 210 indicating whether the issuer associated with the encrypted identifier permits the transaction request 204, as determined by a majority of endorsing ATMs 104 within the distributed ledger network 100.

[0063] Fig. 3A shows a schematic diagram of a server 300 for processing a transaction request at an ATM, in accordance with embodiments of the disclosure. In implementations, the server 202 can be generally described as one or more physical devices (i.e. servers) including at least one processor 302 and at least one memory 304 including computer program code. The at least one memory 304 and the computer program code are configured to, with the at least one processor 302, cause the server to perform the operations described in Fig. 4. An example of the server 202 is shown in Fig. 3A. The server 300 can include a receiver module 306, a cryptography module 308, a transmitter module 310. With reference to Fig. 3A, the receiver module 306 can be configured receive the transaction request comprising an encrypted identifier and account information identifying an account. The cryptography module 308 can be configured to decrypt the the encrypted identifier using a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account. The transmitter module 310 can be configured to transmit a result of processing of the transaction request.

[0064] Fig. 3B shows a schematic diagram of an ATM 320 for processing a transaction request, in accordance with embodiments of the disclosure. In implementations, the ATMs 104, 106 can be generally described as one or more physical devices (i.e. servers) including at least one processor 322 and at least one memory 324 including computer program code. The at least one memory 324 and the computer program code are configured to, with the at least one processor 322, cause the server to perform the operations described in Fig. 5. An example of the ATM is shown in Fig. 3A. The ATM 320 can include a receiver module 326, a cryptography module 328, a transmitter module 330, and a display module 322. The at least one memory 324 and the computer program code can be configured to, with the at least one processor 322, cause the server to additionally perform the operations described below. The receiver module 326 can be configured to receive a transaction request comprising an

encrypted identifier associated with an account, and a transaction amount. The transmitter module 330 can be configured to forward, to a server, the transaction request, the server being one that is managed by the issuer. The receiver module 326 can be further configured to receive from the server, a transaction response based on a result of a decryption of the encrypted identifier, the encrypted identifier decryptable with a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account. The at least one memory 324 and the computer program code can be configured to, with the at least one processor 322, cause the server to additionally perform the operations described in Fig. 5, which shows a flowchart illustrating a method 500 for facilitating a transaction request on an ATM, in accordance with embodiments of the disclosure. The display module 332 can be configured to:

at step 502: provide an instruction to receive an ATM transaction request comprising an encrypted identifier associated with an account and a transaction amount.

at step 504: provide an instruction to display a transaction response, the transaction response based on a result of a decryption of the encrypted identifier using a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account.

[0065] Fig. 6 shows a permissioned distributed ledger architecture 600 for processing a transaction request on an ATM, in accordance with embodiments of the disclosure. The distributed ledger architecture 600 includes membership service 602, ATM application 604, peer ATM(s) 606 and ordering service 608. The membership service 602 forms a component of the distributed ledger architecture 600, and is responsible for enrolling nodes (ATMs) into the permissioned distributed ledger network. In embodiments of the present disclosure, the membership service 600 can be run on the regulator server 108 shown in Fig. 1 and associated with certificate authority 110. The membership service can be associated with an enrolment certificate authority (ECA), a transaction certificate authority (TCA) and a TLS certificate authority (TLSCA). Functions of respective certificate authorities ECA, TCA and TLSCA have been described in the preceding paragraphs.

[0066] The ATM application 604 is stored on a non-transitory medium, which when executed by a computer (e.g. ATM 104, 106 of Fig. 1), causes the ATM to perform the steps comprising, transmitting a transaction request (shown as proposal in Fig. 6) comprising an encrypted identifier associated with an account and a transaction amount, receiving an approval request (shown as endorsed response in Fig. 6) from peer ATMs 606, and

generating and transmitting an approval request (shown as transaction in Fig. 6) to an ordering service 608. The ordering service 608 is configured to commit the validated transactions in blocks on the distributed ledger and distribute the updated distributed ledger to other nodes within the distributed ledger network. Further, in embodiments of the disclosure, the ordering service 608 is configured to validate transactions, order transactions in blocks and sends the blocks to the endorser and committer peers. Each peer ATM 606 holds a copy of distributed ledger.

[0067] Fig. 7 shows a sequence diagram 700 for processing a transaction request on an ATM, in accordance with embodiments of the disclosure. The transaction starts with an invocation by a client ATM. The invocation can be cash withdrawal or money transfer initiated by a bank customer. The transaction proposal is then sent by the ATM to endorsing peers (e.g. endorsing ATMs). The endorsing peers will, at step 1 shown in Fig. 7, execute a smart contract. In other words, the endorsing ATMs will endorse the transaction according to the smart contract defined. The endorsement response is then sent back by the endorsing peers to the client ATM. When majority of the endorsement is received at step 2, the transaction will be sent to the ordering service. The ordering service is configured to receive the transaction request from the client ATM, and will, at step 3, order the transactions in a block. The block will then be broadcast at step 4 to all the nodes within the blockchain network. The block will be added to the distributed shared ledger at step 5 by each peer in the blockchain.

[0068] Fig. 8 depicts an exemplary computing device 800, hereinafter interchangeably referred to as a computer system 800, where one or more such computing devices 800 may be used to execute the method 400 of Fig. 4. One or more components of the exemplary computing device 800 can also be used to implement the network 100, the issuer nodes 102, the endorsing ATMs 104, the non-endorsing ATMs 106, the regulator node 108 and the certificate authority server 110. The following description of the computing device 800 is provided by way of example only and is not intended to be limiting.

[0069] As shown in Fig. 8, the example computing device 800 includes a processor 807 for executing software routines. Although a single processor is shown for the sake of clarity, the computing device 800 may also include a multi-processor system. The processor 807 is connected to a communication infrastructure 806 for communication with other components of the computing device 800. The communication infrastructure 806 may include, for example, a communications bus, cross-bar, or network.

[0070] The computing device 800 further includes a main memory 808, such as a random access memory (RAM), and a secondary memory 810. The secondary memory 810 may include, for example, a storage drive 812, which may be a hard disk drive, a solid state drive or a hybrid drive and/or a removable storage drive 817, which may include a magnetic tape drive, an optical disk drive, a solid state storage drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), or the like. The removable storage drive 817 reads from and/or writes to a removable storage medium 877 in a well-known manner. The removable storage medium 877 may include magnetic tape, optical disk, non-volatile memory storage medium, or the like, which is read by and written to by removable storage drive 817. As will be appreciated by persons skilled in the relevant art(s), the removable storage medium 877 includes a computer readable storage medium having stored therein computer executable program code instructions and/or data.

[0071] In an alternative implementation, the secondary memory 810 may additionally or alternatively include other similar means for allowing computer programs or other instructions to be loaded into the computing device 800. Such means can include, for example, a removable storage unit 822 and an interface 850. Examples of a removable storage unit 822 and interface 850 include a program cartridge and cartridge interface (such as that found in video game console devices), a removable memory chip (such as an EPROM or PROM) and associated socket, a removable solid state storage drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), and other removable storage units 822 and interfaces 850 which allow software and data to be transferred from the removable storage unit 822 to the computer system 800.

[0072] The computing device 800 also includes at least one communication interface 827. The communication interface 827 allows software and data to be transferred between computing device 800 and external devices via a communication path 826. In various embodiments of the disclosure, the communication interface 827 permits data to be transferred between the computing device 800 and a data communication network, such as a public data or private data communication network. The communication interface 827 may be used to exchange data between different computing devices 800 which such computing devices 800 form part an interconnected computer network. Examples of a communication interface 827 can include a modem, a network interface (such as an Ethernet card), a communication port (such as a serial, parallel, printer, GPIB, IEEE 1394, RJ45, USB), an antenna with associated circuitry and the like. The communication interface 827 may be wired or may be wireless. Software and data transferred via the communication interface 827 are in the form of signals which can be electronic, electromagnetic, optical or other

signals capable of being received by communication interface 827. These signals are provided to the communication interface via the communication path 826.

[0073] As shown in Fig. 8, the computing device 800 further includes a display interface 802 which performs operations for rendering images to an associated display 850 and an audio interface 852 for performing operations for playing audio content via associated speaker(s) 857.

[0074] As used herein, the term "computer program product" may refer, in part, to removable storage medium 877, removable storage unit 822, a hard disk installed in storage drive 812, or a carrier wave carrying software over communication path 826 (wireless link or cable) to communication interface 827. Computer readable storage media refers to any non-transitory, non-volatile tangible storage medium that provides recorded instructions and/or data to the computing device 800 for execution and/or processing. Examples of such storage media include magnetic tape, CD-ROM, DVD, Blu-ray™ Disc, a hard disk drive, a ROM or integrated circuit, a solid state storage drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), a hybrid drive, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the computing device 800. Examples of transitory or non-tangible computer readable transmission media that may also participate in the provision of software, application programs, instructions and/or data to the computing device 800 include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

[0075] The computer programs (also called computer program code) are stored in main memory 808 and/or secondary memory 810. Computer programs can also be received via the communication interface 827. Such computer programs, when executed, enable the computing device 800 to perform one or more features of embodiments discussed herein. In various embodiments, the computer programs, when executed, enable the processor 807 to perform features of the above-described embodiments. Accordingly, such computer programs represent controllers of the computer system 800.

[0076] Software may be stored in a computer program product and loaded into the computing device 800 using the removable storage drive 817, the storage drive 812, or the interface 850. The computer program product may be a non-transitory computer readable medium. Alternatively, the computer program product may be downloaded to the computer system 800 over the communication path 826. The software, when executed by the

processor 807, causes the computing device 800 to perform the necessary operations to execute the method 400 as shown in Fig. 4.

[0077] It is to be understood that the embodiment of Fig. 8 is presented merely by way of example to explain the operation and structure of the system 800. Therefore, in some embodiments one or more features of the computing device 800 may be omitted. Also, in some embodiments, one or more features of the computing device 800 may be combined together. Additionally, in some embodiments, one or more features of the computing device 800 may be split into one or more component parts.

[0078] It will be appreciated that the elements illustrated in Fig. 8 function to provide means for performing the various functions and operations of the system as described in the above embodiments.

[0079] When the computing device 800 is configured to realise the server 202 for processing a transaction request, the server 202 will have a non-transitory computer readable medium having stored thereon an application which when executed by a computer causes the computer to perform steps comprising: (i) receiving, at a server managed by an issuer who is a party in a distributed ledger network, the transaction request comprising an encrypted identifier associated with an account and a transaction amount, (ii) decrypting, at the server, the encrypted identifier using a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account, and (iii) processing, with the server, the transaction request in response to the decryption.

[0080] It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present disclosure as shown in the specific embodiments without departing from the spirit or scope of the disclosure as broadly described. The present embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

Claims

1. A server for processing a transaction request at an automated teller machine (ATM), the ATM being a node in a distributed ledger network, the server being managed by an issuer who is a party in the distributed ledger network, the distributed ledger network being configured for maintaining a distributed ledger, the server comprising:
 - at least one processor; and
 - at least one memory including computer program code;the at least one memory and the computer program code configured to, with the at least one processor, cause the server at least to:
 - receive, from the ATM, the transaction request comprising an encrypted identifier associated with an account and a transaction amount;
 - decrypt the encrypted identifier using a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account; and
 - process the transaction request in response to the decryption.
2. The server according to claim 1, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the server to:
 - forward, to an endorsing ATM, an approval request in response to a successful decryption of the encrypted identifier, the endorsing ATM being a node in the distributed ledger network; and
 - receive, from the endorsing ATM, an approval message, the approval message indicating whether an issuer associated with the encrypted identifier permits the transaction request, the endorsing ATM being one that is configured to forward the approval message.
3. The server according to claim 1, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the server to:
 - receive, from an endorsing ATM, an approval message, the approval message indicating whether an issuer associated with the encrypted identifier permits the transaction request, the endorsing ATM being one that is configured to forward the approval message.

4. The server according to claims 2 or 3, wherein the approval message indicates that the issuer permits the transaction request, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the server to:
 - generate a hash value using at least the encrypted identifier, the transaction amount and a timestamp associated with a time at which the transaction request is received;
 - update the distributed ledger using at least the generated hash value; and
 - forward, to the endorsing ATM, the updated distributed ledger.
5. The server according to claim 4, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the server to forward the updated ledger to a non-endorsing ATM, the non-endorsing ATM being one that is not configured to forward the approval message.
6. A method for processing a transaction request at an automated teller machine (ATM), the ATM being a node in the distributed ledger network, the distributed ledger network being configured for maintaining a distributed ledger, the method comprising:
 - receiving, at a server managed by an issuer who is a party in a distributed ledger network, the transaction request comprising an encrypted identifier associated with an account and a transaction amount;
 - decrypting, at the server, the encrypted identifier using a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account; and
 - processing, at the server, the transaction request in response to the decryption.
7. The method as claimed in claim 6, further comprising:
 - forwarding, to an endorsing ATM, an approval request in response to a successful decryption of the encrypted identifier, the endorsing ATM being a node in the distributed ledger network;
 - receiving, from the endorsing ATM, an approval message, the approval message indicating whether an issuer associated with the encrypted identifier permits the transaction request, the endorsing ATM being one that is configured to forward the approval message.

8. The method as claimed in claim 6, further comprising:
 - receiving, from an endorsing ATM, an approval message, the approval message indicating whether an issuer associated with the encrypted identifier permits the transaction request, the endorsing ATM being one that is configured to forward the approval message.
9. The method as claimed in claims 7 or 8, wherein the approval message indicates that the issuer permits the transaction request, the method further comprises:
 - generating, at the server, a hash value using at least the encrypted identifier, the transaction amount and a timestamp associated with a time at which the transaction request is received;
 - updating, at the server, the distributed ledger using at least the generated hash value; and
 - forwarding, to the endorsing ATM, the updated distributed ledger.
10. The method as claimed in claim 9, further comprising, forwarding the updated ledger to a non-endorsing ATM, the non-endorsing ATM being one that is not configured to forward the approval message.
11. An automated teller machine (ATM) for processing a transaction request, the ATM being a node in the distributed ledger network, the distributed ledger network being configured for maintaining a distributed ledger, the ATM associated with an issuer who is a party in the distributed ledger network, the ATM comprising:
 - at least one processor; and
 - at least one memory including computer program code;
 the at least one memory and the computer program code configured to, with the at least one processor, cause the ATM at least to:
 - receive a transaction request comprising an encrypted identifier associated with an account, and a transaction amount;
 - forward, to a server, the transaction request, the server being one that is managed by the issuer; and
 - receive, from the server, a transaction response based on a result of a decryption of the encrypted identifier, the encrypted identifier decryptable with a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account.

12. The ATM according to claim 11, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the ATM to:
 - forward, to an endorsing ATM, an approval request that is generated in response to a successful decryption of the encrypted identifier, the endorsing ATM being a node in the distributed ledger network;
 - receive, from the endorsing ATM, an approval message, the approval message indicating whether an issuer associated with the encrypted identifier permits the transaction request, the endorsing ATM being one that is configured to forward the approval message.
13. The ATM according to claim 11, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the ATM to:
 - receive, from the endorsing ATM, an approval message, the approval message indicating whether an issuer associated with the encrypted identifier permits the transaction request, the endorsing ATM being one that is configured to forward the approval message.
14. The ATM according to claims 12 or 13, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the ATM further to:
 - generate an updated distributed ledger with a hash value, the hash value comprising the encrypted identifier, the transaction amount and a timestamp associated with a time at which the transaction request is received; and
 - forward, to the endorsing ATM, the updated distributed ledger.
15. The ATM according to claim 14, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the ATM to forward the updated ledger to a non-endorsing ATM, the non-endorsing ATM being one that is not configured to forward the approval message.
16. A method for facilitating a transaction request on an automated teller machine (ATM), the ATM being a node in a distributed ledger network, and associated with an issuer who is a party in the distributed ledger network, the method comprising:
 - providing, at the ATM, an instruction to receive an ATM transaction request comprising an encrypted identifier associated with an account, and a transaction amount;

providing, at the ATM, an instruction to display a transaction response, the transaction response based on a result of a decryption of the encrypted identifier using a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account.

17. A distributed ledger network for processing a transaction request, the network comprising a plurality of ATMs, each of the plurality of ATMs being a node in a distributed ledger network and associated with a respective issuer who is a party in the distributed ledger network, each of the plurality of ATMs comprising:
 - at least one processor; and
 - at least one memory including computer program code;
 - the at least one memory and the computer program code configured to, with the at least one processor, cause an ATM of the plurality of ATMs at least to:
 - receive, from one of the plurality of ATMs, the transaction request comprising an encrypted identifier associated with an account, and a transaction amount; the encrypted identifier decryptable with a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account;
 - forward, to at least one of the plurality of ATMs, the transaction request, the at least one of the plurality of ATMs being an endorsing ATM in the distributed ledger network;
 - receive, from the at least one of the plurality of ATMs, an approval message, the approval message indicating whether the issuer associated with the encrypted identifier permits the transaction request.
18. The distributed ledger network as claimed in claim 17, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the ATM of the plurality of ATMs at least to:
 - generate a hash value using at least the encrypted identifier, the transaction amount and a timestamp associated with a time at which the transaction request is received;
 - update the distributed ledger using at least the generated hash value; and
 - forward, to the at least one of the plurality of ATMs, the updated distributed ledger.
19. The distributed ledger network as claimed in claim 18, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the ATM of the plurality of ATMs to forward the updated ledger to

a non-endorsing ATM, the non-endorsing ATM being one that is not configured to forward the approval message.

20. A non-transitory computer readable medium having stored thereon an application which when executed by a computer causes the computer to perform steps comprising:

receiving, at a server managed by an issuer who is a party in a distributed ledger network, the transaction request comprising an encrypted identifier associated with an account and a transaction amount;

decrypting, at the server, the encrypted identifier using a decryption key that is associated with the distributed ledger network to identify an issuer which issues the account; and

processing, with the server, the transaction request in response to the decryption.