(54) Title: DIGITAL BANKING PLATFORM

(57) Abstract: In accordance with certain aspects of the presently disclosed subject matter, there is provided a digital banking platform configured to enable association of each client with one or more accounts in one or more currencies. Each account can be linked to one or more users with equal or differentiated privileges for viewing and/or executing transacting. The provided design supports multi-tenant deployment avoiding a need in software installation or setup when adding new clients and/or new accounts. A method of operating the platform comprises processing internal and/or external transaction events to manage the client's balances with the help of the one or more digital distributed ledgers, wherein a balance of at least one online bank account is managed separately and independently from a balance of at least one physical bank accounts.

DIGITAL BANKING PLATFORM

TECHNICAL FIELD

The presently disclosed subject matter relates to field of digital financial services and, more particularly, to digital banking.

BACKGROUND

With the development of technology, the banking industry has moved transformation from traditional banking to on-line banking services as, for example, remote deposits, money transfers, bill pay, loan management, online management of accounts, etc. Digital banking is the next expected industry shift to digitizing every program and activity undertaken by financial institutions, their partners and their customers.

Problems of digital banking have been recognized in the conventional art and various techniques have been developed to provide solutions, for example:

US Patent Application No. 2020/0372600 entitled "Integration of Workflow with Digital ID" discloses a technique for performing identity validation using a digital ID shared and trusted among a coalition of institutions.

US Patent Application No. 2020/0067906 entitled "Federated Authentication for Information Sharing Artificial Intelligence Systems" discloses a system that includes an artificial intelligence (AI) system and an information service system. The information service system includes an authentication engine configured to authenticate the AI system to enable data transfers between the AI system and the information service system. The information service system further includes an AI service engine configured to receive behaviour information for the user from the AI system and link the user with a classification type based on the content of the behaviour information.

US Patent Application No. 2019/0385223 entitled "Blockchain Banking Gateway" discloses a technique for integration of traditional core banking with blockchain functionality.

US Patent Application No. 2019/0295114 entitled "Digital Banking Platform and Architecture" discloses a technique of maintaining, generating, tracking, and/or updating maintaining electronic representations of aggregate user behaviour and reward information that operates as a component of a digital banking platform and uses

redemption predictor neural network to identify one or more patterns associated with redemption of one or more electronic offers presented to the plurality of users.

US Patent application No. 2017/0046526 entitled "System and method for Implementing Hybrid Public-Private Block-Chain Ledgers" discloses a technique for generating secured distributed storage ledger structures that facilitate event-based control of tracked assets.

The references cited above teach background information that may be applicable to the presently disclosed subject matter. Therefore, the full contents of these publications are incorporated by reference herein where appropriate for appropriate teachings of additional or alternative details, features and/or technical background.

GENERAL DESCRIPTION

In accordance with certain aspects of the presently disclosed subject matter, there is provided a digital banking platform configured to enable association of each client with one or more accounts in one or more currencies. Each account can be linked to one or more users with equal or differentiated privileges for viewing and/or executing transacting. The provided design supports multi-tenant deployment avoiding a need in software installation or setup when adding new clients and/or new accounts.

In accordance with further aspects and, optionally, in combination with other aspects of the presently disclosed subject matter of the presently disclosed subject matter, there is provided a method of operating a digital banking platform comprising one or more digital distributed ledgers. The method comprises: providing a client with at least one online bank account and at least one physical bank account; and processing internal and/or external transaction events to manage the client's balances, wherein the client's balances are managed with the help of the one or more digital distributed ledgers and wherein a balance of the at least one online bank account is managed separately and independently from a balance of the at least one physical bank accounts.

In accordance with further aspects and, optionally, in combination with other aspects of the presently disclosed subject matter of the presently disclosed subject matter, there are provided one or more computing devices comprising processors and memory, the one or more computing devices configured, via computer-executable instructions, to perform operations for operating, in a cloud computing environment, a digital banking platform comprising one or more digital distributed ledgers, the operations comprising: providing a client with at least one online bank account and at

least one physical bank account; and processing internal and/or external transaction events to manage the client's balances, wherein the client's balances are managed with the help of the one or more digital distributed ledgers and wherein a balance of the at least one online bank account is managed separately and independently from a balance of the at least one physical bank accounts.

In accordance with further aspects and, optionally, in combination with other aspects of the presently disclosed subject matter of the presently disclosed subject matter, the balance of the at least one online bank account and the balance of the at least one physical bank accounts can be managed by the same digital distributed ledger. Each of the balances can be provided as an atomic operation. Updating the least one online bank account and the at least one physical bank account can be provided as a single atomic operation.

In accordance with further aspects and, optionally, in combination with other aspects of the presently disclosed subject matter of the presently disclosed subject matter, the provided technique can further comprise using the one or more digital distributed ledgers for plugging an external entity into at least one API call associated with an operational and/or compliance workflow.

In accordance with further aspects and, optionally, in combination with other aspects of the presently disclosed subject matter of the presently disclosed subject matter, the provided technique can further comprise a compliance verification of a pending transaction, the verification comprising: sending a respective compliance request in- parallel via bank and world-check channels; and submitting the transaction for a final approval responsive to approval the compliance request via the both channels.

In accordance with further aspects and, optionally, in combination with other aspects of the presently disclosed subject matter of the presently disclosed subject matter, the provided technique can further comprise real-time monitoring the client's inputs to predict fraudulent activities using a machine learning model. When, during a transaction process, received a prediction of fraudulent activities, the respective transaction is rejected, in response.

BRIEF DESCRIPTION OF THE DRAWINGS

In order to understand the invention and to see how it can be carried out in practice, embodiments will be described, by way of non-limiting examples, with reference to the accompanying drawings, in which:

Fig. 1 illustrates a generalized block diagram of a digital banking system in accordance with certain embodiments of the presently disclosed subject matter;

Figs. 2 - 4 illustrate non-limiting examples of operations/compliance workflows provided in accordance with certain embodiments of the presently disclosed subject matter; and

Fig. 5 illustrates a generalized scheme of fraud predicting module configured in accordance with certain embodiments of the presently disclosed subject matter.

DETAILED DESCRIPTION

In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, it will be understood by those skilled in the art that the presently disclosed subject matter may be practiced without these specific details. In other instances, well-known methods, procedures, components and circuits have not been described in detail so as not to obscure the presently disclosed subject matter.

Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification discussions utilizing terms such as "processing", "computing", "representing", "comparing", "generating", "requesting", "predicting", "updating" or the like, refer to the action(s) and/or process(es) of a computer that manipulate and/or transform data into other data, said data represented as physical, such as electronic, quantities and/or said data representing the physical objects. The term "computer" should be expansively construed to cover any kind of hardware-based electronic device with data processing capabilities including, by way of non-limiting example, the digital banking platform and sub-systems therein.

The terms "non-transitory memory" and "non-transitory storage medium" used herein should be expansively construed to cover any volatile or non-volatile computer memory suitable to the presently disclosed subject matter.

The operations in accordance with the teachings herein may be performed by a computer specially constructed for the desired purposes or by a general-purpose

computer specially configured for the desired purpose by a computer program stored in a non-transitory computer-readable storage medium.

Embodiments of the presently disclosed subject matter are not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the presently disclosed subject matter as described herein.

Bearing this in mind, attention is drawn to **Fig. 1** illustrating a generalized diagram of a digital banking platform in accordance with certain embodiments of the presently disclosed subject matter.

A digital banking platform **100** comprises one or more computers configured to execute several program components in accordance with computer-readable instructions implemented on a non-transitory computer- readable storage medium. Some of such executable program components are referred to hereinafter as functional modules (sub-systems) comprised in digital banking platform **100**. The functional modules can be implemented in any appropriate combination of software with firmware and/or hardware.

The digital banking platform **100** comprises an Authentication Sub-System **101** operatively connected to a Workflow Sub-System **102**. Workflow Sub-System **102** is operatively connected to a Transaction and General Ledger Sub-System **103** which is operatively connected to a Fee Calculation Sub-System **104**. Platform **100** further comprises a User Privileges Store **105** operatively connected to Authentication Sub-System **101** and to Workflow Sub-System **102**, a Transactions and Account Store **106** operatively connected to Transaction and General Ledger Sub-System **103**, and a Fee Configuration Store **107** operatively connected to Fee Calculation Sub-System **104**.

Authentication Sub-System **101** is configured to enable encryption of all in/out traffic of the platform by SSL keys and transmission the traffic in accordance with HTTPS protocol. Logging into platform **100** can be based on multi-factor authentication and can require a unique username and strong password. The User Privileges Store **105** is configured to store and maintain application permissions as well as users' roles and privileges, these data usable by Authentication Sub-System **101** and Workflow Sub-System **102**.

Each client session is configured to be secured by receiving an encrypted JWT token that enables enforcing timeout, securing from session hijack, encrypting user privileges, etc.

In accordance with certain embodiments, JWT (JSON Web Token) tokens are signed either using a private secret or a public/private key, thereby preventing user spoofing. Accordingly, external users can only access their designated accounts and view, merely, their own data.

The platform is configured to enable association of each client with one or more accounts in one or more currencies. Each account can be linked to one or more users with equal or differentiated privileges for viewing and/or executing transacting.

The provided design supports multi-tenant deployment avoiding a need in software installation or setup when adding new clients and/or new accounts.

Transaction & General Ledger Sub-System **103** is configured to support at least the following types of transactions:

- Send payment externally: Creates a debit in the client and bank account and credit to fee account and (optionally) debit to fee account for bank fees

- Receive payment externally: Creates a credit to client and bank account and credit to fee account and (optionally) debit to fee account for bank fees

- Convert currency: Creates a debit in the client account and bank account in the original currency and a credit in client account and bank account in the target currency. The fee is calculated and added as a spread to the conversion rate and a credit is created in the fee account.

- Send payment internally: Creates a debit in the sender client account, a credit in the payee client account and a credit to the fee account.

Internal and external transaction events are processed by sub-system **103** to manage the appropriate balances across multiple client accounts and bank accounts in multiple currencies.

In accordance with certain embodiments, client balances are managed with the help of one or more general ledgers, while the balances in client accounts and physical bank accounts are managed independently. Such dual balance management enables flexibility to the system as physical transactions can be optimized to go into/out of different bank account or remittance partners. Sub-system **103** is configured to ensure that all balances are correct and up to date.

Transaction Management & General Ledger Sub-System **103** is configured to maintain data integrity and prevent inconsistency in transactions and/or balances. In accordance with certain embodiments, an account/balance update is configured as an

atomic operation, i.e. all respective transactions and balances will be updated in a single operation or will all fail.

Transaction Management Sub-System **103** is further configured to enable logical integrity. When a transaction is requested by a user, the sub-system immediately reduces the account's available balance. Thus, sub-system **103** allows user's transaction requests only up to the available balance to prevent reducing the balance below zero. The available balance can be changed back only if the transaction is cancelled or rejected. If the transaction is completed, the balance will be changed to match the available balance.

The sub-system is also configured to enable physical integrity, i.e. maintaining data integrity at a physical level. By way of non-limiting example, it can prevent inconsistency due to multiple requests hitting the system at the same time and reducing the balance beyond zero; inconsistency due to multiple transactions created by the system (e.g. credit and fee) when at the database level one transaction is successful and the other fails thereby leading to inconsistent data, etc.

In certain embodiments the sub-system **103** is configured to implement optimistic locking and database transactions mechanism. The respective application server is configured to use a two-phase-commit with the database to keep database transactions atomic, consistent, and isolated from each other.

Workflow sub-system **102** comprises a workflow engine configured to manage the state of the transactions through compliance and operational flows. The workflow engine uses the user roles to determine what operations can be applied on the transaction in each state.

Combining the workflow engine with the one or more general ledgers enables plugging external partners/providers (e.g. banks/payment providers for transaction automation, validation services for compliance check validation, etc.) into workflow API calls.

Fee Calculation Sub-System **104** is configured to manage fee configuration for transaction fees, currency conversion fees, etc. Default fee can be configured by region and currency pair and can be overwritten for specific client to support further customization. Sub-system **104** calculates the fee when a transaction is processed in the platform **100**, and automatically generates a fee transaction to credit the balance of the fee account (which collects all fees in the system) in the relevant currency.

It is noted that the teachings of the presently disclosed subject matter are not bound by the digital banking platform described with reference to **Fig. 1**. Equivalent and/or modified functionality can be consolidated or divided in another manner and can be implemented in any appropriate combination of software with firmware and/or hardware and executed on one or more suitable devices. The disclosed digital banking platform can run in the cloud.

The sub-systems are configured to enable vertical and/or horizontal scaling up. The platform can be designed is lock-free, stateless processing with multi-threaded multi-processes running across one or more virtual machines. Thereby, the platform can be able to process transactions in parallel and to provide massive performance and throughput scale.

The data repositories can be consolidated or divided in other manner; databases can be shared with other systems or be provided by other systems, including third party equipment.

Referring to **Fig. 2**, there is illustrated a non-limiting example of operations workflow provided in accordance with certain embodiments of the presently disclosed subject matter. The figure illustrates a workflow of external integration with Fx provider. As illustrated, responsive to a "create Fx transaction" request, the pending request is stored at a database and an application server sends the data informative of the request to the sub-system **103** and receives the quote that it transfers to the user. In the case of successful process, the application server, responsive to acceptance of the quote by the user, books the quote at sub-system **103**, receives the respective Fx contract and store the contract in the database. Further, the application server sends request to create the respective transaction and forwards the received acknowledgement to the user.

In accordance with certain embodiments of the presently disclosed subject matter, sub-system **103** further contacts a webhook server (via call back) to initiate database updates. Responsive to the call back, the webhook server issues the automated messages, e.g. message informative of transaction update, message informative of balance updates, message with a command to create credit transaction and message with a command to create fee credit transaction.

It is noted that in certain embodiments the database can be replaced by a distributed ledger.

9

Referring to **Fig. 3**, there is illustrated another non-limiting example of operations/compliance workflow provided in accordance with certain embodiments of the presently disclosed subject matter. In the illustrated workflow of externally sending a payment, the compliance verification of a pending transaction request is provided in-parallel via bank and world-check channels. When the request is approved via both channels, the transaction is submitted for final approval.

Referring to **Fig. 4**, there is illustrated yet another non-limiting example of operations/compliance workflow provided in accordance with certain embodiments of the presently disclosed subject matter. The presented workflow illustrates the flexible online onboarding of the new clients.

The onboarding includes providing information on the client and uploading reference documents. Once the process started the system supports interaction between onboarding analysts, compliance, and the client to complete all required information. When all data is collected the system tracks the approval workflow and stores the reference documents and any recommendations/restrictions to be available in the payment system.

The onboarding system is based on a configuration-driven content and workflow engines. The content engine allows changes to the data that is collected about the client and the workflow engine dictates the state-machine the onboarding will go through until complete.

The above technique enables flexible support of different requirement for data/workflow depending on regulatory requirements in different jurisdictions (including a multi-tenant deployment).

Optionally, digital banking platform **100** can further include a fraud predicting module operatively connected to sub-system **103**. A generalized scheme of the fraud predicting module is illustrated in **Fig. 5**.

Traditional monitoring systems consist of static filters (e.g. total transaction amount in a week not greater than x dollars) which are applied on transaction database to look for rule breaches post transaction. The inventors have recognized and appreciated that there is a need to provide real-time pre-transaction monitoring capable of predicting fraudulent activities.

In accordance with certain embodiments of the presently disclosed subject matter the inputs to the model can include:

- structured data stored in the platform (e.g. client onboarding data, historical transactions, historical validation/verification requests and responses for transactions);

- real time streaming inputs (e.g. transaction requests, validation/verification results, etc.)

- user-specified inputs, e.g. configuration of machine learning model (factors, weights, etc.) and supervised learning (demonstrating to the model how to make decisions).

A proprietary deep learning algorithm continuously learns user behavior and constantly adjusts based on real-time data and user configuration.

The outputs of the model include:

- As transaction requests are entered into the system, deeper analysis can be done (e.g. the transaction request does not meet the standard pattern of behavior for this type of client withing x standard deviations) and flagged to operations and compliance staff.

- Continuous processing of system activity triggers predictive analysis that can identify trends of behavior which are potentially fraudulent.

Further, the above machine-learning based analysis of a client behavior can produce client credibility rating. In regions where standardized credit ratings are not available, this has massive value for receiving loans, credit liens, etc.

It is to be understood that the invention is not limited in its application to the details set forth in the description contained herein or illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways. Hence, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting. As such, those skilled in the art will appreciate that the conception upon which this disclosure is based may readily be utilized as a basis for designing other structures, methods, and systems for carrying out the several purposes of the presently disclosed subject matter.

It will also be understood that the system according to the invention may be, at least partly, implemented on a suitably programmed computer. Likewise, the invention contemplates a computer program being readable by a computer for executing the method of the invention. The invention further contemplates a non-transitory computer-readable memory tangibly embodying a program of instructions executable by the computer for executing the method of the invention.

Those skilled in the art will readily appreciate that various modifications and changes can be applied to the embodiments of the invention as hereinbefore described without departing from its scope, defined in and by the appended claims.

CLAIMS

1. A method of operating a digital banking platform comprising one or more digital distributed ledgers, the method comprising:

providing a client with at least one online bank account and at least one physical bank account; and

processing internal and/or external transaction events to manage the client's balances, wherein the client's balances are managed with the help of the one or more digital distributed ledgers and wherein a balance of the at least one online bank account is managed separately and independently from a balance of the at least one physical bank accounts.

2. The method of Claim 1 wherein the balance of the at least one online bank account and the balance of the at least one physical bank accounts are managed by the same digital distributed ledger.

3. The method of Claim 1, wherein an update of each of the balances is provided as an atomic operation.

4. The method of Claim 1, further comprising updating the least one online bank account and the at least one physical bank account as a single atomic operation.

5. The method of Claim 1, further comprising using the one or more digital distributed ledgers for plugging an external entity into at least one API call associated with an operational and/or compliance workflow.

6. The method of Claim 1 further comprising a compliance verification of a pending transaction, the verification comprising: sending a respective compliance request in- parallel via bank and world-check channels; and submitting the transaction for a final approval responsive to approval the compliance request via the both channels.

7. The method of Claim 1 further comprising real-time monitoring the client's inputs to predict fraudulent activities using a machine learning model.

8. The method of Claim 7, further comprising receiving a prediction of fraudulent activities during a transaction process, and rejecting, in response, the respective transaction.

9. One or more computing devices comprising processors and memory, the one or more computing devices configured, via computer-executable instructions, to perform operations for operating, in a cloud computing environment, a digital banking platform comprising one or more digital distributed ledgers, the operations comprising:

providing a client with at least one online bank account and at least one physical bank account; and

processing internal and/or external transaction events to manage the client's balances, wherein the client's balances are managed with the help of the one or more digital distributed ledgers and wherein a balance of the at least one online bank account is managed separately and independently from a balance of the at least one physical bank accounts.

10.   The one or more computing devices of Claim 9, wherein the balance of the at least one online bank account and the balance of the at least one physical bank accounts are managed by the same digital distributed ledger.

11.   The one or more computing devices of Claim 9, wherein an update of each of the balances is provided as an atomic operation.

12.   The one or more computing devices of Claim 9, wherein the operations further comprising updating the least one online bank account and the at least one physical bank account as a single atomic operation.

13.   The one or more computing devices of Claim 9, wherein the operations further comprising using the one or more digital distributed ledgers for plugging an external entity into at least one API call associated with an operational and/or compliance workflow.

14.   The one or more computing devices of Claim 9, wherein the operations further comprising a compliance verification of a pending transaction, the verification comprising: sending a respective compliance request in- parallel via bank and world-check channels; and submitting the transaction for a final approval responsive to approval the compliance request via the both channels.

15.   The one or more computing devices of Claim 9, wherein the operations further comprising real-time monitoring the client's inputs to predict fraudulent activities using a machine learning model.

16.   The one or more computing devices of Claim 15, further comprising receiving a prediction of fraudulent activities during a transaction process, and rejecting, in response, the respective transaction.

17.   A non-transitory computer-readable medium comprising instructions that, when executed by a computing system comprising a memory storing a plurality of program components executable by the computing system, cause the computing system of a

14

digital banking platform comprising one or more digital distributed ledgers to perform the following operations:

provide a client with at least one online bank account and at least one physical bank account; and

process internal and/or external transaction events to manage the client's balances, wherein the client's balances are managed with the help of the one or more digital distributed ledgers and wherein a balance of the at least one online bank account is managed separately and independently from a balance of the at least one physical bank accounts.

18.   The non-transitory computer-readable medium of Claim 17, wherein the balance of the at least one online bank account and the balance of the at least one physical bank accounts are managed by the same digital distributed ledger.

19.   The non-transitory computer-readable medium of Claim 17, wherein an update of each of the balances is provided as an atomic operation.

20.   The non-transitory computer-readable medium of Claim 17, wherein the operations further comprise updating the least one online bank account and the at least one physical bank account as a single atomic operation.

21.   The non-transitory computer-readable medium of Claim 17, wherein the operations further comprising using the one or more digital distributed ledgers for plugging an external entity into at least one API call associated with an operational and/or compliance workflow.

22.   The non-transitory computer-readable medium of Claim 17, wherein the operations further comprise a compliance verification of a pending transaction, the verification comprising: sending a respective compliance request in- parallel via bank and world-check channels; and submitting the transaction for a final approval responsive to approval the compliance request via the both channels.

23.   The non-transitory computer-readable medium of Claim 17, wherein the operations further comprising real-time monitoring the client's inputs to predict fraudulent activities using a machine learning model.

24.   The non-transitory computer-readable medium of Claim 23, further comprising receiving a prediction of fraudulent activities during a transaction process, and rejecting, in response, the respective transaction.
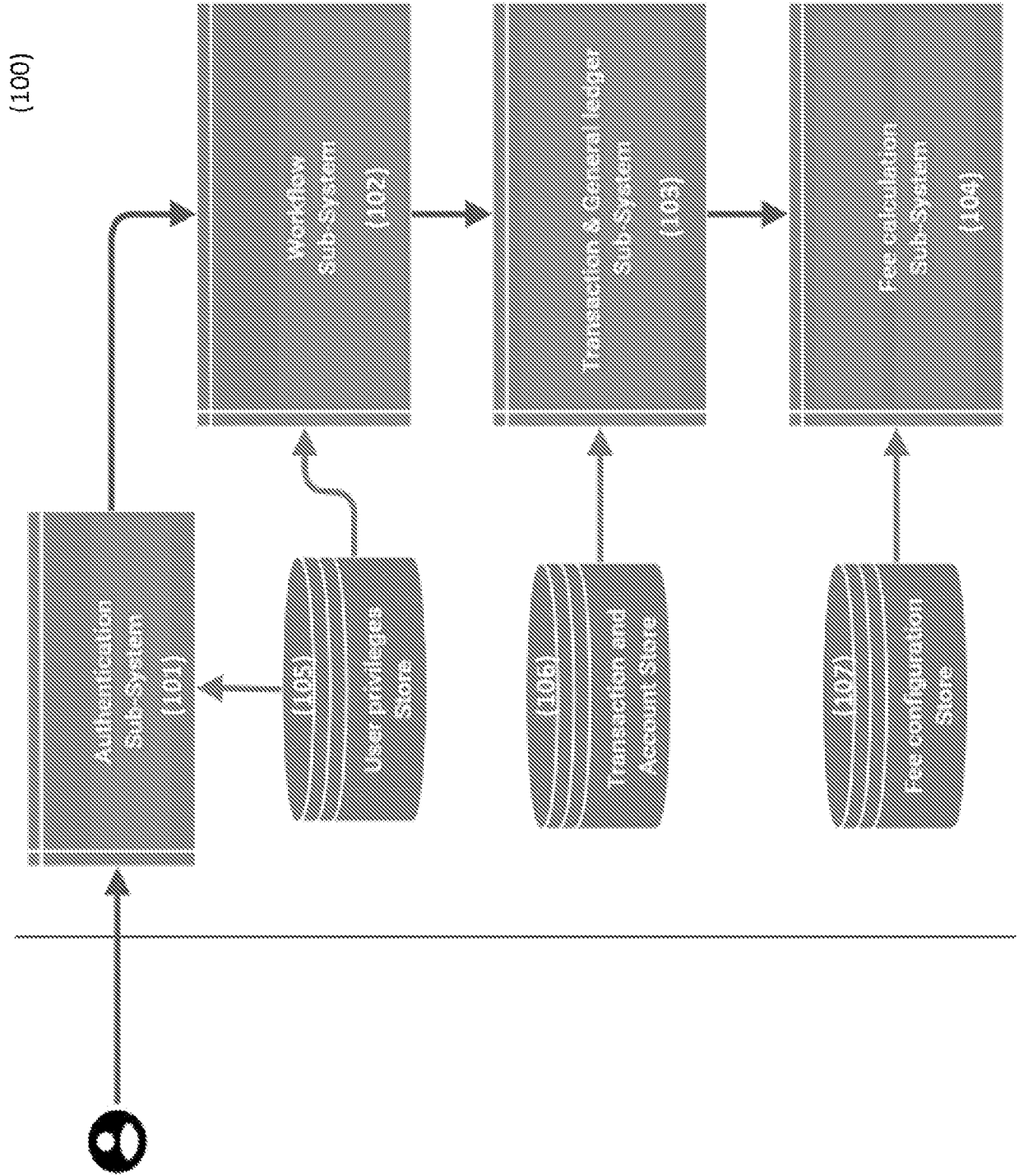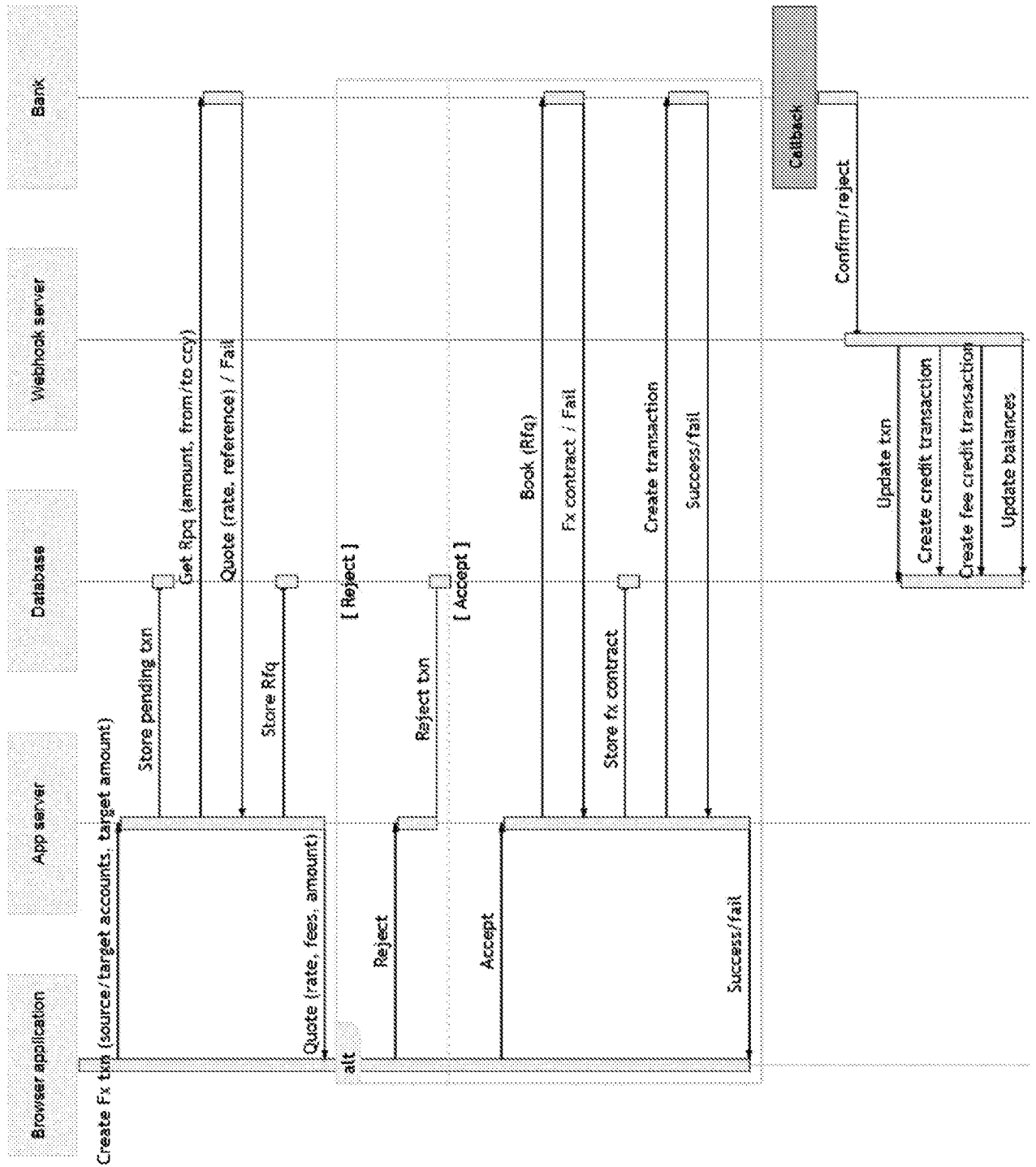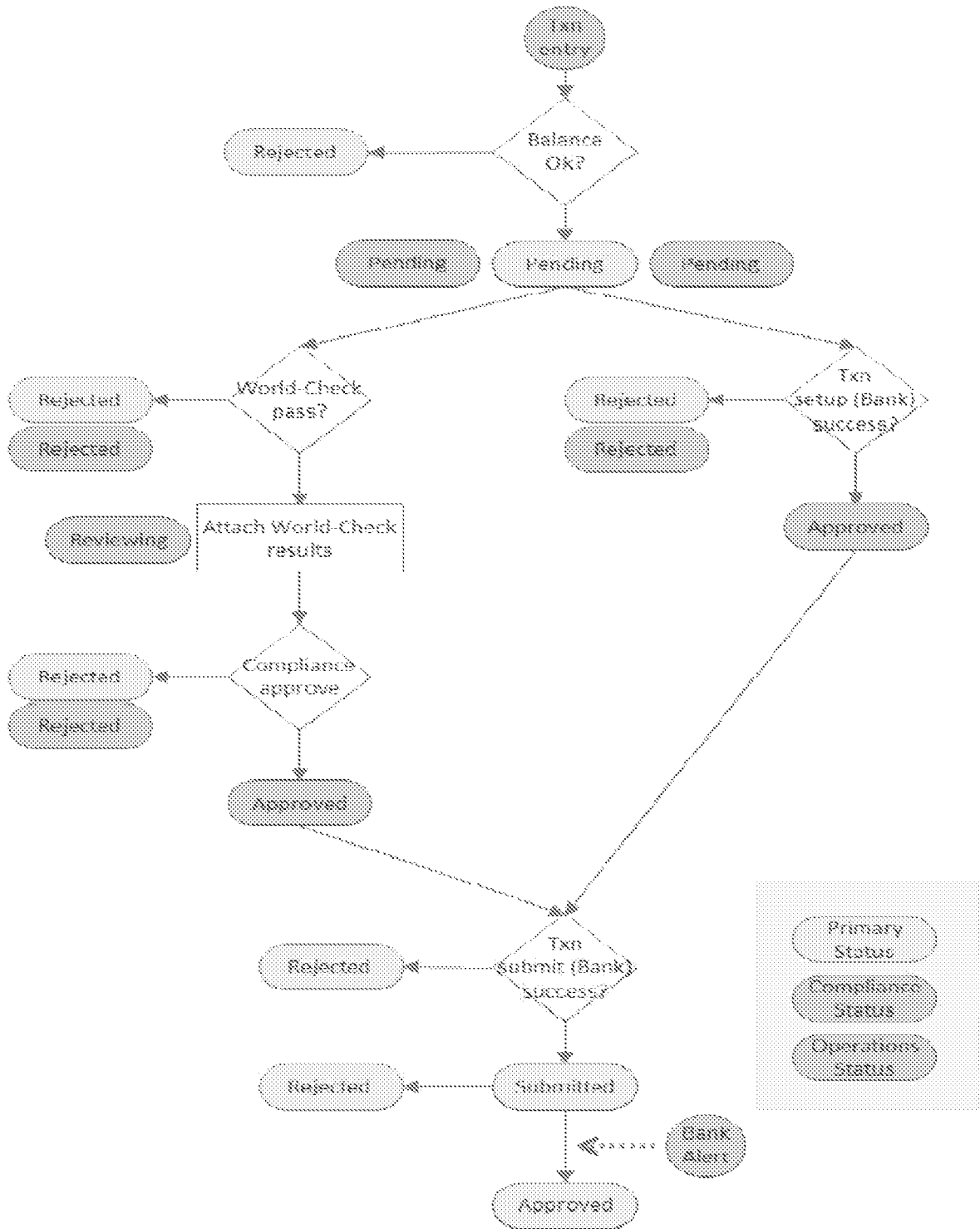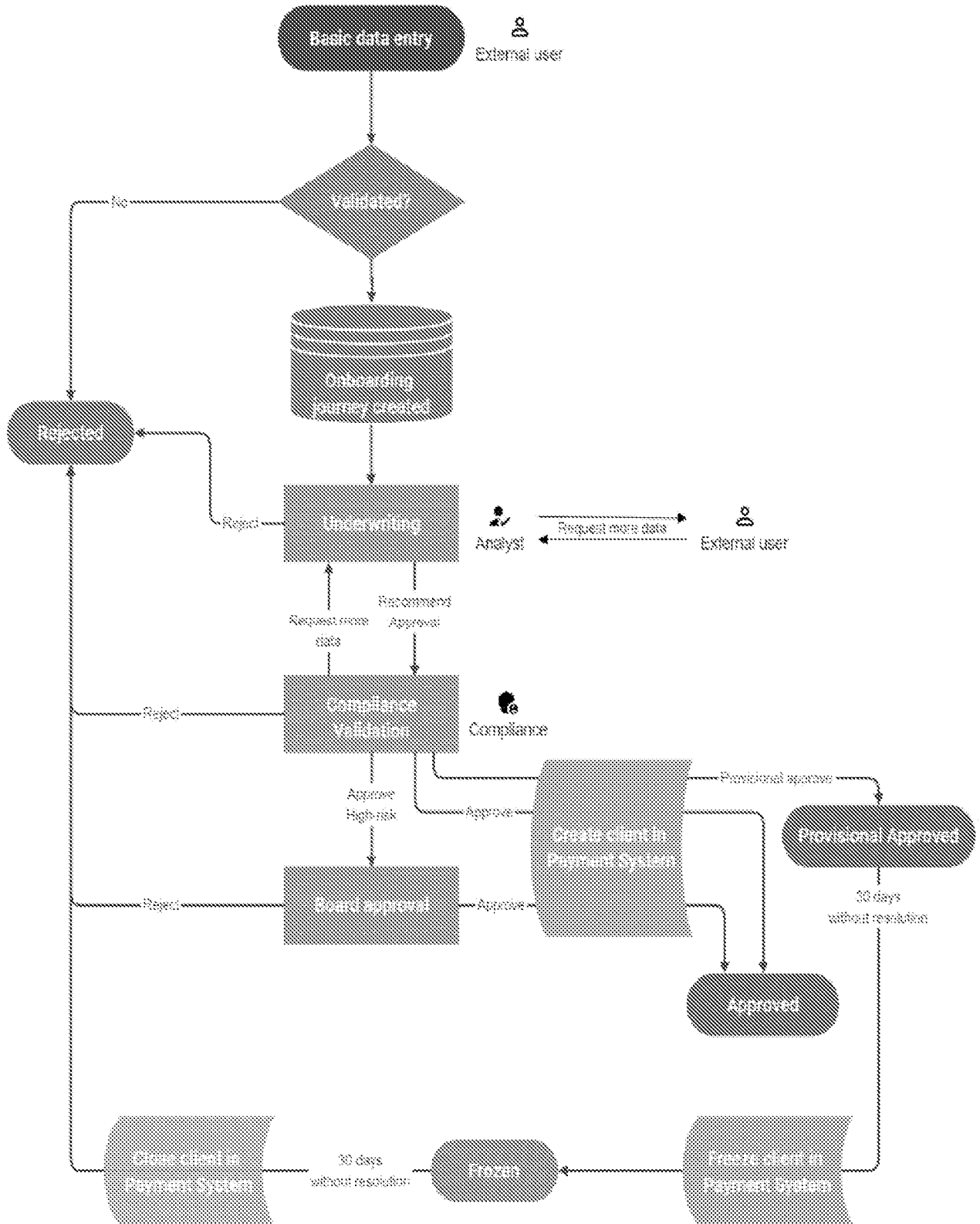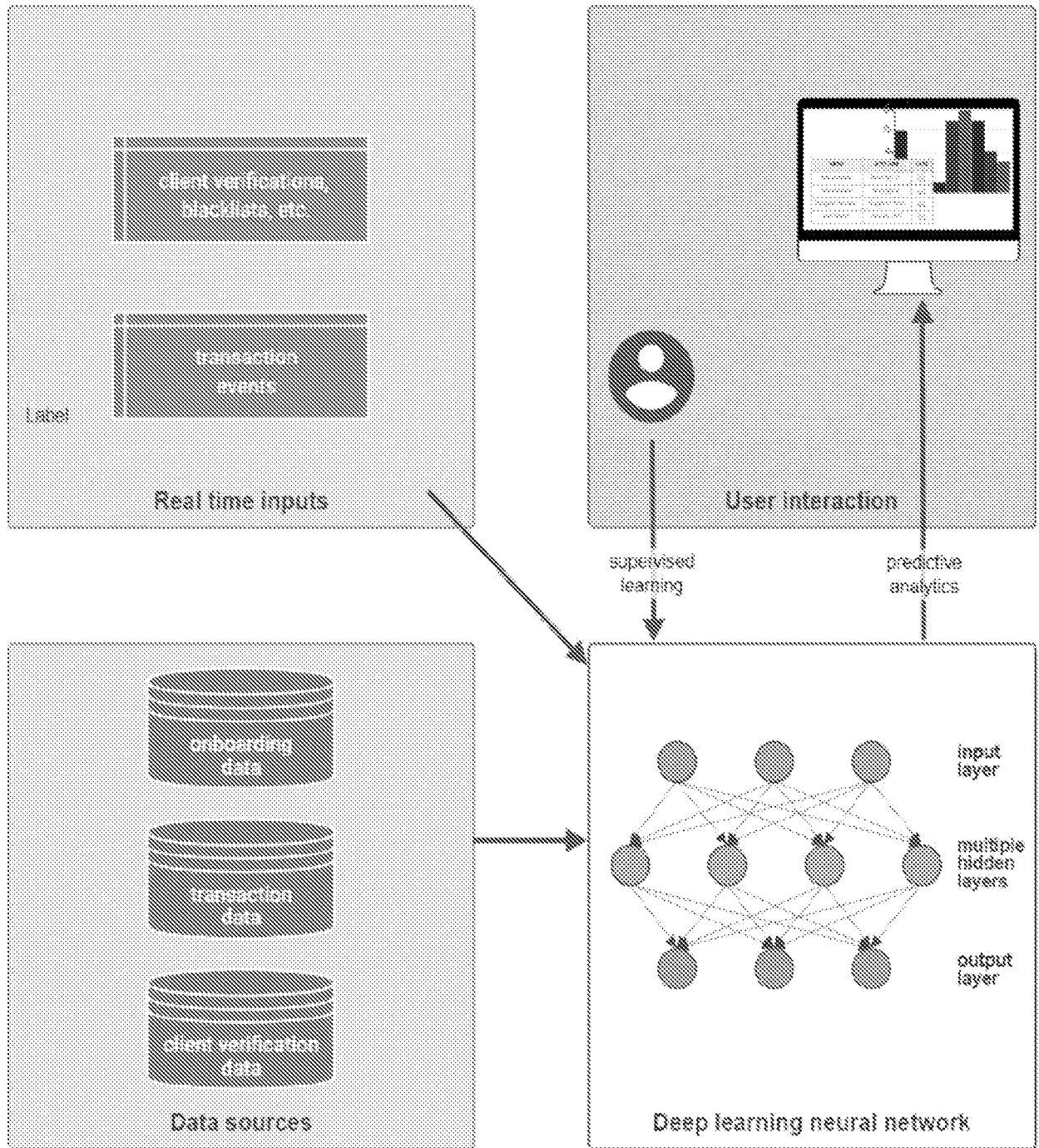
Figure 1

Figure 2

Figure 3

Figure 4

Figure 5

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - INV. - G06Q 20/36; G06Q 20/38 (2022.01)

ADD. - G06Q 20/40 (2022.01)

CPC - INV. - G06Q 20/06; G06Q 20/3676 (2022.08)

ADD. - G06Q 20/4016 (2022.08)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
See Search History document

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/0170112 A1 (DECASTRO) 18 June 2015 (18.06.2015) entire document	1-24
A	US 2017/0178237 A1 (DRAGONFLY FINTECH PTE LTD) 22 June 2017 (22.06.2017) entire document	1-24
A	US 2012/0173415 A1 (EGNATIOS et al) 05 July 2012 (05.07.2012) entire document	1-24
A	US 2021/0004904 A1 (INTERNATIONAL MONETARY EXCHANGE LTD.) 07 January 2021 (07.01.2021) entire document	1-24

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

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"D"	document cited by the applicant in the international application	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier application or patent but published on or after the international filing date		
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 September 2022	OCT 05 2022

Name and mailing address of the ISA/US	Authorized officer
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450	Taina Matos
Facsimile No. 571-273-8300	Telephone No. PCT Helpdesk: 571-272-4300

Form PCT/ISA/210 (second sheet) (July 2019)